ACADEMIC COUNCIL
November 26, 2024
2:30 – 4:30 p.m. – videoconference
Or dial: (CA) +1 289-316-6302 PIN: 845 009 967#

AGENDA	Suggested Start Time
1. Call to Order	2:30 p.m.
2. Agenda (M)	
3. Chair's Remarks	2:35 p.m.
4. Inquiries and Communications a) COU Academic Colleague Report (Mikael Eklund)	2:45 p.m.
5. Provost's Remarks a) Senior Academic Administrator Search Update b) Strategic Mandate Agreement (SMA4) Update (Sarah Thrush)	2:50 p.m.
6. 2025-2026 Budget Approach* (Lori Livingston, Brad MacIsaac & Sarah Thrush)	3:10 p.m.
Committee Reports	
7. Undergraduate Studies Committee (Mary Bluechardt)	3:30 p.m.
8. Graduate Studies Committee (Joe Stokes) a) New Program Proposal – Faculty of Business and IT (FBIT); Doctor of Philosophy – Cybersecurity* (M)	3:35 p.m.

*Documents attached (C) Consultation (D) Discussion (I) Information (M) Motion

9. Research Committee (Les Jacobs) a) New Research Institute – Mindful AI Research Institute* (M) b) Strategic Research Plan Update	3:45 p.m.
10. Policy Consultation (if applicable)	-
11. Consent Agenda: (a) Minutes of the Meeting of October 22, 2024* (M) (b) Conferral of Fall 2024 Degrees*(M)	3:55 p.m.
12. Other Business (a) Land acknowledgement for January Academic Council meeting	4:00 p.m.
Termination (M)	4:05 p.m.

Nicola Crow, University Secretary

Academic Council Written Consultation*:
In accordance with the Policy Framework, see below for items available for Academic Council written consultation by providing feedback to policy@ontariotechu.ca**:**

POLICY	CATEGORY	APPROVING AUTHORITY
1. Anti-Indigenous Racism, Anti-Black Racism Guidelines*	LCG	President
2. Student Mental Health Policy Incl. Supportive Leave Procedure*	ADM	President

ADM = Administrative LCG = Legal, Compliance and Governance

ACADEMIC COUNCIL REPORT

SESSION:		**ACTION REQUESTED:**	
Public	☒	**Decision**	□
Non-Public	□	**Discussion/Direction**	☒
		Information	□

TO: **Academic Council**

DATE: **November 26, 2024**

PRESENTED BY: **Brad MacIsaac, Vice-President, Administration**
Lori Livingston, Provost and Vice-President, Academic
Sarah Thrush, AVP, Planning & Strategic Analysis

SUBJECT: **2025-2026 Budget Assumptions**

BACKGROUND/CONTEXT & RATIONALE:

As we start to plan for the next three years, we will focus on 2025-2026 with assumptions based on this year's information to date. In the past few years, we have provided a Fiscal Blueprint that outlined items such as the provincial landscape, revenue estimates and link funding priorities with the Integrated Academic-Research Plan. With the ongoing funding plus geo-political uncertainty, in addition to stakeholder feedback that the paper was repetitive with the April report, a decision has been made to create a more comprehensive final Budget Paper.

The November information sessions will include the key revenue and expense assumptions for stakeholders to comment on. Leadership has created many scenarios from conservative to aspirational growth plan. The budget will be set with the conservative estimates in mind; however, as in past years, leadership will have a listing of priority spends should extra funds be in place when students register in September. Looking at the conservative scenario the main assumptions to be considered are:

a) Enrolment Revenue: The preparation of the operating budget involves the use of projections and estimates. This major revenue driver assumes enrolment going up over 800 Full-time Equivalents compared to last budget. This is not unrealistic as the number includes an extra 500 that registered September 2024. The risk is related to the international intake due to the federal policy that was implemented in summer 2024 and the revision added in fall 2024.

b) Tuition Revenue: The assumptions include the provincial government continued freeze on domestic rates as announced for at least 2 years. For international we do not have tuition setting restrictions in place; however, based on a review of system comparators both regionally and internationally we are applying a 3% increase to the model. A full program by program review will occur before February.

c) Expenses: We must first manage the mandated salary increases and prioritized hiring plans which will be explained further in the final budget proposal. The first draw on the budget is an investment of $12M more in personnel costs compared to 2023-2024.

d) Reserves: Although there are many competing short-term demands in budget planning we must continue to set aside funds for future years. At the November 2021 Board meeting leadership discussed the Financial Sustainability and Reserves and outlined a need to set aside at least $3M for planned future investments in large-scale repairs/replacements, new priorities/equipment/infrastructure, and contingencies to offset unplanned external budget impacts.

With the current assumptions we are estimating about $260M in revenues and have already committed $252M in expenses. This increased revenue has come from our Differentiated Growth strategy. Maintaining current operating ratios will be a challenge, however we are committed to investing in our people. We are continuing to invest in technology platforms including the new enterprise system plan, and use of AI in reducing effort on high volume tasks. Additionally, the University is undertaking, with funding provided by the government, efficiencies and effectiveness review of key administrative processes.

There are two major unknowns in the revenue scenario. With the international caps we could see intake held at 2023 levels, which could reduce our revenues by over $3M. We also have not heard about the provincial governments efficiency fund which could include an extra $3M one time only support if we receive similar to 2024. As we get closer to setting the budget in March, we will have more clarity on student application numbers and government funding. Like previous years we will work to set a balanced budget along with a list of unfunded priorities that we can act upon should we see more positive numbers.

In every year there is a level of overall risk of not achieving the desired enrolment results (e,g, a 1% deviation in enrolment will lead to ~$1M variance, positive or negative, from tuition fee revenues). Note that the university is normally within ±2% when predicting enrolment totals. The bigger risk may be what is not included in the budget framework. We recognize that inflation and supply issues continue to wreak havoc on some operating expenses. Currently, we have not placed an inflationary increase into the budget. Instead, we are asking for units to put in an ask for us to prioritize or reallocate from within their existing budgets.

DISCUSSIONS:

We are asking if stakeholders are comfortable with the assumption and the balanced approach leadership is taken in setting the budget in these complex times. It is important to note the investments being made to move forward the strategic priorities while balancing the long-term sustainability of the institution.

While this budget continues to move us forward on our mission and priorities there are number of areas that will not be funded to the levels we would like. A desired outcome of the budget presentations is to ensure members are aware of the risks and risk mitigation strategies related most specifically to enrolment, capital renewal and future reserves.

NEXT STEPS:

- Information Sessions will be held over November.
- Budget holders are to complete and submit their budget by December 20th.
- The leadership team will review the formal winter count data and finalize the budget submission.
- This will then be presented to Academic Council in March 2025 and the Audit & Finance Committee in April 2025.

SUPPORTING REFERENCE MATERIALS:

2025-2028 Budget Assumptions, November 2024

OntarioTech
UNIVERSITY

2025-2028 Budget Assumptions

- Lori Livingston, Provost and Vice-President, Academic
- Sarah Thrush, AVP Planning and Strategic Analysis
- Brad MacIsaac, Vice-President Administration

Nov 2024

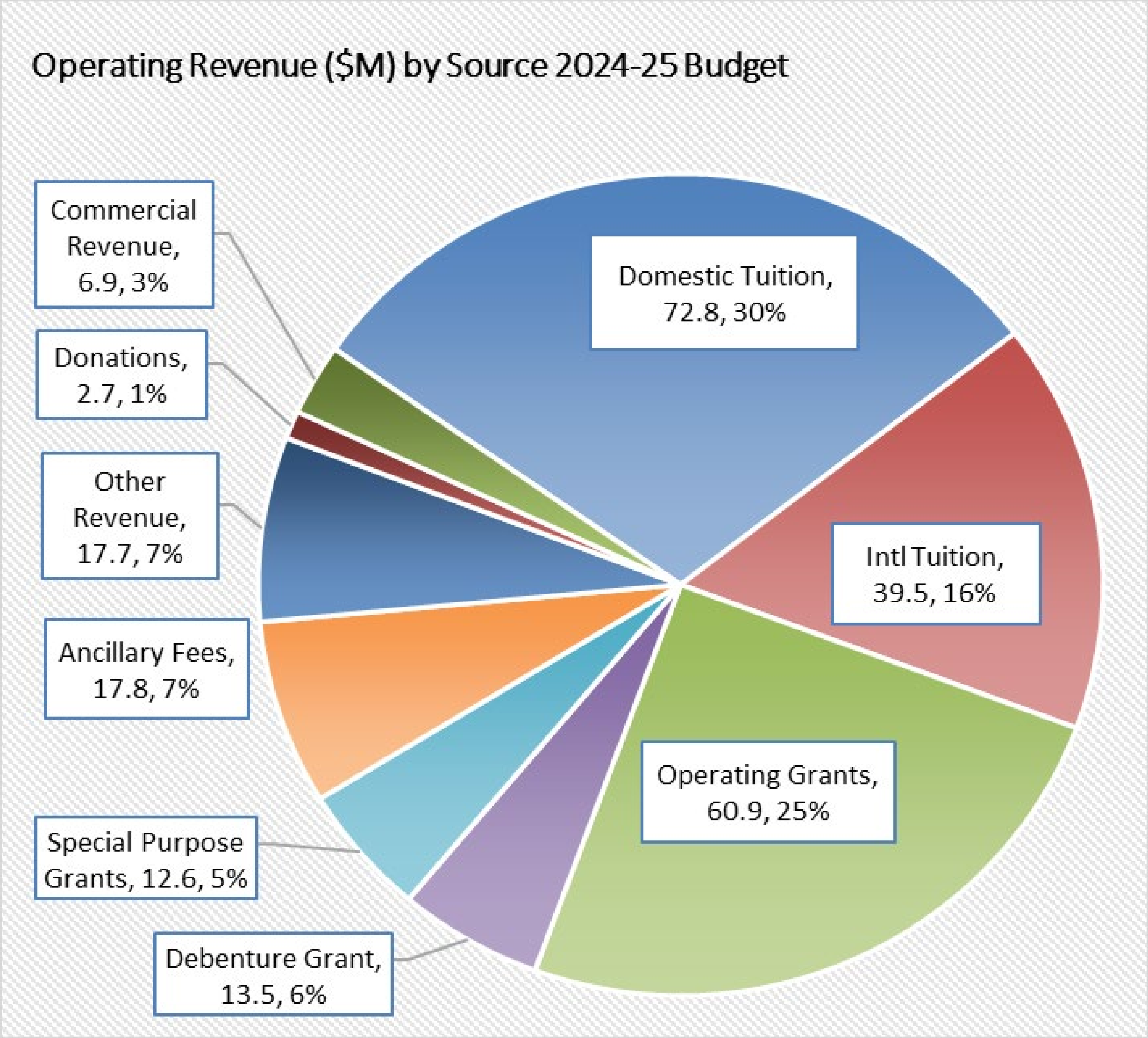
Ontario Tech Budget Process

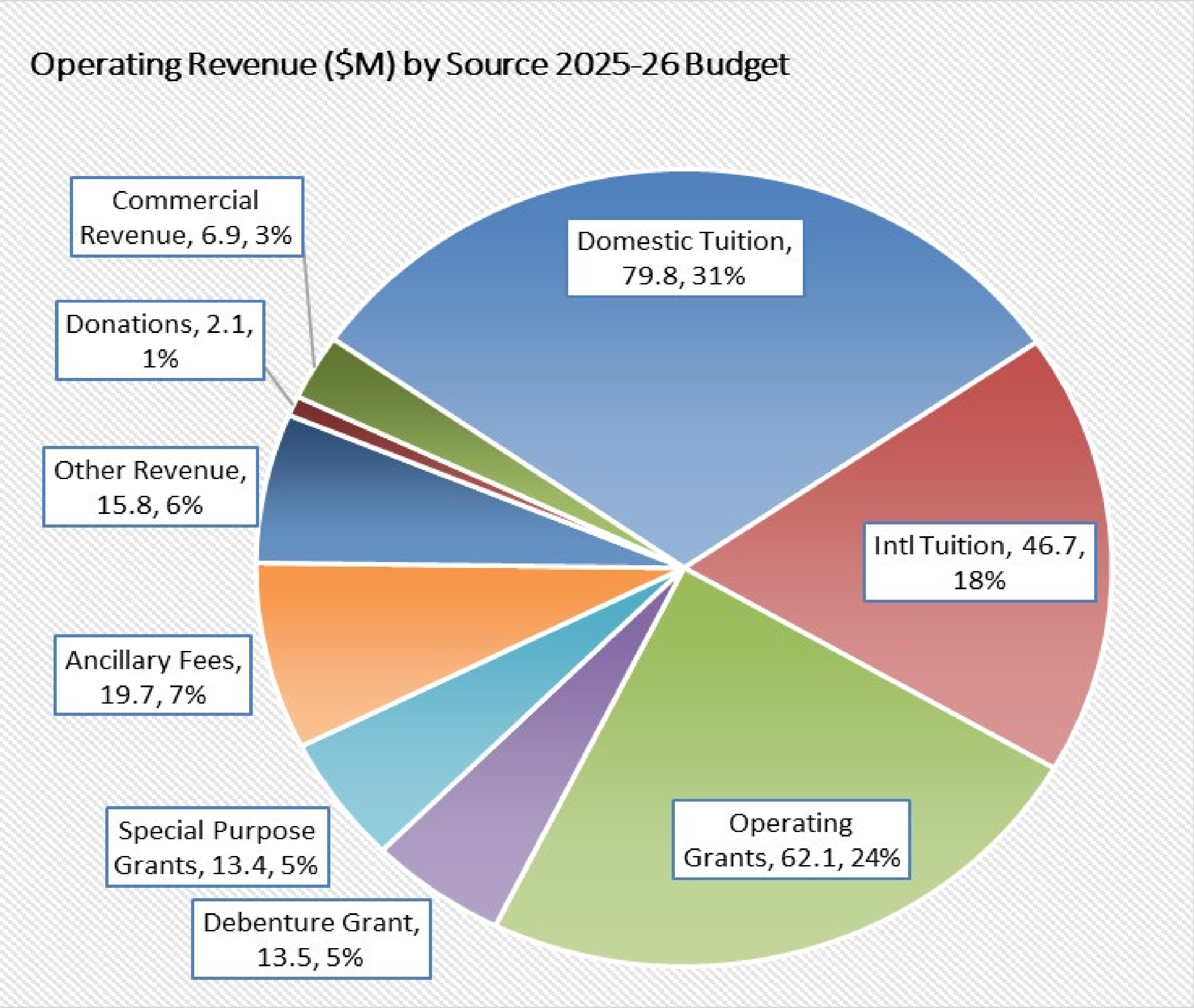
- November present Revenue & Expense assumptions and hold conversation on key priorities

- April present next Budget year plus two out years

  - ❑ https://sites.ontariotechu.ca/finance/index.php
  - ❑ https://sites.ontariotechu.ca/finance/planning-reporting/financial-statements/multi-year-rolling-budget-2024-2027/index.php

Operating Revenue by Source – FY26 ~$260M

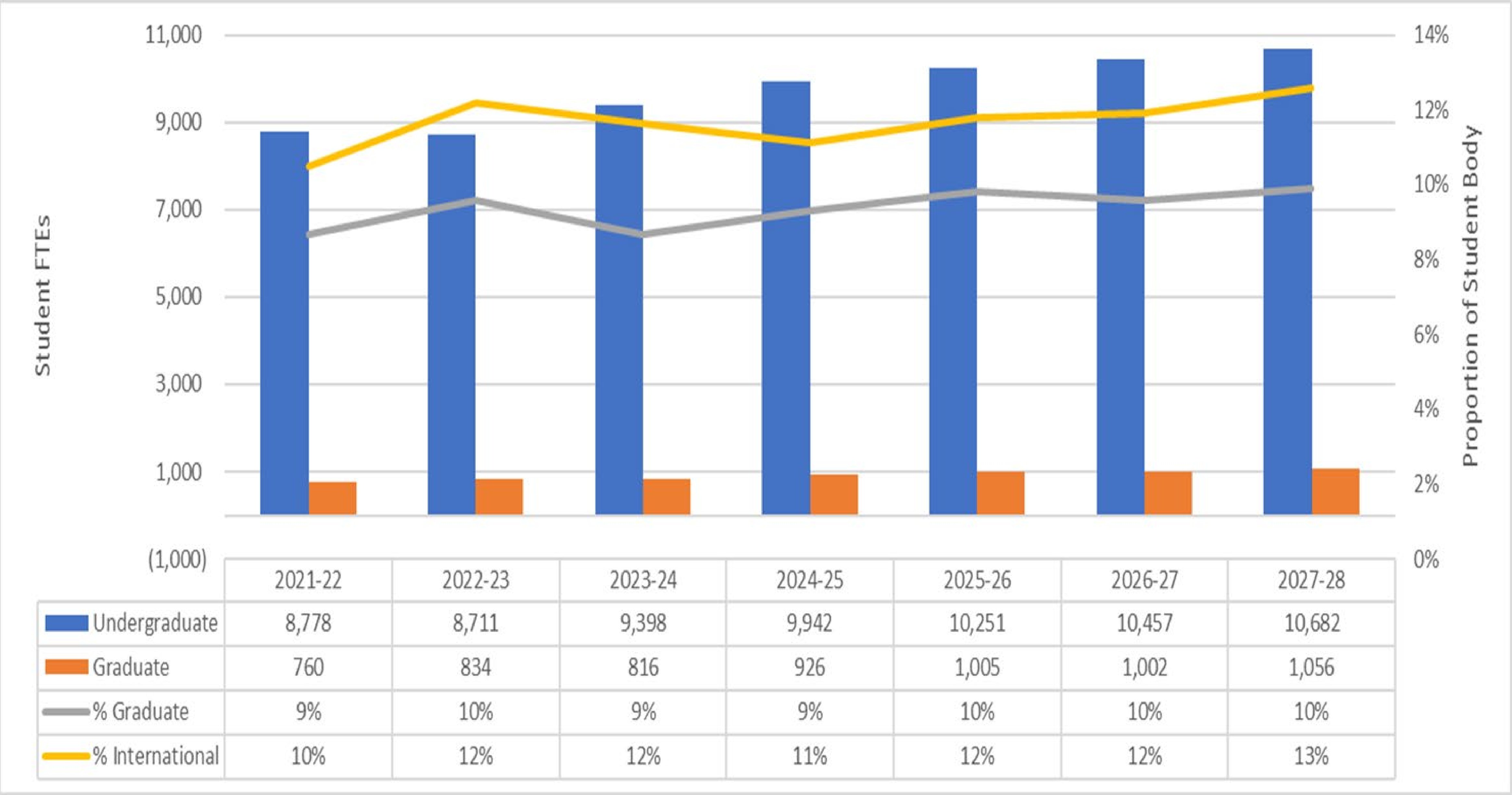




Revenues

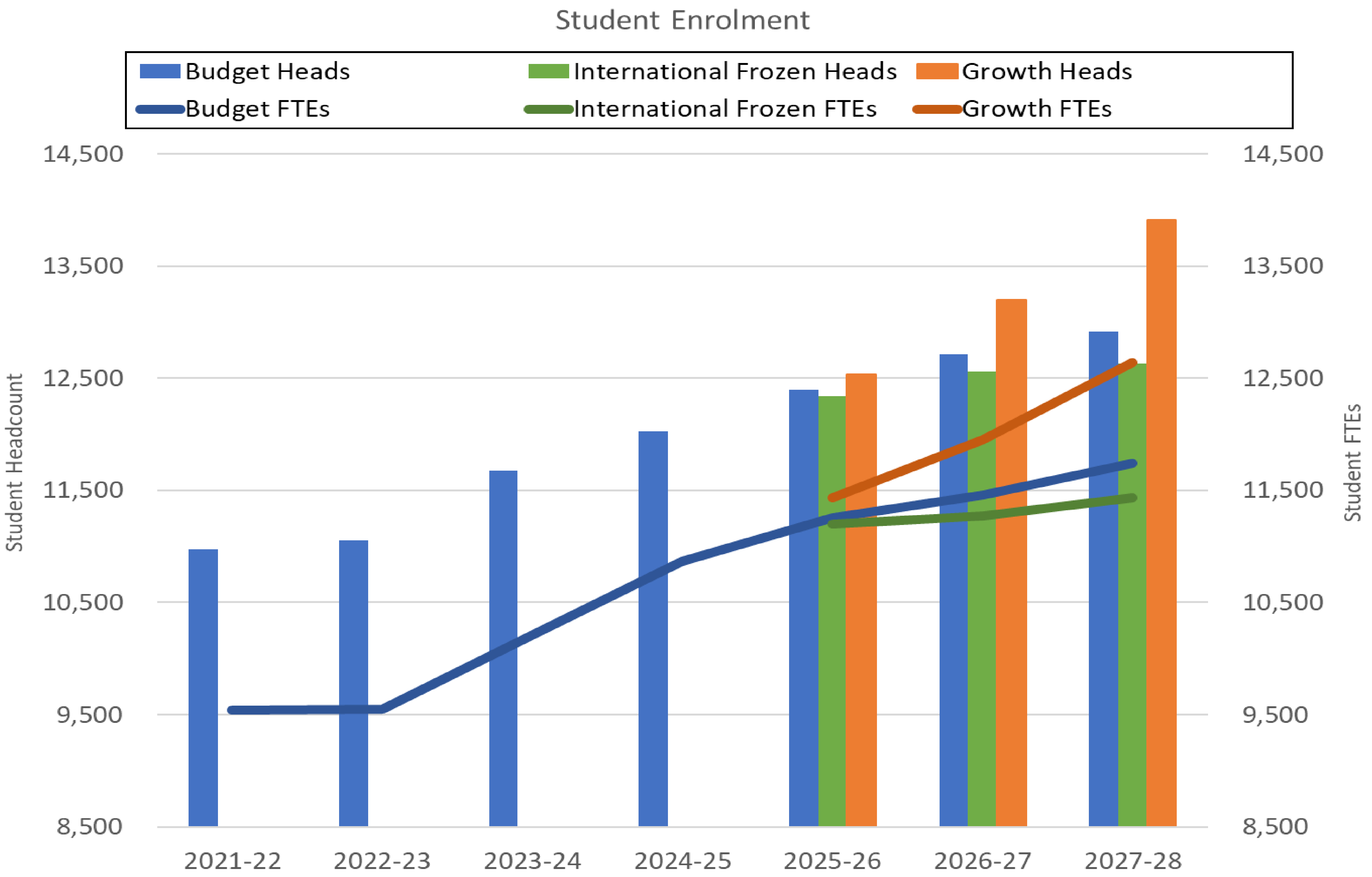
- Government Grants
  - ➢ While modifications have been made over the years, essentially frozen at 2012.
  - ➢ Operating vs Performance
  - ➢ Directed Increases (ie Facilities Renewal, Mental Health, etc)
- Tuition
  - – Domestic (grant eligible) freeze
  - – International 3%
- Ancillary
  - – Fees are collected for specific purposes … so if $2M more basically all allocated

Enrolment Plan - BUDGET



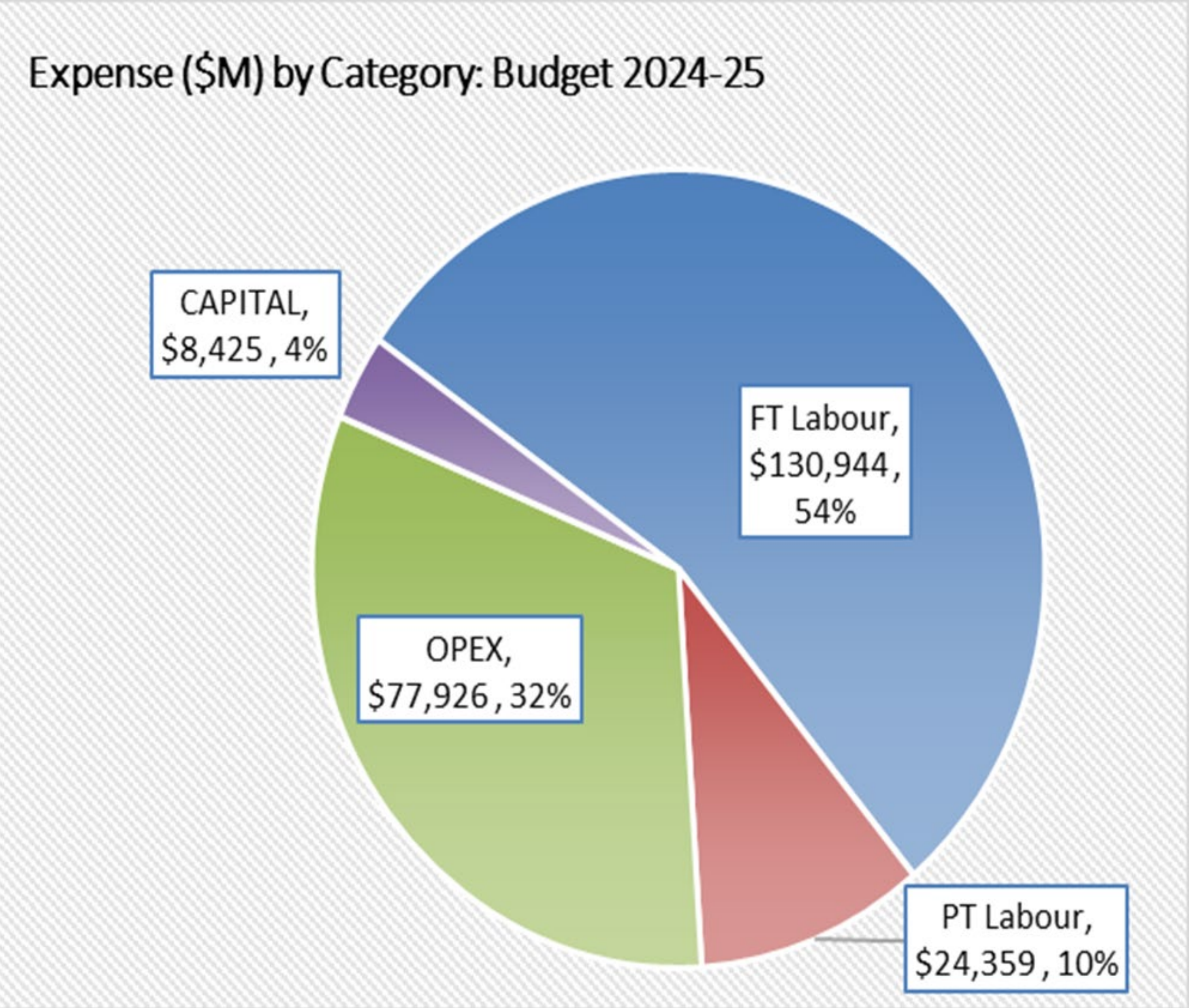
	2021-22	2022-23	2023-24	2024-25	2025-26	2026-27	2027-28
🟦 Undergraduate	8,778	8,711	9,398	9,942	10,251	10,457	10,682
🟧 Graduate	760	834	816	926	1,005	1,002	1,056
▬ % Graduate	9%	10%	9%	9%	10%	10%	10%
▬ % International	10%	12%	12%	11%	12%	12%	13%

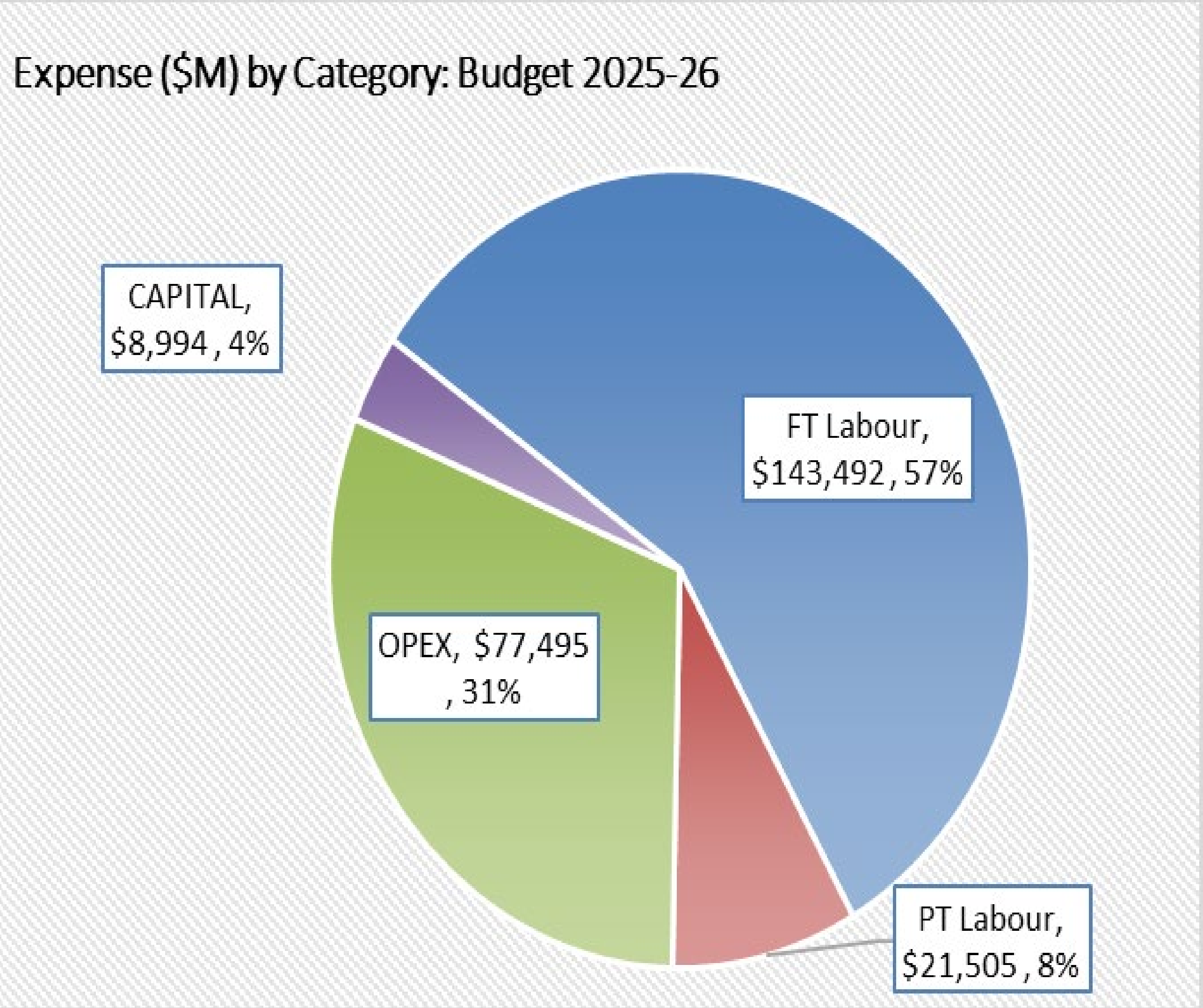
Scenarios



Student Enrolment
Budget Heads
International Frozen Heads
Growth Heads
Budget FTEs
International Frozen FTEs
Growth FTEs
Student Headcount
Student FTEs
14,500
13,500
12,500
11,500
10,500
9,500
8,500
2021-22
2022-23
2023-24
2024-25
2025-26
2026-27
2027-28

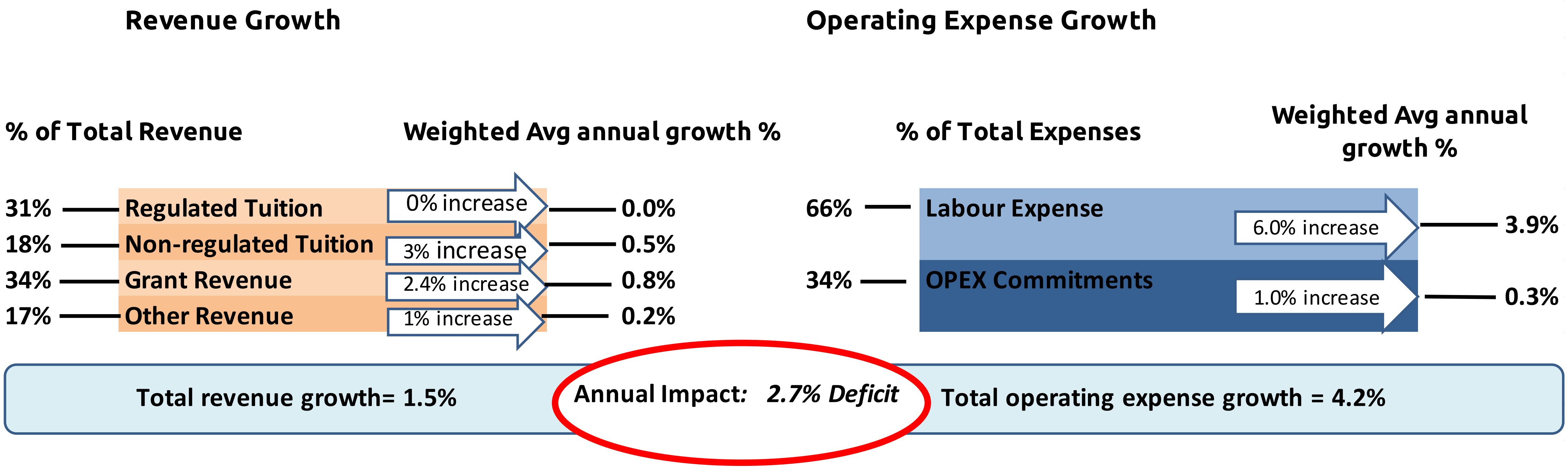
Total Expenses by Category – FT 26 ~252M allocated





Expenses

- Revenue: If UG international went up 3% on average the weighted impact on budget is less than 0.5%.
- Expenses: Looking at current salaries alone when we include ATB and PTR they are going up 6% a year for a weighted average of 3.9%
- Starting base budget DOES NOT include inflationary increase for OPEX. Most units will need to reallocate from within



Revenue Growth

% of Total Revenue

Weighted Avg annual growth %

31% Regulated Tuition 0% increase 0.0%

18% Non-regulated Tuition 3% increase 0.5%

34% Grant Revenue 2.4% increase 0.8%

17% Other Revenue 1% increase 0.2%

Operating Expense Growth

% of Total Expenses

Weighted Avg annual growth %

66% Labour Expense 6.0% increase 3.9%

34% OPEX Commitments 1.0% increase 0.3%

Total revenue growth= 1.5%

Annual Impact: *2.7% Deficit*

Total operating expense growth = 4.2%

Expenses: Examples of Potential Investments by Strategic Priority

- Continued focus on our "Differentiated growth" strategy, other forms of revenue generation (e.g., philanthropy)

- Create reserves to deal with the uncertainty of our fiscal future

Next Steps

- Nov 14 – 27th: Information Sessions (budget managers, Joint Faculty Association, Academic Council, Board Audit & Finance).
- Nov 14th Budget Module Opens
- Dec 20th Budget Submission
- Jan 20th Senior Leaders Budget Retreat
- Late March: Information Sessions
- April 10th Budget presented to Audit & Finance

Questions??

ACADEMIC COUNCIL REPORT

ACTION REQUESTED:

Recommendation ☒
Decision ☒
Discussion/Direction □
Information □

DATE: **26 November 2024**

FROM: **Graduate Studies Committee**

SUBJECT: **New Program Proposal – Doctor of Philosophy - Cybersecurity**

COMMITTEE MANDATE:

In accordance with the Act and By-Law Number 2 the Academic Council (AC) has the delegated authority "to establish the academic standards and curricular policies and procedures of the University, and to regulate such standards, policies and procedures, including…determining the contents and curricula of all programs and courses of study" and, further, to "make recommendations to the Board on matters including…the establishment or termination of degree programs".

In accordance with the Graduate Studies Committee (GSC) Terms of Reference, GSC has the responsibility "to examine proposals for new graduate degree and diploma programs" and "to recommend their approval, as appropriate, to the Academic Council". GSC reviewed the New Program Proposal and recommends approval of the Doctor of Philosophy – Cybersecurity.

MOTION FOR CONSIDERATION:

That pursuant to the recommendation of the Graduate Studies Committee, Academic Council hereby approves the Doctor of Philosophy – Cybersecurity program and recommends approval of the program to the Board of Governors.

BACKGROUND/CONTEXT & RATIONALE:

The proposed PhD in Cybersecurity provides the highest-level degree of expertise in the broad area of Cybersecurity and will be a multidisciplinary research-intensive program that would cover a broad range of themes related to cybersecurity; including technology, policy and governance, AI and human behaviour, aiming to attract students from a variety of backgrounds and prior education, including computer science, information technology, business and management, social and political science.

The importance and emergence of the field of cybersecurity in today's world cannot be overstated, and its impact is no longer limited to technical (e.g. IT) domain. Entire infrastructures, government operations, social connections, health services, and almost every business sector rely on facilities that are potentially vulnerable to cyberattacks. Governments and businesses are increasingly looking for experts who are equipped not only with technical knowledge of the field, but also a deep understanding of its impacts on various aspects of our society. With Ontario Tech's mandate for market-driven programs and the well-established reputation of its IT security programs, it is only natural to add this program to our current portfolio.

The proposed program fits into FBIT strategic research plan themes of Digital Economy, Data Analytics and Artificial Intelligence, and Digital Technologies. This new degree will complement and build upon FBIT's portfolio of programs in information security, which includes our highly reputed bachelor of information technology in networking and IT security (NITS), established in 2005, as well as our successful Master of IT Security program, which is offered with 3 distinct fields: IT security, Artificial Intelligence, and Cybersecurity governance. The proposed program will be housed at FBIT Institute on CyberSecurity and Resilient Systems (ICRS), a multi-disciplinary global centre for cybersecurity research, innovation, teaching, and outreach.

There is a great opportunity within Ontario Tech to establish interdisciplinary research and collaboration among faculties in this program. For instance, research on global impact of cybersecurity policies could be supported by FSSH political science researchers, while applications of machine learning in cybersecurity could be explored by FBIT and FSCI computer science researchers. Cybercrime research can be supported by researchers from both FSSH and FBIT, while FBIT and FEAS experts can collaborate on infrastructure and smart city cybersecurity.

The program includes a number of components that each may be delivered differently. While some courses may be delivered using in-person, online, hybrid or asynchronous modes, it is expected that the seminar and research components will take place mostly on-campus and/or in collaboration with external organizations, industry and government agencies.

To our knowledge, this program will be the first specialized Ph.D. program in Cybersecurity in Canada, and among a handful of elite programs in this area in the world. The cross-faculty and cross-disciplinary nature of this program provides additional strength and differentiates it from cybersecurity specializations at other universities which are typically offered under Computer Science programs.

RESOURCES REQUIRED:

It is expected that most courses will be taught by core faculty members, with occasional hiring of adjunct instructors from the industry for specialized courses, if needed.

Recent TTT hires at FBIT are in line with the requirements of this program. As recommended in the external reviewers' report, it is recommended that the university prioritize hiring or appointing research chairs (NSERC CRC, Industry chairs or university research chairs) in cybersecurity, particularly in areas related to social and business aspects of cybersecurity. This is an important area of growth in the faculty and a differentiating factor that would enhance the multidisciplinary nature of the program.

The administration of the program at the faculty level will be added to the role of the Graduate Program Director and Graduate Program Assistant for Master of IT Security (MITS).

No Additional or dedicated space is required for the new program. Classes will be shared with

MITS and CS graduate programs, and research work will be conducted in supervisors' research labs.

CONSULTATION AND APPROVAL:

- ✓ Academic Resource Committee: 18 December 2023
- ✓ FBIT Faculty Council: 1 October 2024
- ✓ Graduate Studies Committee (Recommendation): 22 October 2024
- Academic Council (Approval and Recommendation): 26 November 2024
- Board of Governors (Approval): Prospective Target Date 28 November 2024

NEXT STEPS:

- Pending the approval and recommendation of Academic Council, the new program will be presented to the Board for final approval. The proposal must also proceed through the following external approval steps:
    - Ontario Universities Council on Quality Assurance
    - Ontario Ministry of Colleges and Universities

The preferred date of implementation is in the Fall of 2025

SUPPORTING REFERENCE MATERIALS:

- New Program Proposal with Appendices
- Reports from External Review

New Graduate Program Proposal

Name of proposed program (as it will appear on the student's transcript):	Doctor of Philosophy in Cybersecurity
Degree Designation/Credential (e.g. BA, BSc, BEng, etc.):	Ph.D.
Cost Recovery Program?	☐ Yes ☑No
Professional Program?	☐ Yes ☑ No
For Graduate Diplomas	☐ Type 2 ☐ Type 3
Faculty (where the program will be housed):	Faculty of Business and Information Technology
Collaborating Faculty (if applicable):	
Program Delivery Location:	North Oshawa Campus
Collaborating Institution(s) (if applicable):	
Proposed Program Start Date:	September 2025
Proposal Contact:	Michael Bliemel, Carolyn McGregor and Shahram S. Heydari
Submission Date:	
Approved by Dean: (signature and date)	

For CIQE Use Only:

Date of Academic Council Approval:	
QAF Version Used:	2021 QAF
☐External reviewers' report ☐Program's and Dean's response (with date)* ☐Summary of changes	☐Final, revised proposal ☐CVs, course outlines, and other supporting material (as appendices)

Table of Contents

1 Introduction

a) Program Abstract

Please provide a brief overview of the proposed program, to be shared with the public, in 1000 characters or less, including:

- *A clear statement of the purpose of the program*
- *Any program components, such as fields, pathways, or micro-credentials (note that fields, pathways, and microcredentials are not required)*
- *Any distinctive elements, including alternative modes of delivery (including online)*
- *Note that this statement is for external purposes; what do you want potential students/advisors to know about this program?*

The PhD in Cybersecurity program is a multidisciplinary research-intensive program that covers a broad range of themes related to cybersecurity; including technology, policy and governance, AI and human behaviour. This program aims to prepare specialized socio-technical academics who can perform leading-edge research and teaching in the academia or industry, and help governments in policymaking in the area of cybersecurity. The proposed PhD in Cybersecurity program is the first of its kind in Canada.

The objectives of the program are achieved through a combination of coursework, seminars and a research thesis. The PhD in Cybersecurity program includes graduate-level courses, a seminar course, a thesis proposal and candidacy exam, a dissertation and final defence. Potential students could come from a broad range of backgrounds including computer science, information technology, business and management, social and political science.

b) Background and Rationale

- *Identify what is being proposed, what are the program objectives, and provide an academic rationale for the proposed program*
- *Explain the appropriateness of the program name and degree nomenclature as they relate to the program objectives; list any program specializations, pathways, etc.* ***(QAF 2.1.2.1a/b)***
- *Describe the mode of delivery (in-class, hybrid, online) and how it will support students in achieving the Degree Level Expectations and learning objectives of the program* ***(QAF 2.1.2.2c)***
- *Describe the ways in which the program fits into the broader array of program offerings within the Faculty and the University*
- *Describe any unique curriculum or program innovations, creative components, or significant high impact practice*

The proposed PhD in Cybersecurity provides the highest-level degree of expertise in the broad area of Cybersecurity and will be a multidisciplinary research-intensive program that would cover a broad range of themes related to cybersecurity; including technology, policy and governance, AI and human behaviour, aiming to attract students from a variety of backgrounds and prior education, including computer science, information technology, business and management, social and political science.

The importance and emergence of the field of cybersecurity in today's world cannot be overstated, and its impact is no longer limited to technical (e.g. IT) domain. Entire infrastructures, government operations, social connections, health services, and almost every business sector rely on facilities that are potentially vulnerable to cyberattacks. Governments and businesses are increasingly looking for experts who are equipped not only with technical knowledge of the field, but also a deep understanding of its impacts on various aspects of our society. With Ontario Tech's mandate for market-driven programs and the well-established reputation of its IT security programs, it is only natural to add this program to our current portfolio.

The proposed program fits into FBIT strategic research plan themes of Digital Economy, Data Analytics and Artificial Intelligence, and Digital Technologies. This new degree will complement and build upon FBIT's portfolio of programs in information security, which includes our highly reputed bachelor of information technology in networking and IT security (NITS), established in 2005, as well as our successful Master of IT Security program, which is offered with 3 distinct fields: IT security, Artificial Intelligence, and Cybersecurity governance. The proposed program will be housed at FBIT Institute on CyberSecurity and Resilient Systems (ICRS), a multi-disciplinary global centre for cybersecurity research, innovation, teaching, and outreach.

There is a great opportunity within Ontario Tech to establish interdisciplinary research and collaboration among faculties in this program. For instance, research on global impact of cybersecurity policies could be supported by FSSH political science researchers, while applications of machine learning in cybersecurity could be explored by FBIT and FSCI computer science researchers. Cybercrime research can be supported by researchers from both FSSH and FBIT, while FBIT and FEAS experts can collaborate on infrastructure and smart city cybersecurity.

The program includes a number of components that each may be delivered differently. While some courses may be delivered using in-person, online, hybrid or asynchronous modes, it is expected that the seminar and research components will take place mostly on-campus and/or in collaboration with external organizations, industry and government agencies.

To our knowledge, this program will be the first specialized Ph.D. program in Cybersecurity in Canada, and among a handful of elite programs in this area in the world. The cross-faculty and cross-disciplinary nature of this program provides additional strength and differentiates it from cybersecurity specializations at other universities which are typically offered under Computer Science programs.

c) Consistency of Program Objectives with University Mission, Vision, Integrated Academic and Research Plan, and Strategic Mandate Agreement (QAF 2.1.2.1c)

- *Describe how the program contributes to the University's Mission and Vision*
- *Explain how the program aligns with the goals and priorities outlined in the Faculty's(ies') and University's Integrated Plan. Identify how the program fits within one or more areas of strength or growth in Ontario Tech University's Strategic Mandate Agreement*

The proposed program is an embodiment of the university's main priority, "Tech with a conscience", to advance scientific and technical knowledge in a domain that affects not just the daily lives of people but also of the well-being of the world.

Through its affiliation with the Institute for Cybersecurity and Resilience Systems (ICRS), the proposed program will achieve the university's strategic priority of "partnership" by connecting researchers across different faculties with industry partners, government organizations and other research institutes outside the university.

The proposed program also aligns with the university's core values, in particular, intellectual resilience and innovation, through developing research expertise, intellectual properties and innovations in the emerging field of cybersecurity. The proposed program builds upon the successful Master of IT Security program at FBIT, which has been one of the fastest growing graduate programs at Ontario Tech University.

The PhD program in Cybersecurity fits into several areas of strengths/growth that were identified in the university's strategic mandate. In particular, it builds upon and grows our strength in digital technologies and artificial intelligence; and due to the multidisciplinary nature of cybersecurity, it also has the potential to expand our strength in crime, justice and forensic science, automotive and transportation systems; and community wellness. The proposed program is also relevant to the university's strategic research priority area of disruptive technology and new economy, as cybersecurity continues to become an increasingly important factor in most social, business and public decision-making processes.

d) Student Demand

- *Provide evidence of student demand, including number of prospective student inquiries; applications and registrations for similar programs; results from surveys/focus groups of existing students, graduates, or professionals in the field*
- *Include information about domestic vs. international student interest*

Considering the rising interest in Cybersecurity programs at universities worldwide and the need for specialist academics to teach and conduct research in the field, we expect the number of applicants to be quite sufficient for our target student numbers. As confirmed by the University Registrar and AVP International, the university's international agent network has confirmed significant demand for cybersecurity among international students, pointing out that our Master of IT Security (MITS) has had as many as 800 applicants for 50-100 spots each year and this alone could likely stimulate a PhD program.

Enrolment Information

- *Please complete Table 1 and provide, in paragraph form, information regarding enrolment projections*
- *Please determine the academic year when the program enrollment will reach a steady-state and add an asterisk (*) in the corresponding box beside the number*

The following numbers indicate the anticipated enrollments per year, based on the typical number of applications to other PhD programs at Ontario Tech, and the number of faculty members who will accept students under this program. It is expected that the program will reach stability in year 5 (2029-2030) for a total number of 20 students.

Table 1: Projected Enrollment by Academic and Program Year

	Academic Year					
	2025-2026	2026-2027	2027-2028	2028-2029	2029-2030	2030-2031
Level of Study						
Ph.D. year 1	4	5	5	5	5	5
Ph.D. year 2		4	5	5	5	5
Ph.D. year 3			4	5	5	5
Ph.D. year 4				4	5	5
Total Enrolment	4	9	14	19	20*	20*

e) Societal Need

- *Evidence of the need for graduates of the program and in which fields (within academic, public, and/or private sectors)*
- *Please indicate up to three occupations in which graduates from this proposed program may be employed using the Ontario Job Futures website; you may also wish to review the Durham Workforce Authority website and provide any relevant sector portfolio or local/community impact information*
- *For professional programs, a description of the program's congruence with current regulatory requirements*
- *Mention if any employers in the area support the need for this program and include a letter(s) of support as an additional appendix*

The number of cybersecurity job openings across the globe is expected to grow to 3.5 million unfilled positions through 2025 (Cybercrime magazine, Nov. 9, 2021). The Canadian federal government has stated that "due to a shortage of cyber security talent in Canada and worldwide, cyber security professionals are needed across government." and "Nearly all Canadian federal government departments have a need for cyber security professionals." Currently roughly 20% of the 130+ postings on the Association of Information Systems job portal are looking for Cybersecurity assistant professors across the English-speaking countries where most are in business schools. This market is relatively new as cybersecurity from a management and technical perspective gains importance globally as a consequence of the digital economy that has accelerated from the pandemic driven digital transformation in all industries.

Given the growing reliance of the society on cyberspace in almost all aspects of life, the need for cybersecurity professionals and services is projected to increase significantly. Consequently, we expect a growing need for highly-skilled experts who could contribute to training, research, policymaking, and consultation in cybersecurity for businesses and governments. Graduates of the proposed program may be employed as university and college professors, industry researchers, government researchers and specialists, policymakers and business consultants.

f) Duplication

- *Describe how the program is distinct from other programs at Ontario Tech. Is it reasonable to anticipate this program might affect enrolment in other related programs? If so, how might this be addressed?*

The PhD program in cybersecurity will provide a venue for aspiring students in MITS (graduate), NITS (undergraduate) as well as graduates of Computer science (CS) and social science programs who want to specialize in the field of cybersecurity. Given that several FBIT faculty members participating in this program are also members of the CS graduate program, some CS grad applicants may choose this specialized Ph.D. program in

Cybersecurity over the general CS graduate program. However, we don’t expect these programs to compete with each other. Both programs are hosted or co-hosted by FBIT. These programs are intended to complement each other for broader attractions of research-focused graduate students to the university. The Ph.D. program in cybersecurity focuses on applications of information Technology, and has a significantly broader scope as it covers policy, governance, privacy and IT management issues that are not covered under the Computer Science program.

- *Identify similar or complementary programs offered elsewhere in Ontario in Table 2. Please be brief but specific in the table. Avoid value-based statements*

Table 2: List of Similar Programs in Ontario

<table>
<tr><th>Institution Name</th><th>Credential Level and Program Name</th></tr>
<tr><td>Queen’s University</td><td>PhD, School of Computing</td></tr>
<tr><td colspan="2"><b>Link to Program Web Page:</b> https://cyber.cs.queensu.ca/program/</td></tr>
<tr><td colspan="2"><b>Brief Program Description:</b>
The school of computing at Queen’s University offers a PhD program in Computing Science in which students can also specialize in Cybersecurity. The program was originally supported by a 2019 NSERC CREATE grant. This is the only PhD program in Ontario currently listed under Government of Canada’s Post-secondary cyber security related programs guide.</td></tr>
<tr><td colspan="2"><b>What differentiates the new program from this existing program:</b>
Queen’s program is a standard computing science PhD by research, with only a condition that students must take two courses in Cybersecurity. The proposed program at Ontario Tech focuses entirely on Cybersecurity (including all coursework), and does it from a multidisciplinary view, allowing non-CS students also to specialize in social, political and governmental aspects of cybersecurity. Such level of breadth does not exist in Queen’s university program.</td></tr>
<tr><td><b>Institution Name</b></td><td><b>Credential Level and Program Name</b></td></tr>
<tr><td>Carleton University</td><td>PhD, School of Information Technology</td></tr>
<tr><td colspan="2"><b>Link to Program Web Page:</b> https://www.csit.carleton.ca/index.php?pageID=GradPHD</td></tr>
<tr><td colspan="2"><b>Brief Program Description:</b>
Carleton’s School of Information technology (CSIT) offers a PhD program in Information Technology with a focus on applications of IT in various fields, including network security. This is one of the few PhD programs in IT (and distinguished from similar programs in Computer Science) in Canada.</td></tr>
</table>

What differentiates the new program from this existing program:
While students in Carleton's PhD in IT program may be able to conduct their research in the area of IT security, the proposed Ontario Tech program provides a broader multidisciplinary focus on cybersecurity. The coursework of our proposed program also covers various aspects of cybersecurity, which gives the graduates both deeper and broader knowledge in this field.

- *Provide additional overall comment on the justification for this duplication*

No similar PhD program with a focus and breadth in the field of cybersecurity currently exists in Ontario, which justifies the launching of this new program at Ontario Tech.

2 Program Requirements

a) Admission Requirements (QAF 2.1.2.5)

- *Outline the formal admission requirements; explain how these are appropriate for the program objectives and program learning outcomes: How will they help to ensure students are successful? How do they align with the learning outcomes of the program? (*
- *Explain any additional requirements for admission to the program such as minimum grade point average, special language, portfolio, etc. (and how the program recognizes prior work or learning experience, if applicable) (*
- *Indicate the programs from which students may be drawn*

In addition to the general admission requirements for graduate studies, PhD in Cybersecurity applicants must meet the following program-specific requirements.

- Students would normally be expected to have completed a four-year undergraduate degree and a thesis-based Masters degree in a relevant field from a Canadian university, or its equivalent from a recognized institution, with an overall academic standing of at least 3.5 on a 4.0/4.3 scale or its equivalent in their last two years of study.

MITS Pathway: Graduates of Ontario Tech University Master of IT Security (MITS) program can apply to the Ph.D. program If they have completed the MITS program with an overall academic standing of at least 3.5/4.3.

- A minimum of two letters of reference from persons having direct knowledge of the applicant's academic competence. Academic references are preferred; however professional references will be accepted. Letters of reference should come from individuals under whom the applicant has worked closely or studied. The quality of the letters will be assessed by the Graduate Committee to make sure relevant requirements have been met.

- Proof of English proficiency is needed from those applicants whose first language is not English, as per university regulations.

- Applicants must find a prospective faculty supervisor from among the list of graduate faculty members of the PhD in Cybersecurity program and receive formal acceptance of the faculty member to supervise their research. No applicant will be accepted to the program without having an approved prospective supervisor in advance.

- As part of the application form, students are required to provide a minimum 3000-word long personal research statement, outlining their area of interest in cybersecurity, their proposed academic research plan, and identify the faculty supervisor who has agreed to supervise their research.

- Students admitted to the program must demonstrate their broad proficiency in the area of cybersecurity through evidence of completing or having completed graduate-level coursework in the fields of theory, applications, legal and governance issues of cybersecurity. Students who do not demonstrate appropriate background in research methods and cybersecurity fundamentals and/or ethics will be required to complete the following additional/prerequisite courses within the first 18 months of the program:

  1. Cybersecurity: The following courses are required for students who do not have prior background in IT security.

     - INFR 5010G - Fundamentals of IT security (6 Credits)
     - MITS 5100G - Law and Ethics of IT Security (3 Credits)

  2. Research methods: The following prerequisite is required for students who have not completed a previous thesis-based Master's program in a relevant field.

     - CSCI 5010G – Survey of Computer Science Research Topics and Methods (3 Credits)

Note: Students who demonstrate sufficient proficiency through prior graduate-level coursework or extensive related work experience, can request a waiver for the corresponding prerequisite course from the Graduate Program Director. Waiver requests are not guaranteed and will be considered on a case-by-case basis.

b) Program Learning Outcomes and Assessment of Student Knowledge (QAF 2.1.2.2 a/b/d, 2.1.2.3, 2.1.2.4)

- ***Connect with CIQE (ciqe@ontariotechu.ca) early in the program development to participate in learning outcome development sessions or arrange for assistance and review prior to the scheduling of the external site visit***
- *In Table 3 below, please describe what the student will know or be able to do (knowledge, methodologies, and skills) by the end of the program and indicate how that knowledge or skill will be demonstrated*
- *An example has been provided in purple in the first row and should be removed.*

Degree Level Expectations are set by the Quality Council of Ontario and should not be modified. For the list of and more information on these expectations, including a detailed description, visit their website.

Table 3: Program Learning Outcomes

Program Learning Outcomes By the end of the program, students graduating will be able to… (normally 6-8 outcomes per program with 12 being the maximum)	Degree Level Expectations (list all that apply; you must align with each expectation at least once)	Relevant courses (provide course code and course title)	Assessment of Learning Outcomes (e.g. test, rubric, self-assessment, etc.)
Demonstrate a thorough understanding and detailed knowledge of the state of the art in threats and attacks against computing systems, cyber-physical systems and social networks	• Depth & Breadth of Knowledge • Research & Scholarship	INFR6040G INFR6110G INFR7100G INFR7200G	Course Exam, Candidacy Defence, Thesis Defence
Analyze, plan and apply various techniques for vulnerability assessment, protection, detection, mitigation and response to cyberattacks	• Research & Scholarship • Application of Knowledge • Awareness of limits of Knowledge • Autonomy and Professional Capacity	INFR6020G INFR6040G INFR7100G INFR7200G	Course Exam, Candidacy Defence, Thesis Defence
Develop and evaluate information security and risk management practices, policies, and procedures that comply with the current standards, federal, provincial and international laws, agreements and policies on issues related to	• Application of Knowledge • Awareness of limits of Knowledge • Autonomy and Professional Capacity	MITS5600G INFR6040G INFR6110G INFR6120G INFR6130G	Course Exam

cybersecurity, ethical hacking and data privacy.			
Demonstrate a thorough understanding and detailed knowledge of the economic, social and business drivers of cybersecurity and related technologies	• Depth & Breadth of Knowledge • Research & Scholarship • Application of Knowledge	INFR6020G INFR6120G INFR6130G MITS6900G	Course Exam
Demonstrate a thorough understanding and detailed knowledge of the state of the art in applications of Artificial Intelligence to cybersecurity, attack detection and mitigation.	• Depth & Breadth of Knowledge • Research & Scholarship • Application of Knowledge	INFR6010G INFR7100G INFR7200G	Course Exam, Candidacy Defence, Thesis Defence
Evaluate, analyze and criticize limitations of cybersecurity and Artificial Intelligence tools in terms of privacy protection, algorithmic and data biases, sociopolitical impact and other potential problems	• Awareness of limits of Knowledge • Autonomy and Professional Capacity	INFR6010G INFR6020G INFR6030G	Course Exam
Communicate effectively and accurately to the public and in professional circles about various aspects of cybersecurity	• Communication Skills	INFR6120G INFR7000G INFR7100G INFR7200G	Seminar Evaluations, Candidacy Defence, Thesis Defence

- *Selecting a few examples from above, and with assistance from CIQE (cige@ontariotechu.ca), please provide further details on:*
    - *Appropriateness of the program's structure and the requirements to meet its objectives and program learning outcomes; Guidance on program objectives and program-level learning outcomes, including examples, is available here*
    - *Appropriateness of the proposed methods for the assessment of student achievement of the intended program learning outcomes and Degree Level Expectations (How will students demonstrate they have learned and can do what we expect them to by the end of the program?); and*
    - *Completeness and appropriateness of plans for monitoring and assessing:*
        - *The overall quality of the program*
        - *Whether the program is achieving in practice its proposed objectives;*

- *Whether the students are achieving the program learning outcomes; and*
- *How the resulting information will be documented and subsequently used to inform continuous program improvement*

Please see Guidance on Assessment of Teaching and Learning for advice on how to satisfy these criteria.

The following includes examples that illustrate the connections between learning outcomes, program elements and structure, and assessment methods. We also describe our plan for monitoring and assessing program quality, objectives and learning outcomes.

Program Learning Outcome: Demonstrate a thorough understanding and detailed knowledge of the state of the art in threats and attacks against computing systems, cyber-physical systems and social networks.

The PhD in Cybersecurity program provides a comprehensive theoretical understanding of the state-of-the art in information security through a foundation course in cybersecurity, INFR5010G. This course is designed particularly for those who enter the program without a deep theoretical knowledge of the field, and includes learning modules in cryptography, principles of network security, system vulnerabilities, malware, and a review of hacker tools and methods. The learning outcomes of this course will be assessed through individual module tests. The students will further enhance their knowledge of the field through developing a PhD research proposal which must be evaluated and defended in front of a committee of examiners, and subsequently write and defend their PhD thesis, which must include sufficient review of state-of-the art and elements of novel contributions to the field.

Program Learning Outcome: Analyze, plan and apply various techniques for vulnerability assessment, protection, detection, mitigation and response to cyberattacks

The PhD in Cybersecurity program provides a thorough understanding of the state-of-the art in cybersecurity defense through a foundation course in cybersecurity, INFR5010G. This course is designed particularly for those who enter the program without a applied knowledge of the field, and includes learning modules in design principles for secure systems, trusted computing base, security models, authentication, authorization and accounting (AAA), identity and access control, logging and auditing, intrusion detection, and information security management. The learning outcomes of this course will be assessed through individual module tests. The students will further enhance their knowledge of the field through developing a PhD research proposal which must be evaluated and defended in front of a committee of examiners, and subsequently write and defend their PhD thesis, which must include sufficient review of state-of-the art and elements of novel contributions to the field.

Program Learning Outcome: Develop and evaluate information security and risk management practices, policies, and procedures that comply with the current standards, federal, provincial and international laws, agreements and policies on issues related to cybersecurity, ethical hacking and data privacy.

The PhD in Cybersecurity program includes two courses that contribute toward this outcome. The INFR5100G – Law and Ethics of IT Security is a prerequisite program course which provides an overview of the laws and professional ethics that information security professionals must understand and apply. This course includes reviews of the current laws on e-contracts, regulations, online crime, intellectual property, privacy and data breach liability. Students will be assessed through research assignments to demonstrate their knowledge of the laws and standards. The INFR5600G – security policies and risk management, is a multidisciplinary course where students will learn about how to develop strong security policies and procedures, conduct risk management and identify vulnerabilities in security policies. The course includes lecture classes and lab exercises, and students will be assessed through quizzes and presentations.

Program Learning Outcome: Demonstrate a thorough understanding and detailed knowledge of the state of the art in applications of Artificial Intelligence to cybersecurity, attack detection and mitigation.

The PhD in Cybersecurity Program offers a course in AI in Cybersecurity – INFR6010G, along with a number of elective courses in this field from the MITS program. This course empowers students with knowledge about how AI can be used by attackers as well as in defence systems, and techniques to mitigate such attacks using machine learning programming. The learning outcomes of this course is assessed through assignments and projects. The students will have further opportunities to enhance their knowledge in this area through developing a relevant PhD research proposal which must be evaluated and defended in front of a committee of examiners, and subsequently write and defend their PhD thesis, which must include sufficient review of state-of-the art and elements of novel contributions to the field.

Program Learning Outcome: Evaluate, analyze and criticize limitations of cybersecurity and Artificial Intelligence tools in terms of privacy protection, algorithmic and data biases, sociopolitical impact and other potential problems

The PhD in Cybersecurity program addresses this important learning outcome in a number of courses that focus on potential issues arising from cybersecurity. The IT Security Law and Ethics – INFR5100G course discusses the issue of privacy from legal and technical standpoints. The AI in Cybersecurity – INFR6010G course includes discussions of algorithmic bias in AI. The Information Trust – INFR6030G course includes discussions of trust in computing and data, and how cybersecurity techniques and policies should be built around this issue. All courses provide assessment of the learning outcomes through student assignments, presentations and course projects.

Program Learning Outcome: Communicate effectively and accurately to the public and in professional circles about various aspects of cybersecurity

The PhD in Cybersecurity program includes several elements to prepare students for effective communication of cybersecurity ideas and solutions. Students are required to register in and participate in a zero-credit seminar course every semester. Each student must present at least two seminars throughout their program: one seminar before the candidacy exam, and one exit seminar before their thesis defence. Additionally, each student must present and defend their research proposal in an open session for an examining committee and public audience, and do the same for defending their thesis. Many of program courses also include student presentations as part of the assessment.

In general, learning outcomes overall are assessed on an ongoing basis by each student's supervisory committee. Student progress reports are submitted each term by the committee to the Graduate Program Director and School of Graduate and Postdoctoral Studies (SGPS) for assessment.

- *Describe the requirements and structure of the program. Is it full-time/part-time? Is this an online or partially online/hybrid program? What are the unique curriculum or program innovations or creative components in this program?*
- *Address how the program's structure, requirements, and program-level learning outcomes are appropriate in meeting the Degree Level Expectations.*

    - *Please attach, as an Appendix, the Program Learning Outcome Alignment Map to Degree Level Expectations*
    - *If the program is to be accredited, include with the above information about the accreditation requirements and add the accreditation tables, if available, as an Appendix.*

- *Provide evidence that each graduate student is required to take a minimum of two-thirds of the course requirements from among graduate-level courses*
- *What is the program length? Provide a rationale for the length that ensures the program learning outcomes and requirements can be reasonably completed*

The Ph.D. program in Cybersecurity is a full-time and includes graduate-level courses, a seminar course, a thesis proposal and candidacy exam, a dissertation and final defence. All coursework is at graduate level.

The course requirements of the program may include a variety of delivery options, including in-person, online or hybrid, depending on the course. The research portion of the program is normally conducted on campus and/or in a research facility.

The Ph.D. program in Cybersecurity is unique in Canada in terms of the scope, breadth and area of focus. It is a multidisciplinary research-intensive program that covers a broad range of themes related to cybersecurity; including technology, policy and governance, AI and human behaviour. No program with such scope currently exists in Canada. Cybersecurity research in other universities is either provided under computer science programs and limited to technical issues, or under political science and governance programs and limited to policy issues. There is a lack of a multidisciplinary program whose graduates are provide opportunities to gain a reasonable grasp of both angles, and the proposed program aims to fill this gap. Additionally, this program will provide a unique opportunity to graduates of Computer Science programs to gain expertise in policy and governance issues of cybersecurity, and to graduates of social policy and governance programs to learn about technical aspects of cybersecurity.

The program follows a traditional model for doctoral studies in North America. Similar to other doctoral programs at Ontario Tech university, students should be able to complete all requirements within four years of full-time study. Students are expected to complete course requirements and pass the candidacy exams within 18-24 months after starting the program, and complete and defend their research thesis within 48 months after starting the program.

Only graduate-level courses are accepted for fulfilling the requirements of this program. That includes both mandatory and elective courses.

- *Describe the ways in which the curriculum addresses the current state of the discipline (QAF 2.1.4a)*
- *For researched-focused graduate programs, provide a clear indication of the nature and suitability of the major research requirements for degree completion*

The proposed curriculum includes common elements of most other PhD by research program at Ontario Tech as well as other Ontario Universities. Those include coursework to prepare students for development of a research proposal; a candidacy exam where faculty experts examine the proposal and provide guidelines and critique to the student with regards to the nature and suitability of the research proposal; and a final thesis defence in front of internal and external arm-length experts to evaluate the quality of research work. Students are supported throughout this process by continuous guidance and feedback from their supervisors as well as regular meeting with their supervisory committee. Regular progress reports will be submitted every semester to SGPS.

- *Is there an experiential learning component (e.g. workplace learning, co-op, internship, field placements, service learning, mandatory professional practice) to the program? If yes, please describe this component in 2500 words or less. Include confirmed partners, duration of the experiential learning component(s), and projected number of placements (where applicable)*

Select students may have the opportunity to work on applied industry sponsored research through the Institute for Cybersecurity and Resilient Systems as part of their dissertation.

- *Describe how the principles of Equity, Diversity, Inclusion, and Decolonization have been considered:*
  - *Does the program contain concepts, materials, or resources from scholars/professionals who are part of one or more historically marginalized groups?*
  - *Are multiple perspectives represented in the program, such as those offered by those who are Indigenous, Black, Persons of Colour, and/or 2SLGBTQIA+?*
  - *How has accessibility been considered? More specifically, have the needs of students with disabilities been integrated into the program design (e.g., the ways that students are asked to demonstrate their learning)?*
  - *Will this program provide space to allow for the discussion of other viewpoints outside the "dominant, Western narrative"?*
  - *Have the principles of Universal Design been considered?*
- *Describe how the potential need to provide accessibility accommodations has been considered in the development of this program; please provide information beyond the services offered by Student Accessibility Services*

The Faculty of Business and IT (FBIT) is among the most diverse and inclusive faculties at Ontario Tech university in terms of racial, religious and gender diversity in faculty members and students. It is expected that the new PhD program in cybersecurity will also follow those standards. In particular, this program will help diversify the extreme gender imbalance in CyberSecurity by looking to recruit from our diverse pool of Master of IT Security students. Training and mentorship of the next generation of female and minority researchers and educators in the field of cybersecurity would also create a pool of role models for historically marginalized groups in this field.

The program also includes areas of research related to marginalized and indigenous communities where such students will have many opportunities to apply their learning back into their own communities through already established research projects and partnerships with communities and organizations. Examples include: cybersecurity policies and their impact on marginalized communities; algorithmic and data biases in cybersecurity; inclusion of marginalized communities and their well-being in cybersecurity decision-making process; and global cybersecurity issues. As part of this proposal, a special scholarship is proposed for indigenous students who intend to complete the Ph.D. program in cybersecurity.

EDI metrics will be evaluated during regular program reviews.

Similar to other graduate programs at Ontario Tech University, this program will also follow the Procedures for Academic Accommodation for Students with Disabilities https://usgc.ontariotechu.ca/policy/policy-library/policies/legal,-compliance-and-governance/procedures-for-academic-accommodation-for-students-with-disabilities.php

c) Calendar Copy with Program Map(s)

- *Provide, as an Appendix using the template provided, a clear and full calendar copy. The template ensures consistency across all programs in the Academic Calendar*
- *Provide, as an Appendix, a full list of the all courses included in the program including course numbers, titles, and descriptions. Please indicate clearly whether they are new/existing. Include full course proposals for new courses, and the most recent course syllabi for existing courses. If you are making changes to existing courses, include instead a course change form. In an appendix noted below, you will note which faculty members are expected to teach in the program and who is responsible for developing any new courses.*

Please see Appendix for proposed calendar copy and a full list of courses in the program.

3 Consultation

- *Describe the expected impact of the new program on the nature and quality of other programs delivered by the home and collaborating Faculty(ies) and any expected impact on programs offered by other Faculties*
- *Outline the process of consultation with the Deans of Faculties that will be implicated or affected by the creation of the proposed program*
- *Provide letters of support for the program from Deans at Ontario Tech and/or from other institutions/partners*
- *Describe any consultation undertaken with regard to the principles of Equity, Diversity, Inclusion, and Decolonization*

The Ph.D. program in cybersecurity would create a new interdisciplinary venue for collaboration between Faculty of Business and IT (FBIT) and Faculty of Social Science and Humanities (FSSH), with additional areas of potential collaborations with Faculty of

Science (FSCI) and Faculty of Engineering and Applied Science (FEAS) too. It is expected that some members from the aforementioned faculties would join this graduate program as associate or full members.

The program has currently been discussed and received support and feedback at FBIT at the current levels:

- Dean
- Academic Resource Committee approval of NOI and feedback (Feb 23, 2023)
- Faculty Council – information and feedback (June 20, 2023)
- Individual feedback from the networking and IT Security area (May-July 2023)
- FBIT Graduate Education Committee Approval (Nov 15, 2023)

Consultation with SGPS – Sep 6, 2023, October 25, 2023
Consultation with FSCI and FEAS faculty members – Sep 13, 2023
Request for comments from IEAC – Nov 10, 2023
Consultation with CIQE and TLC– Nov 10, 2023
External Review (site visit) – June 25/26, 2024
FBIT Faculty Council Approval – Oct 1, 2024
GSC Approval - Oct 22, 2024

Does this Program contain any Indigenous content? □ Yes ☒ No □ Unsure

For more information on how Indigenous content is defined at Ontario Tech University and how to consult with the Indigenous Education Advisory Circle (IEAC), please refer to the Protocol for Consultation with the Indigenous Education Advisory Circle.

Has the IEAC been contacted □ Yes ☒ No

If yes, when?

What was the advice you received from the IEAC, and how has it been included in your proposal?

Did the IEAC ask you to return the proposal to them for review? ☐ Yes ☒ No

If yes, have they completed their review? ☐ Yes ☐ No ☒ N/A

4 Resource Requirements (QAF 2.1.2.6, 2.1.2.7, 2.1.2.8 a)

a) General Resource Considerations

- *Note here if this new program may impact enrolment agreements with other institutions/external partners that exist with the Faculty/Provost's office*
- *Indicate if the new program will require changes to any existing agreements with other institutions, or will require the creation of a new agreement. Please consult with CIQE (cige@ontariotechu.ca) regarding any implications to existing or new agreements.*

There are no impacts on enrollment agreements or agreements with other institutions.

b) Faculty Members - Current and New Faculty Requirements

- *Complete as an Appendix, using the Faculty Information templates provided, charts chart detailing the list of faculty committed to the program and provide any additional details, in paragraph form below; the information in the Appendix or additional information must include clear evidence that faculty have the recent research or professional/clinical expertise needed to sustain the program, promote innovation, and foster an appropriate intellectual climate. This should also demonstrate how supervisory loads are distributed in light of qualifications and appointment status; if necessary, include this information below*
- *Include a brief statement to provide evidence of the participation of a sufficient number and quality of faculty who will actively participate in the delivery of the program and achieve the goals of the program and foster the appropriate academic environment, contribute substantively to the program, and commit to student mentoring*
- *Describe the role of any sessional/part-time faculty; provide an approximate percentage used in the delivery of the program and the plans to ensure the sustainability of the program and quality of the student experience*
- *Explain the provision of supervision of any experiential learning opportunities; how will supervisory loads be distributed?*
- ***If new faculty resources are needed, describe the plan and commitment to provide these resources to support the program and the rationale in section 4h)***

Recent TTT hires at FBIT are in line with the requirements of this program. As recommended in the external reviewers report, it is recommended that the university prioritize hiring or appointing research chairs (NSERC CRC, Industry chairs or university research chairs) in cybersecurity, particularly in areas related to social and business aspects of cybersecurity. This is an important area of growth in the faculty and a differentiating factor that would enhance the multidisciplinary nature of the program.

c) Additional academic and non-academic human resources

- *Give details regarding the nature and level of Sessional Instructor and TA support required by the program, the level of administrative and academic advising support, etc.*
- ***If new resources are needed, describe the plan and commitment to provide these resources to support the program and the rationale in section 4h)***

We expect that most courses will be taught by core faculty members, with occasional hiring of adjunct instructors from the industry for specialized courses, if needed.
The administration of the program at the faculty level will be added to the role of the Graduate Program Director and Graduate Program Assistant for Master of IT Security (MITS).

d) Supporting information for online and hybrid programs

- *Describe the adequacy of the technological platform to be used for online delivery*
- *Describe how the quality of education will be maintained*
- *Describe how the program objectives will be met*
- *Describe how the program learning outcomes will be met*
- *Describe the support services and training for teaching staff that will be made available*
- *Describe the sufficiency and type of supports that will be available to students*
  - *How has accessibility been considered?*
  - *What strategies have been considered to accommodate students with disabilities?*
  - *Have the principles of Universal Design been considered?*
  - *Will course content be offered in both written and audible forms (e.g., closed captioning, transcriptions)?*
  - *Is course content designed logically and is it easy to follow with limited instruction?*
  - *Are assignment expectations clear (i.e., a rubric)?*

- *Have the needs of students with limited or unreliable access to wi-fi been considered (e.g., breaking down pre-recorded lectures into maximum 10-minute videos)?*

Not Applicable.

e) Existing non-financial student supports

School of Graduate and Post-Doctoral Studies

Quality graduate and postdoctoral education combines teaching, research, professional development, disciplinary community involvement and personal growth. It is by nature a shared responsibility between students, faculty members, the programs and a large number of support units, with overarching administration being provided by the School of Graduate and Postdoctoral Studies.

The School of Graduate and Postdoctoral Studies (SGPS) at Ontario Tech University is the main point of contact for our postgraduates, facilitating support and offering guidance for our growing graduate community of students, postdoctoral fellows and graduate faculty members. The SGPS Graduate Academic Affairs Specialist works to identify and provide advice to solutions for graduate students based on graduate policies, resources and working with faculty partners. The SGPS assists students in areas such as: student-supervisor relationships; personal or academic barriers to progression; research progression; and navigating academic regulations. The SGPS works closely with campus partners to refer students to other helpful resources and supports across our campus community.

The SGPS Graduate Engagement Team coordinates a range of programs such as Graduate Pro Skills and the Three Minute Thesis. SGPS' most recent initiative, Base Camp, represents foundational programming that provides our graduate students and postdoctoral fellows with specific skills necessary to succeed as global citizens in the workplace and beyond. Centered around four pillars: Achieve, Empower, Ascend, Inspire, Base Camp builds on the aptitudes and lived experiences of our graduate students and postdoctoral fellows, propelling them forward to new heights. The SGPS team supports prospective, new and returning graduate students from the start of their journey beginning with recruitment and admissions, through registration, funding and scholarships, to then join us at orientation, professional development workshops and a range of events, ultimately supporting our graduates through to successful degree conferral.

Faculty-Specific Support

Academic Advising

Graduate students will receive academic advice and support at FBIT through the office of Graduate program Director (GPD). A dedicated graduate program assistant provides support for all graduate programs at FBIT.

Student Life

Ontario Tech University, as a relatively small campus community, has a centralized delivery model for many student supports. All undergraduate students have access to an extensive support system that ensures a quality student experience. Each Faculty may provide additional, Faculty- or program-specific supports. In addition to the outlined services below, students may also take advantage of the Campus Bookstore, Housing and Living Resources as well as the Ontario Tech Student Union. Further information can be found at: http://studentlife.ontariotechu.ca/.

Student Learning Centre

Ontario Tech University fosters a high level of academic excellence by working with students, undergraduate and graduate, to achieve educational success. Faculty specific academic resources are available online and include tip sheets and videos. Academic specialists offer one-on-one support services in mathematics, writing, study skills, ESL and physics. With the additional support of peer tutors and workshops, the Student Learning Centre can also accommodate the needs of a specific course or program.

Student Accessibility Services

Ontario Tech University ensures that students with disabilities have equal opportunities for academic success. Student Accessibility Services operates under the Ontario Human Rights Code and the Accessibility for Ontarians with Disabilities Act. Services and accommodation support are provided for students with documented disabilities and include:

- Adaptive technology training
- Alternate format course material
- Learning skills support
- Testing support
- Transition support for incoming students

Student Accessibility Services also provides inclusive peer spaces, support groups, and skills workshops for students.

Career Readiness

Ontario Tech University offers comprehensive career service assistance, co-op and internship support and a variety of valuable resources to help students along their career paths, including:

- Assistance with creating effective job-search documents

- Career counselling
- Co-op and internships
- Interview preparation
- Job market information
- Job search strategies

The Career Centre hosts a variety of events during the academic year including employer information and networking sessions, job fairs and interviews conducted by leading employers.

Student Engagement, Equity and Inclusion, and ***Indigenous Education and Cultural Services***

The university supports students' successful transition and provides opportunities to develop leadership and professional skills throughout their university career. Services provided include:

- Equity and inclusivity programming and support groups
- Indigenous Education and Cultural Services provides space and supports for students to connect with Indigenous culture and resources
- Opportunities to grow and develop leadership skills through the Ambassador and Peer Mentorship program
- Orientation and events through first year
- Peer mentoring
- Services and supports for international and exchange students
- Specialized programming for first-generation, graduate, Indigenous, international, mature, online, transfer and diploma-to-degree pathways students

Student Mental Health Services

Student Mental Health Services helps students learn how to better manage the pressures of student life. Students can:

- Access short term counselling and therapy services
- Access tools and resources online to learn about mental health and how to maintain good health and wellness
- Attend drop-in sessions
- Participate in events, activities or support groups that promote positive health and well-being
- Work with a mental health professional to address concerns

Students in distress will also be provided with support and counselling as needed. There is no cost to students and services are confidential. For those who need long-term counselling support or specialized mental health services, Ontario Tech

University will provide referrals to assist the student in accessing resources in the local community or in the student's home community.

Athletics and Recreation Facilities

Ontario Tech University offers a number of recreation facilities and fitness opportunities to meet all lifestyles and needs. On-campus facilities include the state-of-the-art FLEX Fitness Centre which overlooks Oshawa Creek, five gymnasiums, a 200-metre indoor track, two aerobic/dance studios, the Campus Ice Centre, Campus Fieldhouse, a soccer pitch, a fastball diamond, squash courts and an indoor golf training centre. Students are able to participate in varsity and intramural sports as well as group fitness classes and personal training sessions.

Campus Health Centre

The Campus Health Centre provides assistance in numerous confidential health-care options including:

- A medical clinic with daily access to physician and nursing staff
- Treatment of disease, illness, and injury
- Allergy injections, immunizations, and influenza injections
- Complementary Health Services featuring acupuncture, chiropractic, custom orthotics, massage therapy, nutritional counselling, and physical therapy
- An on-site laboratory (blood work, STI testing, throat swabs, etc.)
- Gynaecological health-care and prescriptions

Student Awards and Financial Aid

Student Awards and Financial Aid (SAFA) is dedicated to helping students understand the variety of options available to finance their education. Budgeting and financial planning are essential to their success and SAFA is on hand to help create the right financial plan. Financial assistance can be in the form of bursaries, employment (both on-campus and off), parental resources, scholarships, student lines of credit and the Ontario Student Assistance Program (OSAP).

Information Technology Resources

Ontario Tech University is a leader among North American universities in implementing and using curriculum and industry specific software in a technology-enriched learning environment (TELE). Our unique environment is adapted to each discipline based on faculty requirements and input for optimal student learning. We are committed to providing the greatest value for students' investment in education and technology while studying at Ontario Tech University.

One of the greatest advantages of Ontario Tech University's approach to TELE is that all students have equal access to the same technology, resources and services. Whether you are inside or outside of the classroom, your course-specific software allows you to work on your own or with others and enjoy seamless access to all Ontario Tech online resources. TELE supports Bring-your-own-device (BYOD) which provides you with laptop standards when acquiring the right laptop for your program and software support services onsite and online. An annual fee for TELE covers a wide range of program-specific software, technical software support, exam support and virus protection.

IT Services strives to provide quality services to students at Ontario Tech. To support these objectives, the following components are included:

Wireless network

Wireless internet connection is available in public areas and open-air locations around the Ontario Tech campus where students congregate (North Oshawa and Downtown locations).

Wired network

To ensure the success of the technology-enriched learning environment, a comprehensive data network has been installed on campus. This includes network drops in lecture halls and designated areas as well as network drops for each residence suite.

Ontario Tech students benefit from networked classrooms and learning spaces. Each ergonomically-designed space has data network connection access and electrical connections to ensure battery regeneration. In addition, classrooms include electronic projection equipment and full multimedia support.

Exam support services

IT Services provide hardware, software and technical support during examinations. IT team will be equipped with loaner laptops in the event of major technical issues.

Laptop repairs

IT Services provide on campus repairs on eligible laptop models.

IT Service Desk

The IT Service Desk is equipped with certified technicians and experienced IT professionals offering technical support services on a drop-in, call-in or email basis.

General Use Workstations (GUWs)

Ontario Tech undergraduate students are able to use general workstations available at the library and have access to Bring Your Own Device Technology-Enriched Learning Environment (BYOD TELE) model course-specific software.

Software Support

Software Support specialists are available to students on-site and online to assist in downloading/installing University software and support any other software related issues.

Printing services

Printing services are available to students in the following areas: labs, classrooms, study common areas, the Learning Commons and the Library. All Ontario Tech students receive print credits every year, more Printpacks can be purchased through the Campus Bookstore if students require additional printing services.

Teaching & Learning Centre

The mission of the Teaching and Learning Centre (TLC) at Ontario Tech University is to empower faculty to reach their potential as educators and to create a culture where effective teaching is valued. We champion the scholarship of teaching and implementation of pedagogy. We create valuable teaching and learning professional development experiences. We move Ontario Tech University towards being a leader in teaching excellence, ultimately leading to greater student success.

The TLC provides faculty with a range of tools and facilities to assist them in providing a rich learning experience for students. Experts at the TLC provide support in various areas including curriculum development, multimedia design, learning technology and in the overall improvement of teaching practice.

In addition, the TLC funds teaching-related projects from the Teaching Innovation Fund (TIF) for proposals by faculty members aimed at developing new methods in teaching and learning. The TLC facilitates teaching awards at the University and supports faculty in their application for external awards and funding opportunities that focus on teaching and learning.

f) Graduate student financial support

- *Provide evidence that financial assistance will be sufficient to ensure quality and numbers of students*
- *Provide the teaching assistant hours and capacity within the Faculty*

Full time students in the program will receive guaranteed financial support from the following sources:

1. Graduate Research Assistantship from their supervisors, for the amount set by SGPS and guaranteed for four years of full-time study (subject to satisfactory standing).
2. Graduate Teaching Assistantship from the faculty, for 270 hours of TA work in a year at the rate determined by the university, and guaranteed for four years of full-time study (subject to satisfactory standing).

3. International student tuition scholarship for international students, equivalent to the difference between international and domestic tuition fees, subject to SGPS rules and availability.
4. A special graduate scholarship (funded by SGPS) for indigenous students in the program.

Part-time students in the program will not be guaranteed any financial support.

g) Physical resource requirements

- *Please attach a report, as an Appendix, from the Library regarding existing library holdings and support for student learning; please contact your Subject Librarian as you begin your proposal to request a 'Library statement for new program proposal'*
- *Address any space/infrastructure requirements including information technology, laboratory space, equipment, etc.* ***If new space is required, please complete Table 4 (examples in purple); otherwise, please remove this Table***
- *Ideally, please provide information on the change in the number of faculty, students, administrative staff, etc. as well as information on changes in equipment and activities (additional space; the renovation of existing space; or will the current space allocation accommodate the new program)*
- ***If new resources are needed, d the plan and commitment to provide these resources to support the program and the rationale in section 4h)***

No Additional or dedicated space is required for the new program. Classes will be shared with MITS and CS graduate programs, and research work will be conducted in supervisors' research labs.

Table 4: Additional Space Requirements

Space Type	Number Required	Space Requirements (sq. ft)

h) Resource Summary

Provide a brief statement of the funding requirements and the rationale.

Human Resource Requirements

Are additional faculty required to be able to offer this program? ☒ Yes ☐ No

If yes, what year will the faculty hire be required, and are there additional criteria associated with the hiring requirement (e.g. enrolment levels)?

A new TTT hire with expertise in the area of cybersecurity has already been hired for the program.

Are additional staff required to be able to offer this program? ☐ Yes ☒ No

If yes, please outline what year the staff hire will be required and any additional criteria associated with the hiring requirement:

Space Requirements

Are there additional space requirements specific to being able to successfully launch this program? ☐ Yes ☒ No

If yes, please provide additional details:

Technology Requirements

Are there additional technology requirements specific to being able to successfully launch this program? ☐ Yes ☒ No

If yes, please provide additional details:

Additional Resource Requirements

Are there additional resource requirements not specified above that are required to successfully launch this program? If so, please outline them below:

The resource requirements outlined above have been reviewed and approved by the Academic Resource Committee (ARC): ______________________________

(date of review)

5 Closing Statements Regarding Program Quality (QAF 2.1.2.8)

- *Please describe any additional evidence of the quality of the faculty (e.g. qualifications, funding, honours, awards, research, innovation and scholarly record) not already discussed*
- *Please provide any other evidence that the program and faculty will ensure the intellectual quality of the student experience*

APPENDICES

Please include at minimum the below. Additional Appendices may be added, as appropriate. Appendices should ultimately be listed, attached, and labelled (A, B, C, etc.) in the order in which they first are mentioned in the document.

Appendix A: Program Learning Outcome Alignment Map to DLEs
Appendix B: Calendar Copy
Appendix C: List of Program Courses, New Course Proposals, Required Course Changes, Course Syllabi for Existing Courses (can each be attached as separate appendices)
Appendix D: Detailed Listing of Faculty Committed to the Program (please use template)
Appendix E: Library Report

Items to be separate documents sent to CIQE:

New Program Funding and Tuition form (for CIQE use only)
Budget Spreadsheet (for ARC use only)
CVs for all faculty committed to the program (to be provided to the external reviewers)

Appendix A: Full Doctoral GDLE Mapping

	Demonstrate a thorough understanding and detailed knowledge of the state of the art in threats and attacks against computing systems, cyber-physical systems and social networks	Analyze, plan and apply various techniques for vulnerability assessment, protection, detection, mitigation and response to cyberattacks	Develop and evaluate information security and risk management practices, policies, and procedures that comply with the current standards, federal, provincial and international laws, agreements and policies on issues related to cybersecurity, ethical hacking and data privacy.	Demonstrate a thorough understanding and detailed knowledge of the economic, social and business drivers of cybersecurity and related technologies	Demonstrate a thorough understanding and detailed knowledge of the state of the art in applications of Artificial Intelligence to cybersecurity, attack detection and mitigation.	Evaluate, analyze and criticize limitations of cybersecurity and Artificial Intelligence tools in terms of privacy protection, algorithmic and data biases, sociopolitical impact and other potential problems	Communicate effectively and accurately to the public and in professional circles about various aspects of cybersecurity
Depth and Breadth of Knowledge	X			X	X		
A thorough understanding of a substantial body of knowledge that is at the forefront of their academic discipline or area of professional practice including, where appropriate, relevant knowledge outside the field and/or discipline.	X			X	X		
Research and scholarship	X	X		X	X		
a) The ability to conceptualize, design, and implement research for the generation of new knowledge, applications, or understanding at the forefront of the discipline, and to adjust the research design or methodology in the light of unforeseen problems;	X	X		X	X		
b) The ability to make informed judgments on complex issues in specialist fields, sometimes requiring new methods; and	X	X		X	X		
c) The ability to produce original research, or other advanced scholarship, of a quality to satisfy peer review, and to merit publication.	X	X		X	X		
Level of Application of Knowledge- The capacity to:		X	X	X	X		
a) undertake pure and/or applied research at an advanced level; and		X	X	X	X		
b) contribute to the development of academic or professional skills, techniques, tools, practices, ideas, theories, approaches, and/or materials.		X	X	X	X		
Communication Skills							X
The ability to communicate complex and/or ambiguous ideas, issues and conclusions clearly and effectively.							X
Awareness of limits of knowledge		X	X			X	
An appreciation of the limitations of one's own work and discipline, of the complexity of knowledge, and of the potential contributions of other interpretations, methods, and disciplines.		X	X			X	
Autonomy/Professional capacity		X	X			X	
a) The qualities and transferable skills necessary for employment requiring the exercise of personal responsibility and largely autonomous initiative in complex situations;		X	X			X	
b) The intellectual independence to be academically and professionally engaged and current;		X	X			X	
c) The ethical behaviour consistent with academic integrity and the use of appropriate guidelines and procedures for responsible conduct of research; and		X	X			X	
d) The ability to evaluate the broader implications of applying knowledge to particular contexts.		X	X			X	

Appendix _ – Calendar Copy

Contact Information

Faculty of Business and Information Technology
Ontario Tech University
2000 Simcoe Street North
Oshawa, ON L1G 0C5
T: 905.721.8668
E: fbit@ontariotechu.ca

Program

Ph.D. in CyberSecurity

Program General information

The PhD in Cybersecurity program is a multidisciplinary research-intensive program that covers a broad range of themes related to cybersecurity; including technology, business, policy and governance, AI and human behaviour. This program aims to prepare specialized socio-technical academics who can perform leading edge research and teaching in Academia or in Industry and help governments in policymaking in the area of cybersecurity. The objectives of the program are achieved through a combination of coursework, seminars and a research thesis. Students will gain comprehensive knowledge of theory and technologies of cybersecurity, legal and ethical issues around cybersecurity and privacy, and cybersecurity policies, as well as proficiency in cybersecurity research methodology and state-of-the art research topics. The Ph.D. in cybersecurity program is hosted at Ontario Tech Faculty of Business and Information Technology and affiliated with the Institute for Cybersecurity and Resilient Systems (ICSR), a multi-disciplinary, global centre for cybersecurity research, innovation, teaching, and outreach at Ontario Tech University.

Admission requirements

In addition to the general admission requirements for graduate studies, PhD in Cybersecurity applicants must meet the following program-specific requirements.

- Students would normally be expected to have completed a four-year undergraduate degree and a thesis-based Masters degree in a relevant field from a Canadian university, or its equivalent from a recognized institution, with an overall academic standing of at least 3.5 on a 4.0/4.3 scale or its equivalent in their last two years of study.

MITS Pathway: Graduates of Ontario Tech University Master of IT Security (MITS) program can apply to the Ph.D. program If they have completed the MITS program with an overall academic standing of at least 3.5/4.3.

- A minimum of two letters of reference from persons having direct knowledge of the applicant's academic competence. Academic references are preferred; however professional references will be accepted. Letters of reference should come from individuals under whom the applicant has worked closely or studied. The quality of the letters will be assessed by the Graduate Committee to make sure relevant requirements have been met.

- Proof of English proficiency is needed from those applicants whose first language is not English, as per university regulations.

- Applicants must find a prospective faculty supervisor from among the list of graduate faculty members of the PhD in Cybersecurity program and receive formal acceptance of the faculty member to supervise their research. No applicant will be accepted to the program without having an approved prospective supervisor in advance.

- As part of the application form, students are required to provide a minimum 3000-word long personal research statement, outlining their area of interest in cybersecurity, their proposed academic research plan, and identify the faculty supervisor who has agreed to supervise their research.

- Students admitted to the program must demonstrate their broad proficiency in the area of cybersecurity through evidence of completing or having completed graduate-level coursework in the fields of theory, applications, legal and governance issues of cybersecurity. Students who do not demonstrate appropriate background in research methods and cybersecurity fundamentals and/or ethics will be required to complete the following additional/prerequisite courses within the first 18 months of the program:

    1. Cybersecurity: The following courses are required for students who do not have prior background in IT security.

        - INFR 5010G - Fundamentals of IT security (6 Credits)
        - INFR 5100G - Law and Ethics of IT Security (3 Credits)

    2. Research methods: The following prerequisite is required for students who have not completed a previous thesis-based Master's program in a relevant field.

        - CSCI 5010G – Survey of Computer Science Research Topics and Methods (3 Credits)

Note: Students who demonstrate sufficient proficiency through prior graduate-level coursework or extensive related work experience, can request a waiver for the corresponding prerequisite course from the Graduate Program Director. Waiver requests are not guaranteed and will be considered on a case-by-case basis.

Part-time studies

The PhD in Cybersecurity program is intended to be a full-time program.

Degree requirements

a. Coursework component

The coursework component of the program may include prerequisite courses (if required as noted above), specialized courses, a seminar, a thesis proposal and a final thesis.

Students in the PhD program in Cybersecurity must take three specialized courses with the approval of their supervisory committee. These courses must be completed prior to the thesis candidacy proposal examination. The specialized courses for each year will be announced at the time of registration for that academic year, and may vary from year to year based on instructor availability. Some examples of specialized course topics are as following:

- INFR 6010G - Artificial Intelligence in Cybersecurity
- INFR 6020G - Usable Security
- INFR 6030G - Information Trust
- INFR 6040G - Infrastructure and Cyberphysical Security
- INFR 6050G – Advanced Topics in Cybersecurity
- INFR 6110G - Global Cybersecurity Threats
- INFR 6120G - Cybersecurity Leadership
- INFR 6130G – CyberCrime
- MITS 5600G – Security Policies and Risk Management
- MITS 6900G - Blockchain Fundamentals and Technologies

Note: Students may take up to two relevant MITS or CSCI 5xxx/6xxx-level courses as specialized courses (If not taken in a previous degree) with the approval of their supervisory committee and the Graduate Program Director.

Seminar/Proposal/Thesis Courses

Students must register in the following zero-credit courses for their seminar, proposal and thesis work:

- INFR 7000G - PhD Cybersecurity Seminar
- INFR 7100G - PhD thesis proposal and candidacy Exam
- INFR 7200G - PhD Dissertation

b. Research component

Students who successfully complete their coursework will then enter the thesis phase of the program. At this stage, students must prepare a thesis proposal under the supervision of their supervising committee, and then defend their proposal in an oral candidacy exam. After successful defence of their proposal, they will be considered PhD candidates. It is strongly recommended that students complete their coursework and candidacy exam within 24 months after entering the program on a full-time basis.

All PhD Candidates must defend their final thesis in an oral session in front of a committee of internal and external examiners, as per university regulations. Upon successful defence of their thesis and subject to completion of all other requirements of the program, a degree of PhD in Cybersecurity will be conferred upon them.

c. Seminars

All /students in the PhD in Cybersecurity program must register in and participate in a zero-credit seminar course every semester. Each student must present at least two seminars throughout their program: one seminar before the candidacy exam, and one exit seminar before their thesis defence.

Appendix C – List of Courses

CSCI 5010G – Survey of Computer Science Research Topics and Methods

INFR 5010G - Fundamentals of IT security

MITS 5100G - Law and Ethics of IT Security

INFR 6010G - Artificial Intelligence in Cybersecurity (Syllabus provided for MITS 5620G - Special Topics; this topic is now being offered as a stand-alone course)

INFR 6020G - Usable Security

INFR 6030G - Information Trust

INFR 6040G - Infrastructure and Cyberphysical Security

INFR 6050G – Advanced Topics in Cybersecurity

INFR 6110G - Global Cybersecurity Threats

INFR 6120G - Cybersecurity Leadership

INFR 6130G – CyberCrime

INFR 7000G - PhD Cybersecurity Seminar

INFR 7100G - PhD thesis proposal and candidacy Exam

INFR 7200G - PhD Dissertation

MITS 5600G – Security Policies and Risk Management

MITS 6900G - Blockchain Fundamentals and Technologies

UNIVERSITY OF ONTARIO INSTITUTE OF TECHNOLOGY

Faculty of Business and Information Technology

MITS5100G
Law and Ethics of IT Security
Course outline for Fall 2017

1. Course Details & Important Dates*

Term	Course Type	CRN	Day	Time	Room
Fall	Lecture	42996	Mon	6:40 pm – 9:30 pm	UA3230

Classes Start	Classes End	Last day to drop course without academic consequence	Final Exam Period
September 11th, 2017	December 4th ,2017	October 4th, 2017	December 6-17th, 2017

* for other important dates go to: www.uoit.ca >Current Students >Important Dates and Deadlines

2. Instructor Contact Information

Instructor Name	Office	Phone	Email
David Clark	TBA	416.642.3688	david.clark@uoit.ca
Office Hours: Before and after class, or by arrangement			

3. Course Description

One year ago the big Tech story was Pokémon GO. Today the news is filled with US federal investigations into whether Russian hackers interfered with US federal elections through hacking and online social media manipulation, as well as stories about the surge in ransomware that threatens entire business sectors and even the governments of nation states. And legal issues figured heavily into both. While people wandering the streets playing games on their phones[1] seems to have little in common with cyber attacks on businesses and democratic institutions, both situations point out what happens when technology creates new ways for people to communicate and interact. That is to say, sometimes the law does not keep up very well.

[1] During the summer of 2016 there were many articles in the popular and IT industry media about: the game causing a danger to players and non-players; homeowners suing the publisher Niantic Inc. for trespass (even though no one from Niantic ever sets foot on those properties); calls to regulate the game or the players to remove them from sacred sites like cemeteries and memorials; and even comments that the selection of sites for PokéStops showed unintended racial biases justifying calls for a code of ethics for future programmers of location-based augmented reality games.

Why should we pay attention to this? Because both situations teach us a great deal about why technology, law and ethics sometimes clash. And they also help us understand where the law and technology can work well together.

Information technology in its many forms presents exciting new opportunities for enterprises of all kinds. With each innovation the doors are flung open for new business models to be born and for existing businesses to reinvent themselves. What they all have in common is the need to safeguard information. This is transforming IT departments and professionals into protectors of significant business assets, the custodians of official business records, and the wardens of customers' private information. Laws and the courts impose many of these duties. They also provide critical and effective tools to achieving success in protecting information and other intellectual property.

Yet the very characteristics of e-commerce and online activities that create great opportunities also present significant challenges for the law. And many times, laws are ultimately incapable of providing meaningful protection for computer systems and data. Therefore, as IT Security Professionals, you must understand this interplay between IT and the law. Only then can you anticipate how the law may best be used to achieve IT security in the face of new technologies, and when other tools may be required. Furthermore, when a breach of security actually occurs, you must know how to respond, and even this is shaped by laws and legal principles.

However, as IT Security Professionals responding to the challenges of new technologies, you will also find that the law sometimes fails to provide "real world" guidance about what security methods are acceptable. Moreover, news media are filled with stories about how governments which are are supposed to be protecting citizens are engaging in far-reaching and pervasive monitoring of their electronic communications. Some call these activities illegal. Others defend them and counter that the monitoring is permitted under the law. In these and other circumstances, behaviour that is legally permissible may nevertheless seem improper or ethically challenging. For such cases, you must also have a solid understanding of professional ethics developed by your professional community and peers.

This course will provide an overview of the laws and professional ethics that IT Security Professionals must understand. In the early weeks of the course, we will examine some of the basic ideas and dynamics that will help us analyze and discuss the interplay between technology, law and professional ethics. Later, we will examine one or two substantive areas of law each week, including: e-contracts; e-regulation; online crime; intellectual property; privacy; data breach liability; and we will conclude by examining the concept of ethical hacking, the "white hat" hacker vs. the "black hat" hacker, and those in between.

4. Learning Outcomes

On the successful completion of the course, students will be able to:

- Explain basic principles of substantive areas of law covered in the course;
- Demonstrate a basic understanding of the principles, dynamics and tools of computer law;
- Explain how and why online activities and e-business challenge traditional areas of law, and where the law is successful in regulating behavior;
- Demonstrate an understanding of common ethical systems and professional Codes of Ethics;

- Analyze novel situations to identify IT Security issues from the legal and ethical perspectives;
- Explain issues arising from hacking and ethical hacking.

5. Course Design

Course content will be delivered through a combination of lectures, discussions and assignments. Success in the course will require students to attend and participate in class. Reading assignments must be completed prior to each class in preparation for the more advanced discussions in the lecture.

The lectures and discussions will provide the core theory. Assignments will include short papers. There will also be a term project. These activities allow students to apply information from course theory and readings and to utilize problem solving and decision-making skills to analyze realistic scenarios.

Through written assignments, examination, and participation in class discussions, students will gain practice in the use of oral and written communication skills. There is a Blackboard course web page which includes a constantly updating calendar of course milestones, assignment and test dates, and so on. Students are expected to log on to the page regularly and to keep informed of course requirements. Items posted on the course site are deemed communicated to the class. Students are required to use the email tool attached to the Blackboard course website if they wish to communicate with the instructor by email.

[The rest of this page left blank intentionally.]

6. Outline of Topics in the Course

Lecture #	Date	Topics
Lecture 1	Sept 11	• Introduction to Law and Ethics • What is "Law"? • Computer Ethics
Lecture 2	Sept 18	• Dynamics, Themes and Skill Sets of Computer Law • Law of the Horse: Code as Law
Lecture 3	Sept 25	• Jurisdiction in a Borderless World • Is there a "there" there? • Evidence Law
Lecture 4	Oct 2	• e-Contracts • Implied Click Consent & Express Click Consent
	Oct 9	THANKSGIVING – NO CLASSES
Lecture 5	Oct 16	• Computer Crime in Canada and the US • Preventing Harmful Conduct
Lecture 6	Oct 23	• Privacy Law in Canada, the EU and US • Data Breach Regulation
Lecture 7	Oct 30	• Intellectual Property: Part 1 • Patents • Trade-mark Law
Lecture 8	Nov 6	• Intellectual Property: Part 2 • Copyright • Digital Rights Management (DRM) • DMCA (US and others)
Lecture 9	Nov 13	• Self-Regulation and Indirect Regulation of Online Activities • White House Cybersecurity Framework
Lecture 10	Nov 20	• Regulating Social Media • SPAM - CASL
Lecture 11	Nov 27	• Cyberliability • Privacy breach liability • Cyber Insurance as Risk Management
Lecture 12	Dec 4	• Ethical Hacking

7. Required Texts/Readings

Fitzgerald, P., Wright, B., & Kazmierski, V., *Looking at Law – Canada's Legal System*, 6th Edition. Toronto: LexisNexis Canada, 2010.

Takach, George S., *Computer Law*, 2nd Edition, Toronto: Irwin Law, 2003.

(*Both textbooks are also available on three-hour reserve from the Reserve Desk at the UOIT Library*).

Each week, **additional mandatory readings** will be posted on the course website on Blackboard that **you will be responsible to prepare**.

8. Evaluation Method

The evaluation components and their respective weightings towards the final mark are shown below:

Course Component	**Portion of Final Mark**	**Date Assigned***	**Date Due***
First Assignment	5%	Sept 18	Sept 25
Second Assignment	5%	TBA	TBA
Midterm Exam	30%	Oct 16	Oct 23
Project / Paper	20%	Oct 23	Nov 20
Final Exam	40%	TBA	TBA

*These dates are subject to change. Changes will be announced in class and on Blackboard.

More specific instructions and deadlines for submission will be provided for each Course Component. You are responsible to review and adhere to them.

Final course grades may be adjusted to conform to program or Faculty grade distribution profiles. Further information on grading can be found in the Academic Regulations of the UOIT Academic Calendar.

9. Assignments and Tests

All assignments, tests and examinations will be in a "take home" format. You are expected to adhere to the Academic Regulations contained in the UOIT Academic Calendar 2017/18, as well as all other Academic and Administrative Policies of UOIT.

There will be no make-up assignments or tests.

Missed Term Test

Students who miss a midterm or term test for medical or compassionate grounds may submit a request for deferral along with supporting documentation to the Faculty Advising offices within three (3) working days. Medical deferrals will be comprised of a completed UOIT Medical

Statement form completed by the student and physician within 24 hours of the missed course work. These forms can be found on the UOIT website or the FBIT Announcement Board on Blackboard. If a midterm or term test is missed for approved reasons, the weight of the missed component will be added to the final.

Missed Course Work

Coursework missed for medical or serious personal reasons must be documented and reported to the instructor within three (3) working days of the missed work. Medical absences must be accompanied by a UOIT Medical Statement form completed by the student and physician within 24 hours of the missed course work. Coursework includes, but is not limited to, quizzes; written assignments; participation; case studies; etc… If missed coursework totals more than 20% of the final grade, this must be documented through the FBIT Academic Advising office. The weight of the missed course component will be reweighted to the final examination. If you miss coursework and do not notify the instructor within the three (3) working day deadline, you will receive a score of zero on the missed component.

Any student who faces challenges securing their food or housing and believes this may affect their performance in the course is urged to contact studentlife@uoit.ca for support.

10. Accessibility

Accommodating students with disabilities at UOIT is a responsibility shared among various partners: the students themselves, SAS staff and faculty members. To ensure that disability-related concerns are properly addressed during this course, students with documented disabilities and who may require assistance to participate in this class are encouraged to speak with me as soon as possible. **Students who suspect they have a disability that may affect their participation in this course are advised to go to Student Accessibility Services (SAS) as soon as possible.** Maintaining communication and working collaboratively with SAS and faculty members will ensure you have the greatest chance of academic success.

Students taking courses on the North Campus Location can visit Student Accessibility Services in the U5 Building located in the Student Life Suite. Students taking courses on the Downtown Oshawa Campus Location can visit Student Accessibility Services in the 61 Charles St. Building, 2nd Floor, Room DTA 225 in the Student Life Suite.

Disability-related support and accommodation support is available for students with mental health, physical, mobility, sensory, medical, cognitive, or learning challenges. Office hours are 8:30am-4:30pm, Mon-Fri. For more information on services provided, you can visit the SAS website at http://uoit.ca/studentaccessibility

Students may contact Student Accessibility Services by calling 905-721-3266, or email studentaccessibility@uoit.ca

Students who require the use of the Test Centre to write tests, midterms, or quizzes MUST register online using the SAS test/exam sign-up module, found here www.uoit.ca/SASexams. Students must sign up for tests, midterms or quizzes AT LEAST seven (7) days before the date of the test.

Students must register for final exams by the registration deadline, which is typically 2 weeks prior to the start of the final examination period. SAS will notify students of the registration deadline date.

11. Academic Integrity

Students and faculty at UOIT share an important responsibility to maintain the integrity of the teaching and learning relationship. This relationship is characterized by honesty, fairness and mutual respect for the aim and principles of the pursuit of education. Academic misconduct impedes the activities of the university community and is punishable by appropriate disciplinary action.

Students are expected to be familiar with and abide by UOIT's regulations on Academic Conduct (Section 5.15 of the Academic Calendar) which sets out the kinds of actions that constitute academic misconduct, including plagiarism, copying or allowing one's own work to copied, use of unauthorized aids in examinations and tests, submitting work prepared in collaboration with another student when such collaboration has not been authorized, among other academic offences. The regulations also describe the procedures for dealing with allegations, and the sanctions for any finding of academic misconduct, which can range from a resubmission of work to a failing grade to permanent expulsion from the university. A lack of familiarity with UOIT's regulations on academic conduct does not constitute a defense against its application.

Further information about academic misconduct can be found in the Academic Integrity link on your laptop. Extra support services are available to all UOIT students in academic development, study skills, counseling, and peer mentorship. More information on student support services can be found in the Academic Calendar (Section 8).

12. Turnitin

UOIT and faculty members reserve the right to use electronic means to detect and help prevent plagiarism. Students agree that by taking this course all assignments are subject to submission for textual similarity review by Turnitin.com. Assignments submitted to Turnitin.com will be included as source documents in Turnitin.com's restricted access database solely for the purpose of detecting plagiarism in such documents for five academic years. The instructor may require students to submit their assignments electronically to Turnitin.com or the instructor may submit questionable text on behalf of a student. The terms that apply to UOIT's use of the Turnitin.com service are described on the Turnitin.com website.

Students who do not wish to have their work submitted to Turnitin.com must provide with their assignment at the time of submission to the instructor a signed Turnitin.com Assignment Cover sheet:
http://www.uoit.ca/assets/Academic~Integrity~Site/Forms/Assignment%20Cover%20sheet.pdf

Further information about Turnitin can be found on the Academic Integrity link on your laptop.

13. Final Examinations

Final examinations are held during the final examination period at the end of the semester and may take place in a different room and on a different day from the regularly scheduled class. Check the published Examination Schedule for a complete list of days and times.

Students are advised to obtain their Student ID Card well in advance of the examination period as they will not be able to write their examinations without it. Student ID cards can be obtained at the Campus ID Services, in G1004 in the Campus Recreation and Wellness Centre.

Students who are unable to write a final examination when scheduled due to religious publications may make arrangements to write a deferred examination. These students are required to submit a Request for Accommodation for Religious Obligations to the Faculty concerned as soon as possible and no later than three week prior to the first day of the final examination period.

Further information on final examinations can be found in Section 5.25 of the Academic Calendar.

14. Freedom of Information and Protection of Privacy Act

The following is an important notice regarding the process for submitting course assignments, quizzes and other evaluative material in your courses in the Faculty of Business and Information Technology.

As you may know, UOIT is governed by the *Freedom of Information and Protection of Privacy Act* ("FIPPA"). In addition to providing a mechanism for requesting records held by the university, this legislation also requires that UOIT not disclose the personal information of its students without their consent.

FIPPA's definition of "personal information" includes, among other things, documents that contain both your name and your Banner ID. For example, this could include graded test papers or assignments. To ensure that your rights to privacy are protected, the Faculty of Faculty of Business and Information Technology encourages you to use only your Banner ID on assignments or test papers being submitted for grading. This policy is intended to prevent the inadvertent disclosure of your information where graded papers are returned to groups of students at the same time. If you still wish to write both your name and your Banner ID on your tests and assignments, please be advised that UOIT will interpret this as an implied consent to the disclosure of your personal information in the normal course of returning graded materials to students.

If you have any questions or concerns relating to the new policy or the issue of implied consent addressed above, please contact accessandprivacy@uoit.ca

15. Course Evaluations

Student evaluation of teaching is a highly valued and helpful mechanism for monitoring the quality of UOIT's programs and instructional effectiveness. To that end, course evaluations are administered by an external company in an online, anonymous process during the last few weeks of classes. Students are encouraged to participate actively in this process and will be notified of the dates. Notifications about course evaluations will be sent via e-mail, and posted on Blackboard, Weekly News and signage around the campus.

16. Sexual Violence Policy

UOIT is committed to the prevention of sexual violence in all is forms. For *any* UOIT student who has experienced Sexual Violence, **UOIT can help**. UOIT will make accommodations to cater to the diverse backgrounds, cultures, and identities of students when dealing with individual cases.
If you think you have been subjected to or witnessed sexual violence:

- Reach out to a Support Worker, who are specially trained individuals authorized to receive confidential disclosures about incidents of sexual violence. Support Workers can offer help and resolutions options which can include safety plans, accommodations, mental health support, and more. To make an appointment with a Support Worker, call 905.721.3392 or email supportworker@uoit.ca
- Learn more about your options at: www.uoit.ca/sexualviolence

Appendix: Other Policies and Expectations for the Learning Environment

1. Effective Learning in the Classroom

The following are suggestions on how to carry out effective learning in your daily studying:

• Pre-Class Preparation:

Before you go to your classroom, you should allow enough time for commuting, and eat a healthy meal or snack. Also, you should ask yourself the following questions:

- Have you *previewed* the reading assignments?
- Have you noted down key insights and questions from your reading?

* *Rule of thumb*: for every hour lecture, you need approximately three hours of outside class studying to reinforce the material learnt in class.

• In-Class Attitude:

In order to get the most out of your lectures, you need to:

- Arrive to class On Time
- Concentrate (be curious and be motivated)
- Be Active:
  - in class discussion
  - in group activities
  - in creative and critical thinking

And you should also AVOID the following:

- Eating 'strong smelling' or 'noisy' food
- Getting involved in side conversations
- Sending signs that scheduled class time is up, i.e. closing up your laptop or standing
- Answering cellular phones in class

• After class:

- Review lecture notes; highlight key points
- Consult instructors or TA for unresolved questions
- Seek help when necessary
- Finish assignments on time

2. The use of your laptop in the classroom

The use of laptops often enhances the learning experience. However, there are circumstances when it can be obstructive. Instructors have the right and the responsibility to determine appropriate classroom protocols for student use of laptops. Students refusing to comply with such requests may be requested to remove themselves from the classroom. Students refusing to comply may also be considered to be in violation of our University code of conduct and disciplinary action may result.

- **Examples of appropriate use of laptops**:

- Taking lecture notes
- Course related computing
- Limited messaging for learning purposes
- Download course material from Blackboard

- **Examples of Inappropriate Use of Laptop**

- Watching movies
- Playing computer games
- Social messaging

3. Effective team management

The following are suggestions on how to effectively manage your teamwork:

Setting clear objectives
Signing the team contract
Meeting regularly
Conducting effective meetings

- Assigning roles to members
- Staying in touch: meeting; emails; phones
- Managing conflicts effectively

4. Managing Conflict

The following are suggestions on how to resolve conflict that could possibly happen during your studying:

- Have a team contract to guide conflict resolution.
- The team "leader" might send an e-mail to the absent member, and copy all members, asking why he or she missed the meeting.
- Keep an attendance log and use this as part of your peer review process.
- Try to avoid making any decisions that are known to be an issue for an absent member until that person can be reached.

5. In the event of the illness

In the event of illness, you are suggested to:

- Please stay home so as not to spread it to others
- Contact your Academic Advisor by email or phone right away – not your instructor.

The Academic Advisors will organize any assignment, test or lab adjustments if needed.
You can find your academic advisor contact information at:
http://www.businessandit.uoit.ca/people/academic-advisors.php

- Also check the following website http://www.cdc.gov for further health and wellness information.

6. Academic Planning and General Information

Please follow the link below to view our academic resources and calendar. This link will provide you with information pertaining to Grade point average (GPA), Academic Standing Requirements, Internship Programs, Graduation Information, etc.
https://uoit.ca/current-students/index.php

Other links of interest include:

http://www.businessandit.uoit.ca/undergraduate/index.php for information pertaining to **FBIT Undergraduate Programs**

http://www.gradstudies.uoit.ca/ for information on **Graduate Programs**

https://uoit.ca/current-students/campus-services/ for information on **Campus Services**

http://www.businessandit.uoit.ca/about/student-societies/index.php for information pertaining to **Student Societies**

July 2022

Ontario Tech University

Faculty of Business and Information Technology

MITS6900G Blockchain Foundation and Technology

Course outline for **FALL 2022**

1. Course Details & Important Dates*

Term	Course Type	Day	Time	Location	CRN #
FALL 2022	Lecture	Tuesday	5:10PM – 8:00PM	UA2120	44919

Classes Start	Classes End	Last day to drop course without academic consequence	Final Exam Period
September 6, 2022	December 5, 2022	October 3, 2022	December 7 – 16, 2022

* Visit https://ontariotechu.ca/current-students/academics/important-dates-and-deadlines.php

2. Instructor Contact Information

Instructor Name	Office	Phone	Email
Sheikh Ahmed Munieb	UB2018	905.721.8668 Ext: 5361	Ahmed.sheikh@ontariotechu.ca
Office Hours: By Appointment Tuesday: 12PM – 1:00PM			

Laboratory/Teaching Assistant Name	Email
Divyesh Savani	divyeshlallubhai.savani@ontariotechu.net

3. Course Description

This course introduces blockchains from a technical perspective. Students will learn: the fundamentals of blockchains, cryptocurrencies, and dApps; the key business and value drivers of blockchain services; application development fundamentals, best practices, and supportive technologies; economic drivers and bleeding-edge trends. This course includes the development and deployment of a custom blockchain using Python, followed by multiple smart contract implementations using Solidity.

4. Learning Outcomes

On the successful completion of the course, students will be able to:

- demonstrate and verbalize a deep understanding of blockchains and their technical underpinnings
- understand the economic and business drivers of blockchain and web 3.0
- compare and contrast blockchain technologies, their use cases, and emerging technologies
- architect, develop, and deploy basic blockchain solutions using industry-standard tools and languages

5. Course Design

Course content will be presented to students during the assigned lecture periods. Some lectures will include hands-on components and exercises. Lecture slides will be posted on Canvas, however some hands-on content and discussions or Q/A in the class may not be covered in the lecture slide. Students should plan to attend all lectures and take notes to get the most out of this course.

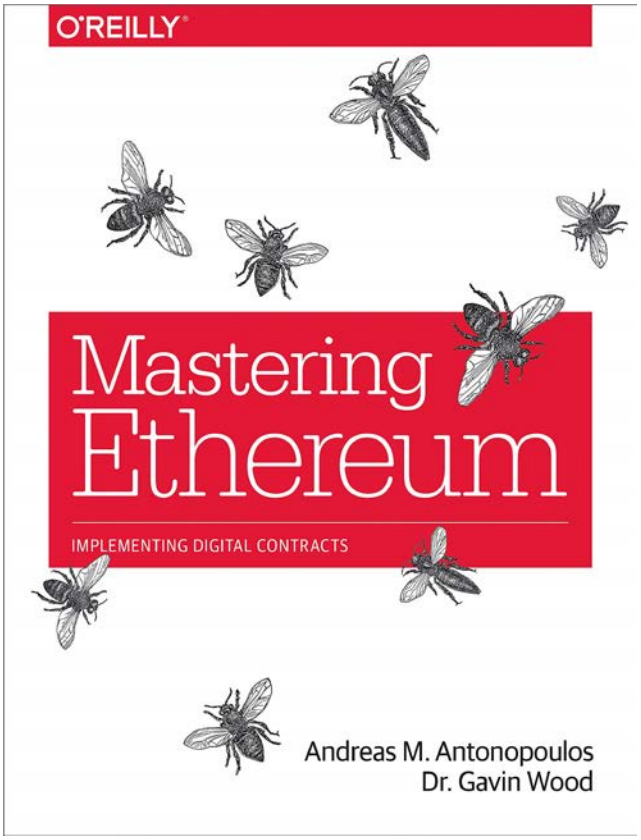
6. Outline of Topics in the Course

Lecture #	Date	Time	Topics	Details of topics to be covered in the course, by unit or by week
1	September 6th ,2022	5:10PM – 8:00PM	Blockchain – Introduction	
2	September 13th ,2022	5:10PM – 8:00PM	Blockchain – Technical Deep-Dive	
3	September 20th ,2022	5:10PM – 8:00PM	Blockchain – Development (Python & Flask)	
4	September 27th, 2022	5:10PM – 8:00PM	Cryptocurrency – Bitcoin 1	
5	October 4th, 2022	5:10PM – 8:00PM	Cryptocurrency – Bitcoin 2	
	October 10, 2022		Thanksgiving Day, no scheduled academic activities.	
STUDY BREAK	October 11 to 16, 2022		Study Break, no scheduled academic activities	

6	October 18th, 2022	5:10PM – 8:00PM	Cryptocurrency – Development (Python & Flask)	
7	October 25th, 2022	5:10PM – 8:00PM	Ethereum & Smart Contracts	
8	November 1st, 2022	5:10PM – 8:00PM	Alternative Cryptocurrencies	
9	November 8th, 2022	5:10PM – 8:00PM	Building Smart Contracts with Solidity – Part 1	
10	November 15th, 2022	5:10PM – 8:00PM	Building Smart Contracts with Solidity – Part 2	
11	November 22nd, 2022	5:10PM – 8:00PM	Building Smart Contracts with Solidity Part-3 / Final Project Presentations	
12	November 29th, 2022	5:10PM – 8:00PM	Final Project Presentations	
	December 6, 2022		Study break, no scheduled academic activities.	

7. Required Texts/Readings

Below is the recommended book for this course:



Publisher: O'Reilly Media; 1st edition (Jan. 8 2019)

Language: English

Paperback: 424 pages

ISBN-10: 1491971940

ISBN-13: 978-1491971949

Additional readings may be assigned or recommended during the course.

8. Evaluation Method

Students will be graded according to the following distribution:

Assignment 1	15%	Details TBA on Canvas
Development Assignment 2	15%	Details TBA on Canvas
Research Assignment 3	15%	Details TBA on Canvas
Cryptocurrency Video Assignment	25%	Details TBA on Canvas
Final Project Code	20%	Details TBA on Canvas
Final Project Presentation	10%	Details TBA on Canvas

Note: You must meet the following criteria in order to receive credit for this course:

1. Pass at least one development assignment
2. Pass one of: cryptocurrency video assignment OR final project code

Final course grades may be adjusted to conform to program or Faculty grade distribution profiles. Further information on grading can be found at:
https://calendar.ontariotechu.ca/content.php?catoid=55&navoid=2422

9. Assignments and Tests

Important Due Dates

Assignment 1	October 7th 2022
Development Assignment 2	October 29th 2022
Research Assignment 3	November 15th 2022
Cryptocurrency Video Assignment	November 1st 2022
Final Project Code	November 21st 2022
Final Project Presentation	22nd & 29th November 2022

Note: All students must demonstrate contribution to their group's video assignment and final project in order to pass this course (unless a deferral has been granted by the faculty or instructor).

All development assignment details will be released in-class prior to the due date. The cryptocurrency video assignment and final project details will be released on Canvas during the third week of September.

Missed Course Work

Coursework missed for medical or serious personal reasons must be documented and reported to the instructor within three (3) working days of the missed work using an Academic Consideration form. Coursework includes, assignments and Project. If missed coursework totals more than 25% of the final grade, this must be documented through the FBIT Academic Advising office, instructor will then contact you for make-up course work. If you miss coursework and do not notify the instructor within the three (3) working day deadline, you will receive a score of zero on the missed component.

10. Technology Requirements and Learning Management System Information

Ontario Tech uses *Canvas*™ as its learning management system (LMS). Access to the LMS is limited to students formally registered in courses. That access is for the duration of the semester **and for an additional 120 days once the semester is over**. Students are strongly encouraged to download any/all relevant course material during that access period. Any requests for access post this period must be made in writing to the instructor/faculty member responsible for the course.

To support online learning, the university recommends certain technology requirements for laptops, software and internet connectivity which are available at: https://itsc.ontariotechu.ca/remote-learning.php.

Students experiencing technical difficulties such that they are unable to meet the technology requirements may contact the IT Service Help Desk at: servicedesk@dc-uoit.ca Students experiencing financial difficulties such that they are unable to meet the technology requirements may contact Student Awards and Financial Aid Office at: connect@ontariotechu.ca

By remaining enrolled in this course, you acknowledge that you have read, understand and agree to observe the Recommended Technology Requirements for accessing university online learning resources, including those minimum requirements that are specific to your faculty and program.

11. Sensitive/Offensive Subject Matter

The classroom (both physical and virtual) is intended to provide a safe, open space for the critical and civil exchange of ideas and opinions. Some articles, media and other course materials may contain sensitive content that is offensive and/or disturbing. For example, some articles or videos may contain e.g. graphical depictions of violence, profanity, human anatomy, sexual acts, matters pertaining to race, gender, or sexuality. The Course Instructor will try to identify such material and communicate warnings to students in advance of the distribution and use of such materials, affording students the choice to either emotionally prepare for, or not to view or interact with, the content.

12. Student Support

Any student who faces challenges securing their food or housing and believes this may affect their performance in the course is urged to contact studentlife@ontariotechu.ca for support. Furthermore, please notify your professor if you are comfortable in doing so. This will enable them to provide any resources and help that they can.

13. Sexual Violence Support and Education

Ontario Tech is committed to the prevention of sexual violence in all its forms. For any student who has experienced Sexual Violence, Ontario Tech can help. We will make accommodations to cater to the diverse backgrounds, cultures, and identities of students when dealing with individual cases.

If you think you have been subjected to or witnessed sexual violence:

- Reach out to a Support Worker, a specially trained individual authorized to receive confidential disclosures about incidents of sexual violence. Support Workers can offer help and resolution options which can include safety plans, accommodations, mental health support, and more. To make an appointment with a Support Worker, call 905.721.3392 or email studentlife@ontariotechu.ca
- Learn more about your options at: https://studentlife.ontariotechu.ca/sexualviolence/

14. Students with Disabilities

Accommodating students with disabilities at Ontario Tech is a responsibility shared among various partners: the students themselves, SAS staff and faculty members. To ensure that disability-related concerns are properly addressed during this course, students with documented disabilities and who may require assistance to participate in this class are encouraged to speak with me as soon as possible. **Students who suspect they have a disability that may affect their participation in this course are advised to go to Student Accessibility Services (SAS) as soon as possible.** Maintaining communication and working collaboratively with SAS and faculty members will ensure you have the greatest chance of academic success.

When on campus access is allowed, students taking courses on north Oshawa campus can visit Student Accessibility Services in Shawenjigewining Hall, third floor, room 320. Students taking courses on the **downtown Oshawa campus** can visit Student Accessibility Services in the 61 Charles St. Building, 2nd Floor, Room DTA 225 in the Student Life Suite.

Disability-related and accommodation support is available for students with mental health, physical, mobility, sensory, medical, cognitive, or learning challenges. Office hours are 8:30am-4:30pm, Monday to Friday, closed Wednesday's 8:30am – 10:00am. For more information on services provided, you can visit the SAS website at https://studentlife.ontariotechu.ca/services/accessibility/index.php. Students may contact Student Accessibility Services by calling 905-721-3266, or email studentaccessibility@ontariotechu.ca.

When on campus access is allowed, students who require the use of the Test Centre to write tests, midterms, or quizzes MUST register online using the SAS test/exam sign-up module, found here https://disabilityservices.ontariotechu.ca/uoitclockwork/custom/misc/home.aspx. Students must sign up for tests, midterms, or quizzes AT LEAST seven (7) days before the date of the test.

Students must register for final exams by the registration deadline, which is typically two (2) weeks prior to the start of the final examination period. SAS will notify students of the registration deadline date.

15. Professional Suitability

Ontario Tech University is a community that values and promotes respect, integrity, diversity and accountability among all members of the university. These values can only be achieved in an environment that supports and protects the safety and security of its members. The Ontario Tech University Policy on Student Conduct defines and guides standards of student behaviour at the university to uphold these values and ensure that behaviour contrary to these standards are dealt with in a manner that is fair, open and effective.

The Faculty of Business & IT has the following expectations related to professionalism for all its community members, including without limitation, students, Staff, and Faculty:

- **Respect, civility, and courtesy:** Community members are expected to treat each other with respect, civility, and courtesy both in and outside of the classroom. Rudeness, profanity, insults, harassment, and class disruptions are unacceptable.
- **Critique ideas, not the people who raise the ideas:** Discussions, debates, and the exchange of ideas are normal parts of life in an academic community. Community members are expected to engage in discussions, debates, and the exchange of ideas in respectful ways, even while vigorously advocating for one's perspective.
- **Talk *to* those with whom you have a complaint, not *about* them.** When community members have disputes, complaints, and/or concerns about another community member, they are expected to do their best to address the matter directly and informally with the other member, provided that it is safe to do so. (See Appendix A for more information about how students can raise concerns about academic matters.)
- **Special obligations:** Community members in positions of authority have special obligations to demonstrate respect, civility, and professionalism and to encourage the development of these values within the FBIT community.

The *Professional Suitability* policy can be found at https://usgc.ontariotechu.ca/policy/policy-library/policies/academic/academic-conduct-and-professional-suitability-policy.php and the related procedures are hosted at https://usgc.ontariotechu.ca/policy/policy-library/policies/academic-misconduct-and-professional-unsuitability.php

16. Academic Integrity

Students and faculty at Ontario Tech University share an important responsibility to maintain the integrity of the teaching and learning relationship. This relationship is characterized by honesty, fairness and mutual respect for the aim and principles of the pursuit of education. Academic misconduct impedes the activities of the university community and is punishable by appropriate disciplinary action.

Students are expected to be familiar with and abide by Ontario Tech University's regulations on Academic Conduct which sets out the kinds of actions that constitute academic misconduct, including plagiarism, copying or allowing one's own work to copied, use of unauthorized aids in examinations and tests, submitting work prepared in collaboration with another student when such collaboration has not been authorized, among other academic offences. The regulations also describe the procedures for dealing with allegations, and the sanctions for any finding of academic misconduct, which can range from a resubmission of work to a failing grade to permanent expulsion from the university. A lack of familiarity with these regulations on academic conduct does not constitute a defense against its application. This information can be found at https://usgc.ontariotechu.ca/policy/policy-library/policies/academic/academic-integrity-policy.php

Extra support services are available to all Ontario Tech University students in academic development, study skills, counseling, and peer mentorship. More information on student support services can be found at https://studentlife.ontariotechu.ca/services/academic-support/index.php

17. Turnitin (if applicable)

Ontario Tech University and faculty members reserve the right to use electronic means to detect and help prevent plagiarism. Students agree that by taking this course all assignments are subject to submission for textual similarity review by Turnitin.com. Assignments submitted to Turnitin.com will be included as source documents in Turnitin.com's restricted access database solely for the purpose of detecting plagiarism in such documents. The instructor may require students to submit their assignments electronically to Turnitin.com or the instructor may submit questionable text on behalf of a student. The terms that apply to Ontario Tech University's use of the Turnitin.com service are described on the Turnitin.com website.

Students who do not wish to have their work submitted to Turnitin.com must provide with their assignment at the time of submission to the instructor a signed Turnitin.com Assignment Cover sheet: https://tlc.ontariotechu.ca/educational-technology/assignment-cover-sheet_updatedmay2021-1.pdf

18. Online Test and Exam Proctoring (Virtual Proctoring)

Ontario Tech University will conduct virtual monitoring of examinations in accordance with Ontario privacy legislation and all approved policy instruments.

19. Final Examinations (if applicable)

Final examinations are held during the final examination period at the end of the semester and **when on campus access is allowed,** may take place in a different room and on a different day from the regularly scheduled class. Check the published Examination Schedule for a complete list of days and times.

Students are required to show their Student ID card (campus ID) when **in-person examinations are allowed.** Students are advised to obtain their Student ID Card well in advance of the examination period as they will not be able to write their examinations without it. More information on ID cards can be found at https://registrar.ontariotechu.ca/campus-id/index.php.

Students who are unable to write a final examination when scheduled due to religious publications may make arrangements to write a deferred examination. These students are required to submit a Request for Accommodation for Religious Obligations to the Faculty concerned as soon as possible and no later than three weeks prior to the first day of the final examination period.

Further information on final examinations can be found at https://usgc.ontariotechu.ca/policy/policy-library/policies/academic/procedures-for-final-examination-administration.php

20. Freedom of Information and Protection of Privacy Act

The following is an important notice regarding the process for submitting course assignments, quizzes, and other evaluative material in your courses in the Faculty of Business and IT.

Ontario Tech University is governed by the Freedom of Information and Protection of Privacy Act ("FIPPA"). In addition to providing a mechanism for requesting records held by the university, this legislation also requires that the University not disclose the personal information of its students without their consent.

FIPPA's definition of "personal information" includes, among other things, documents that contain both your name and your Banner (student) ID. For example, this could include graded test papers or assignments. To ensure that your rights to privacy are protected, the Faculty of Business and IT encourages you to use only your Banner ID on assignments or test papers being submitted for grading. This policy is intended to prevent the inadvertent disclosure of your information where graded papers are returned to groups of students at the same time. If you still wish to write both your name and your Banner ID on your tests and assignments, please be advised that Ontario Tech University will interpret this as an implied consent to the disclosure of your personal information in the normal course of returning graded materials to students.

If you have any questions or concerns relating to the new policy or the issue of implied consent addressed above, please contact accessandprivacy@ontariotechu.ca

Notice of Collection and Use of Personal Information

Throughout this course, personal information may be collected through the use of certain technologies under the authority of the *University of Ontario Institute of Technology Act, SO*

2002, c. 8, Sch. O. and will be collected, protected, used, disclosed and retained in compliance with Ontario's *Freedom of Information and Protection of Privacy Act R.S.O. 1990, c. F.31.*

This course will use the following technologies that may collect, use, disclose and retain personal information (including images) for the purposes described below:

- Peer-shared applications, services or technologies that may be reviewed, assessed, or used as part of coursework.
- Other applications, services, or technologies that support or enhance online learning that include, but are not limited to, the following: Turnitin, cryptocurrency wallets etc

For more information relating to these technologies, we encourage you to visit: https://tlc.ontariotechu.ca/learning-technology/index.php Questions regarding personal information may be directed to: Ontario Tech University Access and Privacy Office, 2000 Simcoe Street North, Oshawa, ON L1G 0C5, email: accessandprivacy@ontariotechu.ca.

By remaining enrolled in this course, you acknowledge that you have read, understand, and agree to the terms and conditions under which the technology provider(s) may collect, use, disclose and retain your personal information. You agree to the university using the technologies and using your personal information for the purposes described in this course outline.

21. Human Rights and Respect

Ontario Tech University is committed to providing a campus environment in which all University Members are treated with dignity and to fostering a climate of understanding and mutual respect. The University will not tolerate, ignore or condone Discrimination or Harassment by or against anyone. Examples of Harassing behavior include, but are not limited to; bullying, taunting or mocking someone's race or creed, ridiculing an individual's disability, or targeting individuals with unwanted sexual or negative stereotypical comments about one's sex, gender, sexual orientation, gender identity and/or gender expression. Pursuant to Ontario Tech's Respectful Campus Policy, students are reminded of their role in ensuring a campus environment that is equitable and inclusive. Requirements to refrain from harassment and discrimination apply broadly to the classroom, including in lectures, labs and practicums, as well as through the use of sanctioned and unsanctioned technological tools that facilitate remote learning, e.g. class and other chat functions, video conferencing, electronic mail and texts, and social media content amongst or about University students, faculty and staff.

22. Freedom of Expression

Pursuant to Ontario Tech's Freedom of Expression Policy, all students are encouraged to express ideas and perspectives freely and respectfully in university space and in the online university environment, subject to certain limitations. Students are reminded that the limits on Freedom of Expression include speech or behaviour that: is illegal or interferes with the university's legal obligations; defames an individual or group; constitutes a threat, harassment or discrimination; is a breach of fiduciary, contractual, privacy or confidentiality obligations or commitments; and unduly disrupts and interferes with the functioning of the university. In the context of working online, different forms of communication are used.

Where permitted, students using “chat” functions or other online forms of communication are encouraged to ensure that their communication complies with the Freedom of Expression Policy.

23. Copyright Notice

All teaching materials provided by the instructor throughout the course, including, but not limited to, in whole or in part, recorded lectures, slides, videos, diagrams, case studies, assignments, quizzes, and examinations are subject to the Copyright Act, R.S.C., 1985, c. C-42. Teaching materials are owned by the faculty member, instructor or other third party who creates such works. The copyright owner(s) reserves all intellectual property rights in and to the teaching materials, including the sole right to copy, reproduce, distribute, and modify the teaching materials. Consistent with the university's Intellectual Property Policy, teaching materials are intended only for the educational use of Ontario Tech University students registered in the course that is the subject of this course outline. Any distribution or publishing of this material (e.g. uploading material to a third-party website) is strictly prohibited under the law unless the student has obtained the copyright owner's prior written consent. Any violation of copyright law or the Intellectual Property Policy, if proven, may be subject to sanction as academic misconduct, and/or under the Student Conduct Policy.

24. Student Course Feedback Surveys

Student evaluation of teaching is a highly valued and helpful mechanism for monitoring the quality of Ontario Tech University’s programs and instructional effectiveness. To that end, course evaluations are administered by an external company in an online, anonymous process during the last few weeks of classes. Students are encouraged to participate actively in this process and will be notified of the dates. Notifications about course evaluations will be sent via e-mail, and posted on Canvas, Weekly News, and signage around the campus.

University Response to COVID-19

The government response to the COVID-19 pandemic is continually evolving. As new information becomes available from federal and provincial public health authorities, the Province of Ontario and the Regional Municipality of Durham, Ontario Tech University will remain nimble and prepared to respond to government orders, directives, guidelines and changes in legislation to ensure the health and safety of all members of its campus community. In accordance with public health recommendations, the university may need to adjust the delivery of course instruction and the availability and delivery mode of campus services and co-curricular opportunities. Ontario Tech University appreciates the understanding and flexibility of our students, faculty and staff as we continue to navigate the pandemic and work together to demonstrate our strong commitment to academic, research and service excellence during these challenging and unprecedented times.

The Accessibility for Ontarians with Disabilities Act (AODA) standards have been considered in the development of this model course template and it adheres to the principles outlined in the University’s Accessibility Policy.

Appendix A – Dealing with Course Concerns

Dealing with Course Concerns: Navigating University Processes

Start with your professor

Suppose you are frustrated with some element of the course organization. Or maybe you disagree with how an assignment was graded. Or perhaps you are struggling to understand a concept. **Your first step is always to talk to your professor.** Set up an appointment. TALK with your professor to ensure clarity in communication.

Ongoing concerns or struggling with your studies

Our Academic Advisors are amazing. They can offer support and point you to resources to assist you with your studies and with other challenges, including anxiety, stress, and concerns about your courses.

Unresolved concerns about grades

If your conversation with your professor does not resolve concerns or questions you have about a grade on a test or assignment, **you can appeal the grade**. At the end of the term, file a Request for a Grade Reappraisal. Your request will be assessed by a neutral, independent faculty member.

Course-related concerns and feedback

The end-of-term course evaluations give you an opportunity to share your feedback about a course. **The course evaluations are taken seriously by the Faculty**, and you should use them to share what worked in the course and what didn't.

More questions about these processes?

Reach out to your advisor! FBITAdvising@ontariotechu.ca

Faculty of Business and Information Technology

MITS 5620G: Special Topics in IT Management – AI & Security

Course outline for **SPRING/SUMMER 2021**

1. Course Details & Important Dates*

Term	Course Type	Day	Time	Location	CRN #
Spring/Summer 2021	Lecture - Online	Tuesdays	6:10 PM – 9:0-0 PM	SYNC - Online	10904

Classes Start	Classes End	Last day to drop course without academic consequence	Final Exam Period
Spring/Summer term: May 3, 2021	August 3, 2021	May 31, 2021	August 5 – 8, 2021

* For other important dates go to: https://ontariotechu.ca/current-students/academics/important-dates-and-deadlines.php

2. Instructor Contact Information

Instructor Name	Office	Phone	Email
Ruba Al Omari	NA	NA	Ruba.alomari@durhamcollege.ca
Office Hours:			

Laboratory/Teaching Assistant Name	Office	Phone	Email
Office Hours:			

3. Course Description

This course introduces the use of artificial intelligence in identifying and predicting cybersecurity threats. Students will learn: the fundamentals of using artificial intelligence in network anomaly detection, malware threat detection, user behavioral analytics for fraud prevention, and detecting email cybersecurity threats; generative adversarial networks and their use in attack and defense scenarios, and the challenges and promises of artificial intelligence in Cybersecurity.

4. Learning Outcomes

On the successful completion of the course, students will be able to:

1. Demonstrate and verbalize a deep understanding of the use of artificial intelligence in predicting security threats
2. Learn how to predict network intrusions and detect anomalies with machine learning algorithms
3. Learn how to detect email threats such as phishing using machine learning algorithms
4. Learn how to detect zero-day and polymorphic malware samples
5. Evaluate the effectiveness of various alternative solutions, using appropriate analysis metrics

5. Course Design

The course is delivered through online class sessions and students must have stable internet connection for the online lectures. Note that this will require access to a specific set of technology tools; access to a laptop/tablet/PC with a built-in or external microphone and camera or web cam.

This course focuses on the use of artificial intelligence (AI) in cybersecurity. It explores the use of machine learning algorithms in detecting threats, network anomaly, spam, malware, and user behavioral analytics for fraud prevention.
The primary teaching method will be class lectures and out of class assignments. The lectures will discuss the course topics listed below, while out of class assignments acquaint students with practical skills and techniques relevant to the disciplines which are discussed in the lectures.

All lecture notes, including student presentations, will be recorded and uploaded to Canvas.

Class attendance is highly recommended, and students must complete all in-class coding exercises in order to understand the concepts and ideas introduced in the class.

6. Outline of Topics in the Course

Lecture #	Date	Time	Topics	Details of topics to be covered in the course, by unit or by week
1	May 4	6:10 pm – 9:00 pm	Introduction to the use of AI and Machine Learning in Cybersecurity	Course Plan
2	May 11	6:10 pm – 9:00 pm	Ham or Spam? Detecting Email Cybersecurity Threats with AI	Assignment#1
3	May 18	6:10 pm – 9:00 pm	Anomaly Detection and Network Traffic Analysis	
4	May 25	6:10 pm – 9:00 pm	Malware Analysis and Threat Detection	Assignment#2
5	June 1	6:10 pm – 9:00 pm	Individual Paper Presentations - I	
6	June 8	6:10 pm – 9:00 pm	Individual Paper Presentations - II	

STUDY BREAK	June 15 – 19, 2021		Study Break, no scheduled academic activities	
7	June 22	6:10 pm – 9:00 pm	Securing User Authentication	Assignment#3
8	June 29	6:10 pm – 9:00 pm	Fraud Prevention with AI Solutions	
9	July 6	6:10 pm – 9:00 pm	Protecting the Consumer Web	
10	July 13	6:10 pm – 9:00 pm	Adversarial Machine Learning	
11	July 20	6:10 pm – 9:00 pm	Final Project Presentations + Group Project Discussion	
12	July 27	6:10 pm – 9:00 pm	Final Project Presentations + Group Project Discussion	
	August 4, 2021		Study break, no scheduled academic activities.	

7. Required Texts/Readings

There is no assigned textbook. All assigned readings and cases will be introduced in the class. A list of recommended readings and references will be provided for each lecture.

Additional readings may be assigned or recommended during the course.

8. Evaluation Method

This course takes a project-based approach to provide experiential learning through its development. Project information will be made available on Canvas after the course starts.

Students will be and evaluated as follows:

Item	Weight (%)
Assignments (3 x 15% each)	45
Individual Paper Presentation	15
Group Project Plan	5
Group Project Report	25
Group Project Presentation	10

Final course grades may be adjusted to conform to program or Faculty grade distribution profiles. Further information on grading can be found at: http://calendar.uoit.ca/content.php?catoid=22&navoid=879#Grading

9. Assignments and Tests

Item	Release Week/Time*	Due Week/Time*	Weight (%)
Assignments (3 x 15% each)	Tuesdays during class time on Weeks 2,4,and 7	Sundays @ 11:59 PM (second Sunday after release)	45
Group Project Plan	Week 1 (In-Class)	Week 4	5
Individual Paper Presentation + Group Project Discussion	Week 1 (In-Class)	Weeks 5 and 6 (In-Class)	15
Group Project Report	Week 1 (In-Class)	Week 10	25
Group Project Presentation	Week 1 (In-Class)	Weeks 11 and 12 (In-Class)	10

*Check Canvas for the exact date and time.

Any issues related to the assignments should be brought to the professor's attention within 5 days of the mark release. No review of assignment's marking will be done after that.

All other term issues must be brought to the professor's attention and be resolved by the last lecture (July 28th). Instructions for the assignments and final project will be available on Canvas. We will be using electronic submission for the labs and final project via Canvas. No other means of submission (e.g., hard copy, email, fax, etc.) will be accepted. Project plan and final project presentations will be presented by students during our class time.

Missed Course Work

Coursework missed for medical or serious personal reasons must be documented and reported to the instructor within three (3) working days of the missed work using an Academic Consideration form. Coursework includes, but is not limited to, quizzes; written assignments; participation; case studies; etc… If missed coursework totals more than 25% of the final grade, this must be documented through the FBIT Academic Advising office. The weight of the missed course component will be reweighted to the next equivalent component (e.g., Assignment#1 mark is carried over to Assignment#2 mark). If you miss coursework and do not notify the instructor within the three (3) working day deadline, you will receive a score of zero on the missed component.

Any student who faces challenges securing their food or housing and believes this may affect their performance in the course is urged to contact studentlife@ontariotechu.ca for support. Furthermore, please notify your professor if you are comfortable in doing so. This will enable them to provide any resources and help that they can.

10. Technology Requirements

To support online learning, the university recommends certain technology requirements for laptops, software and internet connectivity which are available at: https://itsc.ontariotechu.ca/remote-learning.php.

Students experiencing technical difficulties such that they are unable to meet the technology requirements may contact the IT Service Help Desk at: servicedesk@dc-uoit.ca Students experiencing financial difficulties such that they are unable to meet the technology requirements may contact Student Awards and Financial Aid Office at: connect@ontariotechu.ca

By remaining enrolled in this course, you acknowledge that you have read, understand and agree to observe the Recommended Technology Requirements for accessing university online learning resources, including those minimum requirements that are specific to your faculty and program.

11. Sensitive/Offensive Subject Matter

The classroom (both physical and virtual) is intended to provide a safe, open space for the critical and civil exchange of ideas and opinions. Some articles, media and other course materials may contain sensitive content that is offensive and/or disturbing. For example, some articles or videos may contain examples that are applicable to the course subject matter – [e.g. graphical depictions of violence, profanity, human anatomy, sexual acts, matters pertaining to race, gender, or sexuality]. The Course Instructor will try to identify such material and communicate warnings to students in advance of the distribution and use of such materials, affording students the choice to either emotionally prepare for, or not to view or interact with, the content.

12. Student Support

Any student who faces challenges securing their food or housing and believes this may affect their performance in the course is urged to contact studentlife@ontariotechu.ca for support. Furthermore, please notify your professor if you are comfortable in doing so. This will enable them to provide any resources and help that they can.

13. Sexual Violence Support and Education

Ontario Tech is committed to the prevention of sexual violence in all is forms. For any student who has experienced Sexual Violence, Ontario Tech can help. We will make accommodations to cater to the diverse backgrounds, cultures, and identities of students when dealing with individual cases.

If you think you have been subjected to or witnessed sexual violence:

- Reach out to a Support Worker, a specially trained individual authorized to receive confidential disclosures about incidents of sexual violence. Support Workers can offer help and resolution options which can include safety plans, accommodations, mental health support, and more. To make an appointment with a Support Worker, call 905.721.3392 or email studentlife@ontariotechu.ca
- Learn more about your options at: https://studentlife.ontariotechu.ca/sexualviolence/

14. Students with Disabilities

Accommodating students with disabilities at Ontario Tech is a responsibility shared among various partners: the students themselves, SAS staff and faculty members. To ensure that disability-related concerns are properly addressed during this course, students with documented disabilities and who may require assistance to participate in this class are encouraged to speak with me as soon as possible. **Students who suspect they have a disability that may affect their participation in this course are advised to go to Student Accessibility Services (SAS) as soon as possible.** Maintaining communication and working collaboratively with SAS and faculty members will ensure you have the greatest chance of academic success.

When on campus access is allowed, students taking courses on north Oshawa campus can visit Student Accessibility Services in the Student Life Building, U5, East HUB (located in the Founders North parking lot). Students taking courses on the **downtown Oshawa campus** can visit Student Accessibility Services in the 61 Charles St. Building, 2nd Floor, Room DTA 225 in the Student Life Suite.

Disability-related and accommodation support is available for students with mental health, physical, mobility, sensory, medical, cognitive, or learning challenges. Office hours are 8:30am-4:30pm, Monday to Friday, closed Wednesday's 8:30am – 10:00am. For more information on services provided, you can visit the SAS website at https://studentlife.ontariotechu.ca/services/accessibility/index.php. Students may contact Student Accessibility Services by calling 905-721-3266, or email studentaccessibility@ontariotechu.ca.

When on campus access is allowed, students who require the use of the Test Centre to write tests, midterms, or quizzes MUST register online using the SAS test/exam sign-up module, found here https://disabilityservices.ontariotechu.ca/uoitclockwork/custom/misc/home.aspx. Students must sign up for tests, midterms, or quizzes AT LEAST seven (7) days before the date of the test.

Students must register for final exams by the registration deadline, which is typically two (2) weeks prior to the start of the final examination period. SAS will notify students of the registration deadline date.

15. Professional Conduct (if applicable)

Ontario Tech University is a community that values and promotes respect, integrity, diversity and accountability among all members of the university. These values can only be achieved in an environment that supports and protects the safety and security of its members. The Ontario Tech University Policy on Student Conduct defines and guides standards of student behaviour at the university to uphold these values and ensure that behaviour contrary to these standards are dealt with in a manner that is fair, open and effective.

Additional information on professional suitability can be found at http://calendar.uoit.ca/content.php?catoid=22&navoid=879#Academic_conduct

16. Academic Integrity

Students and faculty at Ontario Tech University share an important responsibility to maintain the integrity of the teaching and learning relationship. This relationship is characterized by honesty, fairness and mutual respect for the aim and principles of the pursuit of education. Academic misconduct impedes the activities of the university community and is punishable by appropriate disciplinary action.

Students are expected to be familiar with and abide by Ontario Tech University's regulations on Academic Conduct which sets out the kinds of actions that constitute academic misconduct, including plagiarism, copying or allowing one's own work to copied, use of unauthorized aids in examinations and tests, submitting work prepared in collaboration with another student when such collaboration has not been authorized, among other academic offences. The regulations also describe the procedures for dealing with allegations, and the sanctions for any finding of academic misconduct, which can range from a resubmission of work to a failing grade to permanent expulsion from the university. A lack of familiarity with these regulations on academic conduct does not constitute a defense against its application. This information can be found at https://usgc.ontariotechu.ca/policy/policy-library/policies/academic/academic-conduct-and-professional-suitability-policy-undergraduate.php

Extra support services are available to all Ontario Tech University students in academic development, study skills, counseling, and peer mentorship. More information on student support services can be found at https://studentlife.ontariotechu.ca/services/academic-support/index.php

17. Turnitin (if applicable)

Ontario Tech University and faculty members reserve the right to use electronic means to detect and help prevent plagiarism. Students agree that by taking this course all assignments are subject to submission for textual similarity review by Turnitin.com. Assignments submitted to Turnitin.com will be included as source documents in Turnitin.com's restricted access database solely for the purpose of detecting plagiarism in such documents. The instructor may require students to submit their assignments electronically to Turnitin.com or the instructor may submit questionable text on behalf of a student. The terms that apply to Ontario Tech University's use of the Turnitin.com service are described on the Turnitin.com website.

Students who do not wish to have their work submitted to Turnitin.com must provide with their assignment at the time of submission to the instructor a signed Turnitin.com Assignment Cover sheet: https://shared.uoit.ca/shared/department/academic-integrity/Forms/assignment-cover-sheet.pdf

18. Final Examinations (if applicable)

Final examinations are held during the final examination period at the end of the semester and **when on campus access is allowed,** may take place in a different room and on a different day from the regularly scheduled class. Check the published Examination Schedule for a complete list of days and times.

Students are required to show their Student ID card (campus ID) when **in-person examinations are allowed.** Students are advised to obtain their Student ID Card well in advance of the examination period as they will not be able to write their examinations without it. More information on ID cards can be found at https://registrar.ontariotechu.ca/campus-id/index.php.

Students who are unable to write a final examination when scheduled due to religious publications may make arrangements to write a deferred examination. These students are required to submit a Request for Accommodation for Religious Obligations to the Faculty concerned as soon as possible and no later than three weeks prior to the first day of the final examination period.

Further information on final examinations can be found at https://usgc.ontariotechu.ca/policy/policy-library/policies/academic/procedures-for-final-examination-administration.php

19. Freedom of Information and Protection of Privacy Act

The following is an important notice regarding the process for submitting course assignments, quizzes, and other evaluative material in your courses in the Faculty of Business and IT.

Ontario Tech University is governed by the Freedom of Information and Protection of Privacy Act ("FIPPA"). In addition to providing a mechanism for requesting records held by the university, this legislation also requires that the University not disclose the personal information of its students without their consent.

FIPPA's definition of "personal information" includes, among other things, documents that contain both your name and your Banner (student) ID. For example, this could include graded test papers or assignments. To ensure that your rights to privacy are protected, the Faculty of [Insert Faculty name] encourages you to use only your Banner ID on assignments or test papers being submitted for grading. This policy is intended to prevent the inadvertent disclosure of your information where graded papers are returned to groups of students at the same time. If you still wish to write both your name and your Banner ID on your tests and assignments, please be advised that Ontario Tech University will interpret this as an implied consent to the disclosure of your personal information in the normal course of returning graded materials to students.

If you have any questions or concerns relating to the new policy or the issue of implied consent addressed above, please contact accessandprivacy@ontariotechu.ca

Notice of Collection and Use of Personal Information

Throughout this course, personal information may be collected through the use of certain technologies under the authority of the *University of Ontario Institute of Technology Act, SO*

2002, c. 8, Sch. O. and will be collected, protected, used, disclosed and retained in compliance with Ontario's *Freedom of Information and Protection of Privacy Act R.S.O. 1990, c. F.31.*

This course may use the following technologies that may collect, use, disclose and retain personal information (including images) for the purposes described below; according to the instructor:

- Respondus Monitor and Proctortrack to maintain academic integrity for examinations;
- Google Meet and Kaltura Virtual Classroom to facilitate remote instruction and interactive learning;
- Peer-shared applications, services or technologies that may be reviewed, assessed, or used as part of coursework.
- Other applications, services, or technologies that support or enhance online learning that include, but are not limited to, others indicated by the instructor.

For more information relating to these technologies, we encourage you to visit: https://tlc.ontariotechu.ca/learning-technology/index.php Questions regarding personal information may be directed to: Ontario Tech University Access and Privacy Office, 2000 Simcoe Street North, Oshawa, ON L1G 0C5, email: accessandprivacy@ontariotechu.ca.

By remaining enrolled in this course, you acknowledge that you have read, understand, and agree to the terms and conditions under which the technology provider(s) may collect, use, disclose and retain your personal information. You agree to the university using the technologies and using your personal information for the purposes described in this course outline.

20. Freedom of Expression

Pursuant to Ontario Tech's Freedom of Expression Policy all students are encouraged to express ideas and perspectives freely and respectfully in university space and in the online university environment, subject to certain limitations. Students are reminded that the limits on Freedom of Expression include speech or behaviour that: is illegal or interferes with the university's legal obligations; defames an individual or group; constitutes a threat, harassment or discrimination; is a breach of fiduciary, contractual, privacy or confidentiality obligations or commitments; and unduly disrupts and interferes with the functioning of the university. In the context of working online, different forms of communication are used. Where permitted, students using "chat" functions or other online forms of communication are encouraged to ensure that their communication complies with the Freedom of Expression Policy.

21. Student Course Feedback Surveys

Student evaluation of teaching is a highly valued and helpful mechanism for monitoring the quality of Ontario Tech University's programs and instructional effectiveness. To that end, course evaluations are administered by an external company in an online, anonymous process during the last few weeks of classes. Students are encouraged to participate actively in this process and will be notified of the dates. Notifications about course evaluations will be sent via e-mail, and posted on Canvas, Weekly News, and signage around the campus.

University Response to COVID-19

The government response to the COVID-19 pandemic is continually evolving. As new information becomes available from federal and provincial public health authorities, the Province of Ontario and the Regional Municipality of Durham, Ontario Tech University will remain nimble and prepared to respond to government orders, directives, guidelines and changes in legislation to ensure the health and safety of all members of its campus community. In accordance with public health recommendations, the university may need to adjust the delivery of course instruction and the availability and delivery mode of campus services and co-curricular opportunities. Ontario Tech University appreciates the understanding and flexibility of our students, faculty and staff as we continue to navigate the pandemic and work together to demonstrate our strong commitment to academic, research and service excellence during these challenging and unprecedented times.

The Accessibility for Ontarians with Disabilities Act (AODA) standards have been considered in the development of this model course template and it adheres to the principles outlined in the University's Accessibility Policy.

UNIVERSITY™
OF ONTARIO
INSTITUTE OF TECHNOLOGY

Faculty of Science

CSCI 5010G – Survey of Computer Science Research Topics & Methods

Course outline for Fall 2016

1. Course Details & Important Dates*

Course Type	Day	Time	Location
Lecture	Tues.	2:10pm – 5:00pm	ERC1094

* for other important dates go to: www.uoit.ca >Current Students >Important Dates and Deadlines

2. Instructor Contact Information

Instructor Name	Office	Email
Dr. Jeremy S. Bradbury	UA4016	jeremy.bradbury@uoit.ca
Office Hours: Fri. 11:00am-12:00pm, or by appointment.		

3. Course Description

CSCI 5010G – Survey of Computer Science Research Topics and Methods. This course is a survey of some of the main research topics in computer science and the corresponding computer science research methods. Topics covered vary from year to year and may include digital media, computer graphics, human-computer interaction, computer networks, security, health informatics, databases and software design. Research methods covered include library methods, topic analysis, data management, technical writing, presentations, evaluation methods and peer review. This course includes guest lectures by experts in the research topics covered. Credit hours: 3

5. Course Design

Survey of Computer Science is a required course for all Computer Science MSc and PhD students. The course is designed as a comprehensive survey of Computer Science research areas and research methods that provides a strong research foundation for any student pursing graduate studies in Computer Science. The research areas/topics surveyed will be presented by weekly guest lectures from graduate faculty in the Computer Science program. In addition to surveying Computer Science topics the course will also survey Computer Science research methods. Each week half of the lecture will be devoted to introducing a new research method. Students will be evaluated by applying the covered research methods to their own area of interest within Computer Science.

6. Outline of Topics in the Course

- State-of-the-art research examples from the Computer Science graduate program fields:
  - Digital Media
  - Information Systems
  - Networks and IT Security
  - Software Design
- Research Methods to address the following questions:
  - How do I learn about my chosen field of research?
    - Finding research papers and creating an annotated bibliography
    - Conducting literature reviews, classifications and taxonomies
  - How do I select a research topic?
    - Conducting a topic analysis
    - Technical writing
  - How do I write a thesis proposal?
    - The structure of a thesis proposal
    - Defining a research hypothesis
    - Proposing a methodology and understanding the possible outcomes
  - Is there a right way to manage my research?
    - Research logs
    - Research meetings – agendas, notes
    - Backing up data! – The benefit of version control systems
  - How do I evaluate my research work?
    - Evaluation methods for computer science research tools and techniques
    - Evaluation methods for computer science research involving human subjects
    - The importance of reproducibility, threats to validity
    - Conducting ethical research
  - How do I write up and defend my thesis?
    - The structure of a thesis proposal
    - Advice on obtaining feedback from your supervisor and committee
  - How do I publish and disseminate my research?
    - Different kinds of research publication venues – workshops, conferences, journals, books
    - Publication quantity vs. quality – understanding publication metrics, citation counts, etc.
    - The peer review process and how to review a paper
    - Oral communication and research presentations

7. Required Texts/Readings

Textbooks.

Writing the Doctoral Dissertation: A Systematic Approach, 3/E
by Gordon B. Davis & Clyde A. Parker

Writing for Computer Science, 3/E
by Justin Zobel

Online Resources.

Online articles and websites will be used to supplement the textbook. Links to all online resources will be posted on the course website.

8. Evaluation Method

Annotated Bibliography	15%
Paper	25%
Peer Review	15%
Presentations	25%
Attendance & Participation	20%

All students are required to attend 80% of the lectures and 80% of the Computer Science seminars in order to pass the course.

9. Assignments and Tests

The schedule for course deliverables is as follows:

- Presentation 1 –Oct. 11, 2016
- Annotated Bibliography – mid Oct. 2016
- Paper (preliminary submission) – mid. Nov. 2016
- Peer Review – late Nov. 2016
- Paper (final submission) – early Dec. 2016
- Presentation 2 – Nov. 29, 2016

10. Students with Disabilities

Accommodating students with disabilities at UOIT is a responsibility shared among various partners: the students themselves, SAS staff and faculty members. To ensure that disability-related concerns are properly addressed during this course, students with documented disabilities and who may require assistance to participate in this class are encouraged to speak with me as soon as possible. **Students who suspect they have a disability that may affect their participation in this course are advised to go to Student Accessibility Services (SAS) as soon as possible.** Maintaining communication and working collaboratively with SAS and faculty members will ensure you have the greatest chance of academic success.

Students taking courses on the North Campus Location can visit Student Accessibility Services in the U5 Building located in the Student Life Suite
Students taking courses on the Downtown Oshawa Campus Location can visit Student Accessibility Services in the 61 Charles St. Building, 2nd Floor, Room DTA 225 in the Student Life Suite.

Disability-related support and accommodation support is available for students with mental health, physical, mobility, sensory, medical, cognitive, or learning challenges. Office hours are 8:30am-4:30pm, Mon-Fri. For more information on services provided, you can visit the SAS website at http://uoit.ca/studentaccessibility

Students may contact Student Accessibility Services by calling 905-721-3266, or email studentaccessibility@uoit.ca

Students who require the use of the Test Centre to write tests, midterms, or quizzes MUST register online using the SAS test/exam sign-up module, found here www.uoit.ca/SASexams. Students must sign up for tests, midterms or quizzes AT LEAST seven (7) days before the date of the test.
Students must register for final exams by the registration deadline, which is typically 2 weeks prior to the start of the final examination period. SAS will notify students of the registration deadline date.

12. Academic Integrity

Students and faculty at UOIT share an important responsibility to maintain the integrity of the teaching and learning relationship. This relationship is characterized by honesty, fairness and mutual respect for the aim and principles of the pursuit of education. Academic misconduct impedes the activities of the university community and is punishable by appropriate disciplinary action.

Students are expected to be familiar with and abide by UOIT's regulations on Academic Conduct (Section 5.15 of the Academic Calendar) which sets out the kinds of actions that constitute academic misconduct, including plagiarism, copying or allowing one's own work to copied, use of unauthorized aids in examinations and tests, submitting work prepared in collaboration with another student when such collaboration has not been authorized, among other academic offences. The regulations also describe the procedures for dealing with allegations, and the sanctions for any finding of academic misconduct, which can range from a resubmission of work to a failing grade to permanent expulsion from the university. A lack of familiarity with UOIT's regulations on academic conduct does not constitute a defense against its application.

Further information about academic misconduct can be found in the Academic Integrity link on your laptop. Extra support services are available to all UOIT students in academic development, study skills, counseling, and peer mentorship. More information on student support services can be found in the Academic Calendar (Section 8).

15. Freedom of Information and Protection of Privacy Act

The following is an important notice regarding the process for submitting course assignments, quizzes and other evaluative material in your courses in the Faculty of Science.

As you may know, UOIT is governed by the *Freedom of Information and Protection of Privacy Act* ("FIPPA"). In addition to providing a mechanism for requesting records held by the university, this legislation also requires that UOIT not disclose the personal information of its students without their consent.

FIPPA's definition of "personal information" includes, among other things, documents that contain both your name and your Banner ID. For example, this could include graded test papers or assignments. To ensure that your rights to privacy are protected, the Faculty of Science encourages you to use only your Banner ID on assignments or test papers being submitted for grading. This policy is intended to prevent the inadvertent disclosure of your information where graded papers are returned to groups of students at the same time. If you still wish to write both your name and your Banner ID on your tests and assignments, please be advised that UOIT will interpret this as an implied consent to the disclosure of your personal information in the normal course of returning graded materials to students.

If you have any questions or concerns relating to the new policy or the issue of implied consent addressed above, please contact accessandprivacy@uoit.ca

16. Course Evaluations

Student evaluation of teaching is a highly valued and helpful mechanism for monitoring the quality of UOIT's programs and instructional effectiveness. To that end, course evaluations are administered by an external company in an online, anonymous process during the last few weeks of classes. Students are encouraged to participate actively in this process and will be notified of the dates. Notifications about course evaluations will be sent via e-mail, and posted on Blackboard, Weekly News and signage around the campus.

Ontario Tech University acknowledges the lands and people of the Mississaugas of Scugog Island First Nation. We are thankful to be welcomed on these lands in friendship. The lands we are situated on are covered under the Williams Treaties and the traditional territory of the Mississaugas, a branch of the greater Anishinaabeg Nation, including Algonquin, Ojibway, Odawa and Pottawatomi. These lands remain home to a number of Indigenous nations and people.

We acknowledge this land out of respect for the Indigenous nations who have cared for Turtle Island, also called North America, from before the arrival of settler peoples until this day. Most importantly, we remember the history of these lands has been tainted by poor treatment and a lack of friendship with the First Nations who call them home.

This history is something we are all affected by as we are all treaty people in Canada. We all have a shared history to reflect on, and each of us is affected by this history in different ways. Our past defines our present, but if we move forward as friends and allies, then it does not have to define our future.

FACULTY OF BUSINESS AND IT

Fundamentals of Cybersecurity
2024-25

1. Course Details & Important Dates*

Term	Course Type	Day	Time	Location	CRN#
2024-25	Online				

Classes Start	Classes End	**Last day to drop course without academic consequence**	Final Exam Period

* Visit Ontario Tech's Important Dates and Deadlines for other dates.

2. Instructor Contact Information

Instructor Name	Office	Phone	Email
Stephen Marsh			Canvas Email
Office Hours: by appointment			

Laboratory/Teaching Assistant Name	Office	Phone	Email
Office Hours: by appointment			

3. Course Description

This course introduces a concise review of the foundations of IT Security. It is designed as a collection of six modules using asynchronous online delivery method, covering the following topics:

Module 1: Fundamentals of Networking
Module 2: Foundations of Cryptography
Module 3: Authentication and Identity Management
Module 4: Network attacks and malicious codes
Module 5: Intrusion Detection and Protection
Module 6: IT Forensics

Each module includes approximately 8-10 hours of video lectures and reading material, and is expected to be completed over four weeks.

4. Learning Outcomes

On successful completion of the course, students will be able to:

- Describe the architecture of today's Internet; identify and differentiate TCP/IP layers and protocols; and analyze various communication technologies.
- Explain the basic concepts and theoretical underpinnings of symmetric cryptography, public-key cryptography and hash functions.
- Explain the basic concepts of authentication and access control, and differentiate various techniques.
- Describe different types of malicious software, and explain how OS and software vulnerabilities can be exploited by malware and network attacks.
- Understand Intrusion Detection Systems (IDSs), Anomaly Detection and Behavior Analysis, Security Information and Event Management Systems and Deception Technologies.
- Describe how to implement a computer forensics incident-response strategy, and how to conduct proper IT forensics and investigation.

5. Course Design

The course will be modular, with 6 modules over two semesters, each focusing on a different aspect of cybersecurity. Each module has its own assessment and a grade of 70% per module is required to pass the entire course. The course is delivered entirely online, with recorded lectures, extensive office hours available per week, an online synchronous (1.5 hour) exam per module, and readings in the form of academic papers and an Open Educational Resource.

Students requiring assistance are encouraged to speak to their instructor during class or during office hours. Should you wish to meet with the instructor outside of office hours, please email first to make an appointment. Students should get into the habit of making and keeping business appointments. Should you fail to attend or cancel the appointment at least 24 hours in advance, you will lose the right to book another appointment.

Email is commonly used by students to communicate with their instructor. However, it does limit the effectiveness of the communications and may not be the best way for instructors to answer student questions, especially those requiring an explanation of concepts covered in this course or some personal concerns. Therefore, the instructor may request a telephone call or personal/online meeting. *Your instructor will inform you as to their expectations about emails.*

6. Outline of Topics in the Course

Tentative Course Schedule, Fall 2024 and Winter 2025			
Module/Week #	**Date**	**Topics**	**Material Covered**
1/1		Fundamentals of Networking	Data communication Fundamentals
1/2			Network models and architectures
1/3			Emerging trends in networking
1/4			
			Module assessment
2/1		Foundations of Cryptography	Random bit generation and stream ciphers
2/2			Advanced Encryption Standard
2/3			Secure Hash Algorithm (SHA-2)
2/4			Message Authentication Codes Public-Key Certificates
			Module assessment
3/1			User Authentication
3/2		Authentication and Identity Management	Access control
3/3			OS Security (Windows, Linux) Mobile Authentication and Zero Trust
3/4			Audits and logs
			Module assessment
Semester Break			
4/1			Denial of Service Attacks and Botnets
4/2			Malicious Software
4/3			
4/4			Disaster Recovery
			Module assessment
5/1		Intrusion Detection and Prevention	Intrusion Detection Systems
5/2			Firewalls and Network Security
5/3			
5/4			AI and IDS/IDP
			Module assessment
6/1		IT Forensics	Introduction to Digital Forensics Digital Investigation Fundamentals
6/2			Volume Analysis File System Analysis

6/3			Operating System Forensics
6/4			Mobile forensics
			Module assessment
			Final presentation (online, recorded)

***Important Notes:** Adjustment of scheduled lectures might be made in accordance with any unforeseen circumstances during the semester.*

7. Required Readings

An Open Educational Resource is available for the course which contains the reading material for each module.

Additional readings may be assigned or recommended during the course.

8. Evaluation Method

Each module will have a final assessment in its fourth (4th) week, which usually takes the form of an exam. To pass the course, each assessment must be passed with at least 70% in the assessment. The final grade is an average of each of the modules amounting to 90% of the final grade of the course, with an additional 10% for an online recorded final presentation and engagement, due date end of final module.

A within-exam grade of 70% (10.5/15) or higher is necessary **in each module** in order to pass the entire course.

Final course grades may be adjusted to conform to program or Faculty grade distribution profiles. Further information on grading can be found under Academic Regulations at: Ontario Tech's Academic regulations

9. Assignments and Tests

Each module has a final online assessment (usually in the form of an exam) of one hour which is worth 15% of the final grade for the course. In order to pass the course it is necessary to achieve a grade of 70% (or 10.5 out of 15) in each of these exams. The assessment will normally be held during an online synchronous session in the final week of each module.

Missed In-Term Course Work

A request for consideration for missed course work worth 20% or less of the final grade must be documented and reported to the instructor in writing within the deadlines specified in the Procedures for Consideration of Missed In-Term Course Work and Examinations. Course work includes, but is not limited to: quizzes, written assignments (problem set), participation, case studies, etc. If missed coursework totals more than 20% of the final grade, the request for consideration must be submitted to the Faculty of Business and IT Advising Office and to the course instructor in writing using the Academic Consideration Form, along with supporting documentation. The request must be submitted within the deadlines specified in the Procedures for Consideration of Missed In-Term Course Work and Examinations. If approved, the extended deadline of the missed course component will be granted. If a student misses coursework and does not follow the procedure above, they will receive a score of zero on the missed component.

All forms can also be found through MyOntarioTech or on the Ontario Tech University website.

For information on how missed/late assignments and medical excuses are managed, please refer to the university's revised *Procedures for Consideration of Missed In-Term Course Work and Examinations*

10. Technology Requirements and Learning Management System Information

Ontario Tech uses *Canvas*™ as its learning management system (LMS). Access to the LMS is limited to students formally registered in courses. That access is for the duration of the semester **and for an additional 120 days once the semester is over**. Students are strongly encouraged to download any/all relevant course material during that access period. Any requests for access post this period must be made in writing to the instructor/faculty member responsible for the course.

To support online learning, the university recommends certain technology requirements for laptops, software and internet connectivity which are available at: Ontario Tech's Remote Learning Policies.

Students experiencing technical difficulties such that they are unable to meet the technology requirements may contact the IT Service Help Desk at: servicedesk@dc-uoit.ca
Students experiencing financial difficulties such that they are unable to meet the technology requirements may contact Student Awards and Financial Aid Office at: connect@ontariotehu.ca

By remaining enrolled in this course, you acknowledge that you have read, understand and agree to observe the Recommended Technology Requirements for accessing university online learning resources, including those minimum requirements that are specific to your faculty and program.

11. Sensitive/Offensive Subject Matter

The classroom (both physical and virtual) is intended to provide a safe, open space for the critical and civil exchange of ideas and opinions. Some articles, media and other course materials may contain sensitive content that is offensive and/or disturbing. For example, some articles or videos may contain graphical depictions of violence, profanity, human anatomy, sexual acts, matters pertaining to race, gender, or sexuality. The Course Instructor will try to identify such material and communicate warnings to students in advance of the distribution and use of such materials, affording students the choice to either emotionally prepare for, or not to view or interact with, the content.
Disclaimer: "The content you are about to view contains sensitive subject matter that may be considered offensive and/or disturbing to some viewers. By viewing and/or interacting with the content you acknowledge and agree that it is your decision to view and interact with the content and to take the risk that you will experience a negative emotional response or reaction to the nature of the content."

12. Student Support

Any student who faces challenges securing their food or housing and believes this may affect their performance in the course is urged to contact studentlife@ontariotechu.ca for support. Furthermore, please notify your professor if you are comfortable in doing so. This will enable them to provide any resources and help that they can.

13. Student Sexual Violence Support and Education

Ontario Tech is committed to the prevention of sexual violence in all its forms. For any student who has experienced Sexual Violence, Ontario Tech can help. We will make accommodations to cater to the diverse backgrounds, cultures, and identities of students when dealing with individual cases.

If you think you have been subjected to or witnessed sexual violence:

- Reach out to the gender-based case specialist in the Human Rights office, a specially trained individual authorized to receive confidential disclosures about incidents of sexual violence. The Human Rights Office will make support services, including counselling, access or referrals to medical services, safety planning and accommodations, available to Students affected by an Incident of Sexual Violence. Book a consultation with the Case Specialist for more information.

Learn more about your options at: Ontario Tech's Policy on Sexual Violence and Support Information.

14. Students with Disabilities

Ontario Tech University is committed to promoting an environment where everyone has an equal opportunity to contribute to their fullest potential. Students who require accommodation for a disability are advised to contact Student Accessibility Services (SAS) as soon as possible. Accommodation decisions will be made in accordance with the Ontario Human Rights Code. Accommodations will be consistent with and supportive of the essential requirements of courses and programs, and provided in a way that respects the dignity of students with disabilities and encourages integration and equality of opportunity. Reasonable academic accommodation may require instructors to exercise creativity and flexibility in responding to the needs of students with disabilities while maintaining integrity.

Disability-related and accommodation support is available for students with mental health, physical, mobility, sensory, medical, cognitive, or learning challenges. Office hours are 8:30am-4:30pm, Monday, Tuesday, Thursday, and Friday, Wednesday's 10:00 am to 4:30. Please note they are closed each day between noon and 1:00 pm. For more information on services provided, you can visit the SAS website at Ontario Tech's Student Accessibility Services (SAS). Students may contact Student Accessibility Services by calling 905-721-3266, or email studentaccessibility@ontariotechu.ca.

Students who require the use of the Test Centre to write tests, midterms, or quizzes MUST register online using the SAS test/exam sign-up module, found here Registration Link to write examinations in SAS at Ontario Tech. Students must sign up for tests, midterms, or quizzes **AT LEAST seven (7) working days before the date of the test.**

Students must register for final exams no later **than 3 weeks prior to the start of the final examination period**. The final examination period is given at Ontario Tech University's Important dates and deadlines.

15. Professional Suitability (if applicable)

Ontario Tech University is a community that values and promotes respect, integrity, diversity and accountability among all members of the university. These values can only be achieved in an environment that supports and protects the safety and security of its members. The Ontario Tech University Policy on Student Conduct defines and guides standards of student behaviour at the university to uphold these values and ensure that behaviour contrary to these standards are dealt with in a manner that is fair, open and effective.

The Faculty of Business & IT has the following expectations related to professionalism for all its community members, including without limitation, students, Staff, and Faculty:

- **Respect, civility, and courtesy:** Community members are expected to treat each other with respect, civility, and courtesy both in and outside of the classroom. Rudeness, profanity, insults, harassment, and class disruptions are unacceptable.
- **Critique ideas, not the people who raise the ideas:** Discussions, debates, and the exchange of ideas are normal parts of life in an academic community. Community members are expected to engage in discussions, debates, and the exchange of ideas in respectful ways, even while vigorously advocating for one's perspective.
- **Talk *to* those with whom you have a complaint, not *about* them.** When community members have disputes, complaints, and/or concerns about another community member, they are expected to do their best to address the matter directly and informally with the other member, provided that it is safe to do so.
- **Special obligations:** Community members in positions of authority have special obligations to demonstrate respect, civility, and professionalism and to encourage the development of these values within the FBIT community.

The *Professional Suitability* policy can be found at Ontario Tech's Professional Suitability Policy and the related procedures are hosted at Ontario Tech's Professional Suitability Procedures.

16. Academic Integrity

Students and faculty at Ontario Tech University share an important responsibility to maintain the integrity of the teaching and learning relationship. This relationship is characterized by honesty, fairness and mutual respect for the aim and principles of the pursuit of education. Academic misconduct impedes the activities of the university community and is punishable by appropriate disciplinary action.

Students are expected to be familiar with and abide by Ontario Tech University's regulations on Academic Conduct which sets out the kinds of actions that constitute academic misconduct, including plagiarism, copying or allowing one's own work to copied, use of unauthorized aids in examinations and tests, submitting work prepared in collaboration with another student when such collaboration has not been authorized, among other academic offences. The regulations also describe the procedures for dealing with allegations, and the sanctions for any finding of academic misconduct, which can range from a resubmission of work to a failing grade to permanent expulsion from the university. A lack of familiarity with these regulations on academic conduct does not constitute a defense against its application. Please note that generative artificial intelligence (GAI) tools should not be utilized without advance, specific written approval by the faculty member teaching the course.

More information can be found at Ontario Tech's Academic Integrity Policy.

Extra support services are available to all Ontario Tech University students in academic development, study skills, counseling, and peer mentorship. More information on student support services can be found at Academic Support at Ontario Tech.

17. Turnitin (if applicable)

Ontario Tech University and faculty members reserve the right to use electronic means to detect and help prevent plagiarism. Students agree that by taking this course all assignments are subject to submission for textual similarity review by Turnitin.com. Assignments submitted to Turnitin.com will be included as source documents in Turnitin.com's restricted access database solely for the purpose of detecting plagiarism in such documents. The instructor may require students to submit their assignments electronically to Turnitin.com or the instructor may submit questionable text on behalf of a student. The terms that apply to Ontario Tech University's use of the Turnitin.com service are described on the Turnitin.com website.

Students who do not wish to have their work submitted to Turnitin.com must provide with their assignment at the time of submission to the instructor a signed Turnitin.com Assignment Cover sheet: Signed Turnitin Coversheet to Withdraw Permission to Submit Work.

18. Online Test and Exam Proctoring (Virtual Proctoring)

Ontario Tech University will conduct virtual monitoring of examinations in accordance with Ontario privacy legislation and all approved policy instruments.

19. Final Examinations (if applicable)

Final examinations are held during the final examination period at the end of the semester and may take place in a different room and on a different day from the regularly scheduled class. Check the published Examination Schedule for a complete list of days and times.

Students are required to show their valid physical or digital Ontario Tech University student photo ID card (campus ID), or a valid government issued photo ID that is in English when writing an **in-person examination.** Students are advised to obtain their Student ID Card well in advance of the examination period as they will not be able to write their examinations without it. More information on ID cards can be found at Information on Ontario Tech's Student ID Cards.

Students who are unable to write a final examination when scheduled due to religious publications may make arrangements to write a deferred examination. These students are required to submit an Academic Consideration form to the applicable Faculty as soon as possible and no later than three weeks prior to the first day of the final examination period.

Further information on final examinations can be found in the university's *Procedures for Final Examination Administration* Ontario Tech's Procedures for Final Examinations and in the Procedures for Consideration of Missed In-Term Course Work and Examinations.

20. Freedom of Information and Protection of Privacy Act

The following is an important notice regarding the process for submitting course assignments, quizzes, and other evaluative material in your courses in the Faculty of Business and IT.

Ontario Tech University is governed by the Freedom of Information and Protection of Privacy Act ("FIPPA"). In addition to providing a mechanism for requesting records held by the university, this legislation also requires that the University not disclose the personal information of its students without their consent.

FIPPA's definition of "personal information" includes, among other things, documents that contain both your name and your Banner (student) ID. For example, this could include graded test papers or assignments. To ensure that your rights to privacy are protected, the Faculty of Business and IT encourages you to use only your Banner ID on assignments or test papers being submitted for grading. This policy is intended to prevent the inadvertent disclosure of your information where graded papers are returned to groups of students at the same time. If you still wish to write both your name and your Banner ID on your tests and assignments, please be advised that Ontario Tech University will interpret this as an implied consent to the disclosure of your personal information in the normal course of returning graded materials to students.

If you have any questions or concerns relating to the new policy or the issue of implied consent addressed above, please contact accessandprivacy@ontariotechu.ca

Notice of Collection and Use of Personal Information
Throughout this course, personal information may be collected through the use of certain technologies under the authority of the *University of Ontario Institute of Technology Act, SO 2002, c. 8, Sch. O.* and will be collected, protected, used, disclosed and retained in compliance with Ontario's *Freedom of Information and Protection of Privacy Act R.S.O. 1990, c. F.31.*

This course will use the following technologies that may collect, use, disclose and retain personal information (including images) for the purposes described below:

- Respondus Monitor and Proctortrack to maintain academic integrity for examinations;
- Google Meet and Kaltura Virtual Classroom to facilitate remote instruction and interactive learning;
- Peer-shared applications, services or technologies that may be reviewed, assessed, or used as part of coursework.
- Other applications, services, or technologies that support or enhance online learning that include, but are not limited to, the following: Internet and Webcam.

For more information relating to these technologies, we encourage you to visit: Educational Technologies used at Ontario Tech.

Questions regarding personal information may be directed to: Ontario Tech University Access and Privacy Office, 2000 Simcoe Street North, Oshawa, ON L1G 0C5, email: accessandprivacy@ontariotechu.ca.

By remaining enrolled in this course, you acknowledge that you have read, understand, and agree to the terms and conditions under which the technology provider(s) may collect, use, disclose and retain your personal information. You agree to the university using the technologies and using your personal information for the purposes described in this course outline.

21. Human Rights and Respect

Ontario Tech University is committed to providing a campus environment in which all University Members are treated with dignity and to fostering a climate of understanding and mutual respect. The University will not tolerate, ignore or condone Discrimination or Harassment by or against anyone. Examples of Harassing behavior include, but are not limited to; bullying, taunting or mocking someone's race or creed, ridiculing an individual's disability, or targeting individuals with unwanted sexual or negative stereotypical comments about one's sex, gender, sexual orientation, gender identity and/or gender expression. Pursuant to Ontario Tech's Respectful Campus Policy, students are reminded of their role in ensuring an equitable and inclusive learning environment. Requirements to refrain from harassment and discrimination apply broadly to on campus activities, e.g., on University property, in the classroom, including in lectures, labs and practicums, and also apply to off-campus activities, e.g. during any organized Ontario Tech class or extra-curricular activity including experiential learning opportunities such as co-op, practicum or during research endeavors, during official Ontario Tech events or using University equipment and technological tools that facilitate remote learning, e.g., class and other chat functions, video conferencing, and electronic mail.

22. Freedom of Expression

Pursuant to Ontario Tech's Freedom of Expression Policy, all students are encouraged to express ideas and perspectives freely and respectfully in university space and in the online university environment, subject to certain limitations. Students are reminded that the limits on Freedom of Expression include speech or behaviour that: is illegal or interferes with the university's legal obligations; defames an individual or group; constitutes a threat, harassment or discrimination; is a breach of fiduciary, contractual, privacy or confidentiality obligations or commitments; and unduly disrupts and interferes with the functioning of the university. In the context of working online, different forms of communication are used. Where permitted, students using "chat" functions or other online forms of communication are encouraged to ensure that their communication complies with the Freedom of Expression Policy.

23. Copyright Notice

All Teaching Materials, as they are defined under Ontario Tech's Intellectual Property policy ("IP Policy"), provided by the instructor throughout the course, including, but not limited to, in whole or in part, course notes, teaching notes, custom books, tutorials, evaluation tools, presentations and examinations are subject to the Copyright Act, R.S.C., 1985, c. C-42 and the IP Policy. Subject to the IP Policy, Teaching Materials are owned by the faculty member, instructor or other third party who creates such works, with a license to the University. The copyright owner(s) reserves all intellectual property rights in and to the foregoing materials. Consistent with the IP Policy, Teaching Materials are intended to be used by Ontario Tech University students registered in the course that is the subject of this course outline for educational purposes only. Any distribution or publishing of this material (e.g., uploading material to a third-party website) by a student is strictly prohibited under the law unless the student has obtained the copyright owner's prior written consent. Any violation of copyright law or the IP Policy, if proven, may be subject to sanction as academic misconduct, and/or under the Student Conduct Policy.

24. Student Course Feedback Surveys

Student evaluation of teaching is a highly valued and helpful mechanism for monitoring the quality of Ontario Tech University's programs and instructional effectiveness. To that end, course evaluations are administered by an external company in an online, anonymous process during the last few weeks of classes. Students are encouraged to participate actively in this process and will be notified of the dates. Notifications about course evaluations will be sent via e-mail, and posted on Canvas, Weekly News, and signage around the campus.

25. AODA

The Accessibility for Ontarians with Disabilities Act (AODA) standards have been considered in the development of this model course template and it adheres to the principles outlined in the University's Accessibility Policy.

Ontario Tech University acknowledges the lands and people of the Mississaugas of Scugog Island First Nation. We are thankful to be welcomed on these lands in friendship. The lands we are situated on are covered under the Williams Treaties and the traditional territory of the Mississaugas, a branch of the greater Anishinaabeg Nation, including Algonquin, Ojibway, Odawa and Pottawatomi. These lands remain home to a number of Indigenous nations and people.

We acknowledge this land out of respect for the Indigenous nations who have cared for Turtle Island, also called North America, from before the arrival of settler peoples until this day. Most importantly, we remember the history of these lands has been tainted by poor treatment and a lack of friendship with the First Nations who call them home.

This history is something we are all affected by as we are all treaty people in Canada. We all have a shared history to reflect on, and each of us is affected by this history in different ways. Our past defines our present, but if we move forward as friends and allies, then it does not have to define our future.

FACULTY OF BUSINESS AND IT

INFR 6020: Usable Security
Course outline for Fall 2024

1. Course Details & Important Dates*

Term	Course Type	Day	Time	Location	CRN#
FALL 2024	Lecture	TBA	TBA	TBA	TBA

Classes Start	Classes End	**Last day to drop course without academic consequence**	Final Exam Period
TBA, 2024	TBA, 2024	TBA	TBA

* Visit Ontario Tech's Important Dates and Deadlines for other dates.

Important Note – Final Exams

The final exam for this course will be run ON CAMPUS during the regular final exam period. If a student cannot attend due to COVID-19 related international travel restrictions you **must email your course instructor ASAP** (as soon as possible) regarding the possibility of alternate arrangements.

2. Instructor Contact Information

Instructor Name	Office	Phone	Email
Dr. Julie Thorpe	UB2016		Julie.thorpe@ontariotechu.ca
Office Hours: TBA			

Laboratory/Teaching Assistant Name	Office	Phone	Email
Office Hours:			

3. Course Description

The security offered by a system can be dramatically influenced by its user interface. This effect has been observed across many cybersecurity applications that aim to help users in tasks such as secure authentication, encryption, system administration, and secure software development. The user interfaces for such applications require not only good usability, but also need to assist users in understanding risks and making decisions, typically in environments and situations where cybersecurity is not their primary concern. This course provides foundational knowledge on general HCI, usable security, and user interface techniques that have been proposed for cybersecurity applications. The course also discusses a set of cybersecurity problems whereby usable security approaches have been proposed.

4. Learning Outcomes

On successful completion of the course, students will be able to:

- Explain the challenges of usable security
- Describe, review, and critique recent literature in usable security
- Compare the strengths and weaknesses of usable security solutions, from both a usability perspective and a cybersecurity perspective
- Propose solutions to current problems in usable security
- Design user studies and analyze their results

5. Course Design

Each lecture period reviews and discusses the materials of that week. There will be in-class paper presentations and related activities. Assignments and quizzes will reinforce the weekly topics. Understanding of course concepts will be demonstrated through a final project. The scheduled topics and readings are detailed below.

6. Outline of Topics in the Course

Week #	Date	Topics	Readings (papers may vary slightly based on most recent research at the time of offering)
1		Introduction to Usable Security	- Garfinkel Chapters 1 and 2
2		Experimental Research and Design	- Lazar Chapters 2 and 3
3		Authentication	- Garfinkel Chapters 3.1 and 5.1
4		Statistical Analysis in HCI Research	- Lazar Chapter 4
5		Social Engineering and Phishing	- Garfinkel Chapters 3.3 and 4
6		Nudging and Cybersecurity Decisions	- A. Caraban et al. “23 Ways to Nudge: A Review of Technology-Mediated Nudging in Human-Computer Interaction”. Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems, 2019. - V. Zimmermann and K. Renaud. “The Nudge Puzzle: Matching Nudge Interventions to Cybersecurity Decisions.” ACM Trans. Comput.-Hum. Interact. 28, 1, Article 7 (2021).
7		Designing Surveys	- Lazar Chapter 5 - E. Redmiles et al. “A Summary of Survey Methodology Best Practices for Security and Privacy Researchers.” University of Maryland CS-TR-5055, 2017.
8		Usability Testing and Working with Human Subjects	- Lazar Chapters 10 and 15 - Schechter, Stuart. "Common pitfalls in writing about security and privacy human subjects experiments, and how to avoid them." Microsoft, 2013, URL: https://www.microsoft.com/en-us/research/wp-content/uploads/2016/02/commonpitfalls.pdf
9		Mental Models and User Education in Cybersecurity	- Jampen, D., Gür, G., Sutter, T. et al. Don’t Click: Towards an Effective Anti-Phishing Training. A Comparative Literature Review. Hum. Cent. Comput. Inf. Sci. 10, 33 (2020). - Elissa M. Redmiles et al., A Comprehensive Quality Evaluation of Security and Privacy Advice on the Web, In Proceedings of the 29th USENIX Security Symposium, 2020.

10		Usable Encryption	• Garfinkel Chapter 3.2 • Scott Ruoti, Nathan Kim, Ben Burgon, Timothy van der Horst, and Kent Seamons. 2013. Confused Johnny: when automatic encryption leads to confusion and mistakes. In Proceedings of the Ninth Symposium on Usable Privacy and Security (SOUPS), 2013. • C. Stransky et al. On the Limited Impact of Visualizing Encryption: Perceptions of E2E Messaging Security. In Proceedings of SOUPS, 2021. • C. Stransky, O. Wiese, V. Roth, Y. Acar and S. Fahl. 27 Years and 81 Million Opportunities Later: Investigating the Use of Email Encryption for an Entire University. In Proceedings of the IEEE Symposium on Security and Privacy, 2022.
11		Usability for Secure Software Development	• M. Green and M. Smith, "Developers are Not the Enemy!: The Need for Usable Security APIs," in IEEE Security & Privacy, vol. 14, no. 5, pp. 40-46, Sept.-Oct. 2016. • D. Votipka et al. “Understanding security mistakes developers make: Qualitative analysis from Build It, Break It, Fix It.” In Proceedings of the USENIX Security Symposium, 2020. • A. Krause et al. “Pushed by Accident: A Mixed-Methods Study on Strategies of Handling Secret Information in Source Code Repositories.” In Proceedings of the 32nd USENIX Security Symposium, 2023.
12		Usability for Secure System Administration	• Garfinkel Chapters 3.10 and 5.3 • Schreuders, Z. Cliffe, Tanya McGill, and Christian Payne. "Empowering end users to confine their own applications: The results of a usability study comparing SELinux, AppArmor, and FBAC-LSM." ACM Transactions on Information and System Security (TISSEC) 14.2 (2011): 1-28.

7. Required Texts/Readings

The following textbooks are mandatory for this course:

1. Garfinkel, Simson and Lipford, Heather Richter. *Usable Security: History, Themes, and Challenges.* Synthesis Lectures on Information Security, Privacy, and Trust, 2014.
2. Lazar, Jonathan, Jinjuan Heidi Feng, and Harry Hochheiser. *Research Methods in Human-Computer Interaction*. Morgan Kaufmann, 2017.

Additional readings may be assigned or recommended during the course.

8. Evaluation Method

- Paper presentation: 20%
- Final project: 40%
- Assignments: 20%
- Quizzes: 20%

Final course grades may be adjusted to conform to program or Faculty grade distribution profiles. Further information on grading can be found under Academic Regulations at: Ontario Tech's Academic regulations

9. Assignments and Tests

- Week 1: Paper presentation sign-up. Paper presentation will be in-class, the date will depend on the paper signed up for.
- Week 2: Assignment #1 released, due Week 4
- Week 3: Quiz #1
- Week 4: Assignment #2 released, due Week 6
- Week 6: Quiz #2
- Week 9: Quiz #3
- Week 12: Quiz #4
- Final Project: Due 1 week after last class

Missed In-term Examination
Students who miss an in-term examination such as a midterm or a term test may submit a request for consideration to the Faculty of Business and IT Advising Office and to the course instructor in writing using the Academic Consideration Form, along with supporting documentation. The request must be submitted within the deadlines specified in the Procedures for Consideration of Missed In-Term Course Work and Examinations. If a midterm or term test is missed for approved reasons, the weight of the missed component will be added to the weight of the final exam (or another exam component). If a student misses an in-term examination and does not follow the procedure above, they will receive a score of zero on the missed component.

All forms can also be found through MyOntarioTech or on the Ontario Tech University website.

Missed In-Term Course Work
A request for consideration for missed course work worth 20% or less of the final grade must be documented and reported to the instructor in writing within the deadlines specified in the Procedures for Consideration of Missed In-Term Course Work and Examinations. Course work includes, but is not limited to: quizzes, written assignments, participation, case studies, etc. If missed coursework totals more than 20% of the final grade, the request for consideration must be submitted to the Faculty of Business and IT Advising Office and to the course instructor in writing using the Academic Consideration Form, along with supporting documentation. The request must be submitted within the deadlines specified in the Procedures for Consideration of Missed In-Term

Course Work and Examinations. If approved, the weight of the missed course component will be added to the weight of the final project. If a student misses coursework and does not follow the procedure above, they will receive a score of zero on the missed component.

For information on how missed/late assignments and medical excuses are managed, please refer to the university's revised ***Procedures for Consideration of Missed In-Term Course Work and Examinations***

10. Technology Requirements and Learning Management System Information

Ontario Tech uses *Canvas*™ as its learning management system (LMS). Access to the LMS is limited to students formally registered in courses. That access is for the duration of the semester **and for an additional 120 days once the semester is over**. Students are strongly encouraged to download any/all relevant course material during that access period. Any requests for access post this period must be made in writing to the instructor/faculty member responsible for the course.

To support online learning, the university recommends certain technology requirements for laptops, software and internet connectivity which are available at: Ontario Tech's Remote Learning Policies.

Students experiencing technical difficulties such that they are unable to meet the technology requirements may contact the IT Service Help Desk at: servicedesk@dc-uoit.ca
Students experiencing financial difficulties such that they are unable to meet the technology requirements may contact Student Awards and Financial Aid Office at: connect@ontariotehu.ca

By remaining enrolled in this course, you acknowledge that you have read, understand and agree to observe the Recommended Technology Requirements for accessing university online learning resources, including those minimum requirements that are specific to your faculty and program.

11. Sensitive/Offensive Subject Matter

The classroom (both physical and virtual) is intended to provide a safe, open space for the critical and civil exchange of ideas and opinions. Some articles, media and other course materials may contain sensitive content that is offensive and/or disturbing. For example, some articles or videos may contain e.g. graphical depictions of violence, profanity, human anatomy, sexual acts, matters pertaining to race, gender, or sexuality. The Course Instructor will try to identify such material and communicate warnings to students in advance of the distribution and use of such materials, affording students the choice to either emotionally prepare for, or not to view or interact with, the content.

12. Student Support

Any student who faces challenges securing their food or housing and believes this may affect their performance in the course is urged to contact studentlife@ontariotechu.ca for support. Furthermore, please notify your professor if you are comfortable in doing so. This will enable them to provide any resources and help that they can.

13. Student Sexual Violence Support and Education

Ontario Tech is committed to the prevention of sexual violence in all its forms. For any student who has experienced Sexual Violence, Ontario Tech can help. We will make accommodations to cater to the diverse backgrounds, cultures, and identities of students when dealing with individual cases.

If you think you have been subjected to or witnessed sexual violence:

- Reach out to the gender-based case specialist in the Human Rights office, a specially trained individual authorized to receive confidential disclosures about incidents of sexual violence. The Human Rights Office will make support services, including counselling, access or referrals to medical services, safety planning and accommodations, available to Students affected by an Incident of Sexual Violence. Book a consultation with the Case Specialist for more information.

Learn more about your options at: Ontario Tech's Policy on Sexual Violence and Support Information.

14. Students with Disabilities

Ontario Tech University is committed to promoting an environment where everyone has an equal opportunity to contribute to their fullest potential. Students who require accommodation for a disability are advised to contact Student Accessibility Services (SAS) as soon as possible. Accommodation decisions will be made in accordance with the Ontario Human Rights Code. Accommodations will be consistent with and supportive of the essential requirements of courses and programs, and provided in a way that respects the dignity of students with disabilities and encourages integration and equality of opportunity. Reasonable academic accommodation may require instructors to exercise creativity and flexibility in responding to the needs of students with disabilities while maintaining integrity.

Disability-related and accommodation support is available for students with mental health, physical, mobility, sensory, medical, cognitive, or learning challenges. Office hours are 8:30am-4:30pm, Monday, Tuesday, Thursday, and Friday, Wednesday's 10:00 am to 4:30. Please note they are closed each day between noon and 1:00 pm. For more information on services provided, you can visit the SAS website at Ontario Tech's Student Accessibility Services (SAS). Students may contact Student Accessibility Services by calling 905-721-3266, or email studentaccessibility@ontariotechu.ca.

Students who require the use of the Test Centre to write tests, midterms, or quizzes MUST register online using the SAS test/exam sign-up module, found here Registration Link to write examinations in SAS at Ontario Tech. Students must sign up for tests, midterms, or quizzes **AT LEAST seven (7) working days before the date of the test.**

Students must register for final exams no later **than 3 weeks prior to the start of the final examination period**. The final examination period is given at Ontario Tech University's Important dates and deadlines.

15. Professional Suitability (if applicable)

Ontario Tech University is a community that values and promotes respect, integrity, diversity and accountability among all members of the university. These values can only be achieved in an environment that supports and protects the safety and security of its members. The Ontario Tech University Policy on Student Conduct defines and guides standards of student behaviour at the university to uphold these values and ensure that behaviour contrary to these standards are dealt with in a manner that is fair, open and effective.

The Faculty of Business & IT has the following expectations related to professionalism for all its community members, including without limitation, students, Staff, and Faculty:

- **Respect, civility, and courtesy:** Community members are expected to treat each other with respect, civility, and courtesy both in and outside of the classroom. Rudeness, profanity, insults, harassment, and class disruptions are unacceptable.
- **Critique ideas, not the people who raise the ideas:** Discussions, debates, and the exchange of ideas are normal parts of life in an academic community. Community members are expected

to engage in discussions, debates, and the exchange of ideas in respectful ways, even while vigorously advocating for one's perspective.

- **Talk *to* those with whom you have a complaint, not *about* them.** When community members have disputes, complaints, and/or concerns about another community member, they are expected to do their best to address the matter directly and informally with the other member, provided that it is safe to do so.
- **Special obligations:** Community members in positions of authority have special obligations to demonstrate respect, civility, and professionalism and to encourage the development of these values within the FBIT community.

The *Professional Suitability* policy can be found at Ontario Tech's Professional Suitability Policy and the related procedures are hosted at Ontario Tech's Professional Suitability Procedures.

16. Academic Integrity

Students and faculty at Ontario Tech University share an important responsibility to maintain the integrity of the teaching and learning relationship. This relationship is characterized by honesty, fairness and mutual respect for the aim and principles of the pursuit of education. Academic misconduct impedes the activities of the university community and is punishable by appropriate disciplinary action.

Students are expected to be familiar with and abide by Ontario Tech University's regulations on Academic Conduct which sets out the kinds of actions that constitute academic misconduct, including plagiarism, copying or allowing one's own work to copied, use of unauthorized aids in examinations and tests, submitting work prepared in collaboration with another student when such collaboration has not been authorized, among other academic offences. The regulations also describe the procedures for dealing with allegations, and the sanctions for any finding of academic misconduct, which can range from a resubmission of work to a failing grade to permanent expulsion from the university. A lack of familiarity with these regulations on academic conduct does not constitute a defense against its application. Please note that generative artificial intelligence (GAI) tools should not be utilized without advance, specific written approval by the faculty member teaching the course.

More information can be found at Ontario Tech's Academic Integrity Policy.

Extra support services are available to all Ontario Tech University students in academic development, study skills, counseling, and peer mentorship. More information on student support services can be found at Academic Support at Ontario Tech.

17. Turnitin (if applicable)

Ontario Tech University and faculty members reserve the right to use electronic means to detect and help prevent plagiarism. Students agree that by taking this course all assignments are subject to submission for textual similarity review by Turnitin.com. Assignments submitted to Turnitin.com will be included as source documents in Turnitin.com's restricted access database solely for the purpose of detecting plagiarism in such documents. The instructor may require students to submit their assignments electronically to Turnitin.com or the instructor may submit questionable text on behalf of a student. The terms that apply to Ontario Tech University's use of the Turnitin.com service are described on the Turnitin.com website.

Students who do not wish to have their work submitted to Turnitin.com must provide with their assignment at the time of submission to the instructor a signed Turnitin.com Assignment Cover sheet: Signed Turnitin Coversheet to Withdraw Permission to Submit Work.

18. Online Test and Exam Proctoring (Virtual Proctoring)

Ontario Tech University will conduct virtual monitoring of examinations in accordance with Ontario privacy legislation and all approved policy instruments.

19. Final Examinations (if applicable)

Final examinations are held during the final examination period at the end of the semester and may take place in a different room and on a different day from the regularly scheduled class. Check the published Examination Schedule for a complete list of days and times.

Students are required to show their valid physical or digital Ontario Tech University student photo ID card (campus ID), or a valid government issued photo ID that is in English when writing an **in-person examination.** Students are advised to obtain their Student ID Card well in advance of the examination period as they will not be able to write their examinations without it. More information on ID cards can be found at Information on Ontario Tech's Student ID Cards.

Students who are unable to write a final examination when scheduled due to religious publications may make arrangements to write a deferred examination. These students are required to submit an Academic Consideration form to the applicable Faculty as soon as possible and no later than three weeks prior to the first day of the final examination period.

Further information on final examinations can be found in the university's *Procedures for Final Examination Administration* Ontario Tech's Procedures for Final Examinations and in the Procedures for Consideration of Missed In-Term Course Work and Examinations.

20. Freedom of Information and Protection of Privacy Act

The following is an important notice regarding the process for submitting course assignments, quizzes, and other evaluative material in your courses in the Faculty of Business and IT.

Ontario Tech University is governed by the Freedom of Information and Protection of Privacy Act ("FIPPA"). In addition to providing a mechanism for requesting records held by the university, this legislation also requires that the University not disclose the personal information of its students without their consent.

FIPPA's definition of "personal information" includes, among other things, documents that contain both your name and your Banner (student) ID. For example, this could include graded test papers or assignments. To ensure that your rights to privacy are protected, the Faculty of Business and IT encourages you to use only your Banner ID on assignments or test papers being submitted for grading. This policy is intended to prevent the inadvertent disclosure of your information where graded papers are returned to groups of students at the same time. If you still wish to write both your name and your Banner ID on your tests and assignments, please be advised that Ontario Tech University will interpret this as an implied consent to the disclosure of your personal information in the normal course of returning graded materials to students.

If you have any questions or concerns relating to the new policy or the issue of implied consent addressed above, please contact accessandprivacy@ontariotechu.ca

Notice of Collection and Use of Personal Information

Throughout this course, personal information may be collected through the use of certain technologies under the authority of the *University of Ontario Institute of Technology Act, SO 2002, c. 8, Sch. O.* and will be collected, protected, used, disclosed and retained in compliance with Ontario's *Freedom of Information and Protection of Privacy Act R.S.O. 1990, c. F.31.*

This course will use the following technologies that may collect, use, disclose and retain personal information (including images) for the purposes described below:

- Google Meet and Kaltura Virtual Classroom to facilitate remote instruction and interactive learning;
- Peer-shared applications, services or technologies that may be reviewed, assessed, or used as part of coursework.
- Other applications, services, or technologies that support or enhance online learning that include, but are not limited to, the following: Turnitin.

  For more information relating to these technologies, we encourage you to visit: Educational Technologies used at Ontario Tech.

Questions regarding personal information may be directed to: Ontario Tech University Access and Privacy Office, 2000 Simcoe Street North, Oshawa, ON L1G 0C5, email: accessandprivacy@ontariotechu.ca.

By remaining enrolled in this course, you acknowledge that you have read, understand, and agree to the terms and conditions under which the technology provider(s) may collect, use, disclose and retain your personal information. You agree to the university using the technologies and using your personal information for the purposes described in this course outline.

21. Human Rights and Respect

Ontario Tech University is committed to providing a campus environment in which all University Members are treated with dignity and to fostering a climate of understanding and mutual respect. The University will not tolerate, ignore or condone Discrimination or Harassment by or against anyone. Examples of Harassing behavior include, but are not limited to; bullying, taunting or mocking someone’s race or creed, ridiculing an individual’s disability, or targeting individuals with unwanted sexual or negative stereotypical comments about one’s sex, gender, sexual orientation, gender identity and/or gender expression. Pursuant to Ontario Tech’s Respectful Campus Policy, students are reminded of their role in ensuring an equitable and inclusive learning environment. Requirements to refrain from harassment and discrimination apply broadly to on campus activities, e.g., on University property, in the classroom, including in lectures, labs and practicums, and also apply to off-campus activities, e.g. during any organized Ontario Tech class or extra-curricular activity including experiential learning opportunities such as co-op, practicum or during research endeavors, during official Ontario Tech events or using University equipment and technological tools that facilitate remote learning, e.g., class and other chat functions, video conferencing, and electronic mail.

22. Freedom of Expression

Pursuant to Ontario Tech’s Freedom of Expression Policy, all students are encouraged to express ideas and perspectives freely and respectfully in university space and in the online university environment, subject to certain limitations. Students are reminded that the limits on Freedom of Expression include speech or behaviour that: is illegal or interferes with the university’s legal obligations; defames an individual or group; constitutes a threat, harassment or discrimination; is a breach of fiduciary, contractual, privacy or confidentiality obligations or commitments; and unduly disrupts and interferes with the functioning of the university. In the context of working online, different forms of communication are used. Where permitted, students using “chat” functions or other online forms of communication are encouraged to ensure that their communication complies with the Freedom of Expression Policy.

23. Copyright Notice

All Teaching Materials, as they are defined under Ontario Tech's Intellectual Property policy ("IP Policy"), provided by the instructor throughout the course, including, but not limited to, in whole or in part, course notes, teaching notes, custom books, tutorials, evaluation tools, presentations and examinations are subject to the Copyright Act, R.S.C., 1985, c. C-42 and the IP Policy. Subject to the IP Policy, Teaching Materials are owned by the faculty member, instructor or other third party who creates such works, with a license to the University. The copyright owner(s) reserves all intellectual property rights in and to the foregoing materials. Consistent with the IP Policy, Teaching Materials are intended to be used by Ontario Tech University students registered in the course that is the subject of this course outline for educational purposes only. Any distribution or publishing of this material (e.g., uploading material to a third-party website) by a student is strictly prohibited under the law unless the student has obtained the copyright owner's prior written consent. Any violation of copyright law or the IP Policy, if proven, may be subject to sanction as academic misconduct, and/or under the Student Conduct Policy.

24. Student Course Feedback Surveys

Student evaluation of teaching is a highly valued and helpful mechanism for monitoring the quality of Ontario Tech University's programs and instructional effectiveness. To that end, course evaluations are administered by an external company in an online, anonymous process during the last few weeks of classes. Students are encouraged to participate actively in this process and will be notified of the dates. Notifications about course evaluations will be sent via e-mail, and posted on Canvas, Weekly News, and signage around the campus.

25. AODA

The Accessibility for Ontarians with Disabilities Act (AODA) standards have been considered in the development of this model course template and it adheres to the principles outlined in the University's Accessibility Policy.

Ontario Tech University acknowledges the lands and people of the Mississaugas of Scugog Island First Nation. We are thankful to be welcomed on these lands in friendship. The lands we are situated on are covered under the Williams Treaties and the traditional territory of the Mississaugas, a branch of the greater Anishinaabeg Nation, including Algonquin, Ojibway, Odawa and Pottawatomi. These lands remain home to a number of Indigenous nations and people.

We acknowledge this land out of respect for the Indigenous nations who have cared for Turtle Island, also called North America, from before the arrival of settler peoples until this day. Most importantly, we remember the history of these lands has been tainted by poor treatment and a lack of friendship with the First Nations who call them home.

This history is something we are all affected by as we are all treaty people in Canada. We all have a shared history to reflect on, and each of us is affected by this history in different ways. Our past defines our present, but if we move forward as friends and allies, then it does not have to define our future.

FACULTY OF BUSINESS AND IT

INFR 6030G: Information Trust
Course outline for ----

1. Course Details & Important Dates*

Term	Course Type	Day	Time	Location	CRN#
----				----	

Classes Start	Classes End	**Last day to drop course without academic consequence**	Final Exam Period
----	----	----	----

* Visit Ontario Tech's Important Dates and Deadlines for other dates.

Please Choose ONE of the following, *if applicable*:

Important Note – Final Exams

There is no final exam for this course

2. Instructor Contact Information

Instructor Name	Office	Phone	Email
Office Hours:			

Laboratory/Teaching Assistant Name	Office	Phone	Email

Office Hours:			

3. Course Description

In this course, students examine trust, provenance, critical thinking and design thinking for information from first principles to action. How to measure and judge information quality is discussed, as well as the various ways in which trust can be attacked in the context of information. More specifically, we will also examine how to use information to make trustworthy decisions in different cybersecurity and other contexts.

4. Learning Outcomes

On the successful completion of the course, students will be able to:

- Compare and Contrast different philosophies and models of trust
- Apply Design Thinking and Critical Thinking to information trust and provenance problems
- Discuss different approaches for the protection of information as an object
- Construct learning materials to help others in the understanding of information trust problems
- Hypothesize on the ways in which information is useful and used in the context of trust and future technoloogies

5. Course Design

The course is an online discussion-based course with presentations from experts from industry and academia on the ways in which trust, information design, critical and design thinking come together to address the increasingly difficult provenance questions as they relate to information that can be used to inform decisions, justify actions and build worthwhile, trustworthy knowledge.

We will use lectures to discuss the fundamentals of the concepts, and case or paper-based student-led discussions about how real examples reflect the content of the course fundamentals. This is a student-driven course and students are expected to provide their own personal and/or professional examples of how information trust works (or doesn't) for the class.

6. Outline of Topics in the Course

Lecture #	Topics	Details of topics to be covered in the course, by unit or by week
1	What is trust? How can we even use it?	Trust fundamentals, computational trust, computing trust.
2	Trust in information, the basics	
3	Provenance	What it is, what is means, how it can be determined, what it means to trust
4	Building knowledge	How is knowledge built? What builds it? What links together? What are the problems?
5	Design Thinking	An introduction to design thinking and why it matters here

6	Critical Design Thinking	Applying critical thinking to the design thinking problem and coming up with a new paradigm
7	Information Trust, tying it all together	A look at Atele-William's Information Trust models
8	Applying what was learned	How can what we have looked at help with things like provenance and knowledge bulding? We will do our information trust problem this week.
9	Attacks on trust	Trust is fragile. How? Why? What can kill or damage it?
10	Attacks on information	Information has always been precious, and has always been attacked, to be stolen or (more relevant to us) weaponized. How, when and why?
11	Defences and panaceas	And how can we defend it, either by being pre-informed or by putting sensible checks and balances in place?
12	Wrapping up: a design for information trust for the LLM world and beyond	The world is changing. How can we best adapt and put in place a sensible way to think about what we see before us based on what we have learned?

7. Required Texts/Readings

The course is reading and discussion-based. Some of the materials are expected to come from students themselves (related to their own experiences in the area) whilst some are drawn from sources that are either freely available or available through the library at no cost to the student. There is no textbook but as a reference we will be using the Open Educational Resource, "Trust Systems" (Marsh, 2022) which is available on the Ontario Open Library. Further open resources will be curated during the course by the students as part of their evaluated work.

The readings and cases will be assigned at the start of the course, and will include sections and papers related to:

- Design Thinking
- Critical Thinking
- Computational Trust
- Information Trust
- Decision-making
- Trust Attacks
- Provenance
- AI and LLMs
- Privacy

Additional readings may be assigned or recommended during the course.

8. Evaluation Method

Participation in classes is expected, attendance is mandatory (a maximum of 2 classes can be missed before the final grade becomes a zero). Participation is 30% of the final grade.

Presentation of case/papers (weekly, assigned at the start of the class): 25%

A recorded video presentation of one of the class topics will be required by students: 25%

Peer evaluation of recorded presentations: 10%

Worked problem example: 10% (this will use the skills developed in the course of the class in order to address information trust in a curated information sample).

Final course grades may be adjusted to conform to program or Faculty grade distribution profiles. Further information on grading can be found under Academic Regulations at: Ontario Tech's Academic regulations

9. Assignments and Tests

Missed In-Term Course Work

A request for consideration for missed course work worth 20% or less of the final grade must be documented and reported to the instructor in writing within the deadlines specified in the Procedures for Consideration of Missed In-Term Course Work and Examinations. Course work includes, but is not limited to: quizzes, written assignments, participation, case studies, etc. If missed coursework totals more than 20% of the final grade, the request for consideration must be submitted to the Faculty of Business and IT Advising Office and to the course instructor in writing using the Academic Consideration Form, along with supporting documentation. The request must be submitted within the deadlines specified in the Procedures for Consideration of Missed In-Term Course Work and Examinations. If approved, the weight of the missed course component will be added to the weight of the final information trust problem. If a student misses coursework and does not follow the procedure above, they will receive a score of zero on the missed component.

Attendance in the weekly classes is mandatory. Given the discussional nature of the course, students who miss more than 2 of the weekly sessions will receive an automatic zero for the course.

For information on how missed/late assignments and medical excuses are managed, please refer to the university's revised ***Procedures for Consideration of Missed In-Term Course Work and Examinations***

10. Technology Requirements and Learning Management System Information

Ontario Tech uses *Canvas*™ as its learning management system (LMS). Access to the LMS is limited to students formally registered in courses. That access is for the duration of the semester **and for an additional 120 days once the semester is over**. Students are strongly encouraged to download any/all relevant course material during that access period. Any requests for access post this period must be made in writing to the instructor/faculty member responsible for the course.

To support online learning, the university recommends certain technology requirements for laptops, software and internet connectivity which are available at: Ontario Tech's Remote Learning Policies.

Students experiencing technical difficulties such that they are unable to meet the technology requirements may contact the IT Service Help Desk at: servicedesk@dc-uoit.ca
Students experiencing financial difficulties such that they are unable to meet the technology requirements may contact Student Awards and Financial Aid Office at: connect@ontariotehu.ca

By remaining enrolled in this course, you acknowledge that you have read, understand and agree to observe the Recommended Technology Requirements for accessing university online learning resources, including those minimum requirements that are specific to your faculty and program.

11. Sensitive/Offensive Subject Matter

The classroom (both physical and virtual) is intended to provide a safe, open space for the critical and civil exchange of ideas and opinions. Some articles, media and other course materials may contain sensitive content that is offensive and/or disturbing. For example, some articles or videos may contain Instructors should provide examples that are applicable to the course subject matter – e.g. graphical depictions of violence, profanity, human anatomy, sexual acts, matters pertaining to race, gender, or sexuality. The Course Instructor will try to identify such material and communicate warnings to students in advance of the distribution and use of such materials, affording students the choice to either emotionally prepare for, or not to view or interact with, the content. Instructors should publish a warning statement in advance so as to give students adequate opportunity to make a choice to avoid any such matter. The following is a sample disclaimer: “The content you are about to view contains sensitive subject matter that may be considered offensive and/or disturbing to some viewers. By viewing and/or interacting with the content you acknowledge and agree that it is your decision to view and interact with the content and to take the risk that you will experience a negative emotional response or reaction to the nature of the content.”

12. Student Support

Any student who faces challenges securing their food or housing and believes this may affect their performance in the course is urged to contact studentlife@ontariotechu.ca for support. Furthermore, please notify your professor if you are comfortable in doing so. This will enable them to provide any resources and help that they can.

13. Student Sexual Violence Support and Education

Ontario Tech is committed to the prevention of sexual violence in all its forms. For any student who has experienced Sexual Violence, Ontario Tech can help. We will make accommodations to cater to the diverse backgrounds, cultures, and identities of students when dealing with individual cases.

If you think you have been subjected to or witnessed sexual violence:

- Reach out to the gender-based case specialist in the Human Rights office, a specially trained individual authorized to receive confidential disclosures about incidents of sexual violence. The Human Rights Office will make support services, including counselling, access or referrals to medical services, safety planning and accommodations, available to Students affected by an Incident of Sexual Violence. Book a consultation with the Case Specialist for more information.

Learn more about your options at: Ontario Tech's Policy on Sexual Violence and Support Information.

14. Students with Disabilities

Ontario Tech University is committed to promoting an environment where everyone has an equal opportunity to contribute to their fullest potential. Students who require accommodation for a disability are advised to contact Student Accessibility Services (SAS) as soon as possible. Accommodation decisions will be made in accordance with the Ontario Human Rights Code. Accommodations will be consistent with and supportive of the essential requirements of courses and programs, and provided in a way that respects the dignity of students with disabilities and encourages integration and equality of opportunity. Reasonable academic accommodation may require instructors to exercise creativity and flexibility in responding to the needs of students with disabilities while maintaining integrity.

Disability-related and accommodation support is available for students with mental health, physical, mobility, sensory, medical, cognitive, or learning challenges. Office hours are 8:30am-4:30pm, Monday, Tuesday, Thursday, and Friday, Wednesday's 10:00 am to 4:30. Please note they are closed each day between noon and 1:00 pm. For more information on services provided, you can visit the SAS website at Ontario Tech's Student Accessibility Services (SAS). Students may contact Student Accessibility Services by calling 905-721-3266, or email studentaccessibility@ontariotechu.ca.

Students who require the use of the Test Centre to write tests, midterms, or quizzes MUST register online using the SAS test/exam sign-up module, found here Registration Link to write examinations in SAS at Ontario Tech. Students must sign up for tests, midterms, or quizzes **AT LEAST seven (7) working days before the date of the test.**

Students must register for final exams no later **than 3 weeks prior to the start of the final examination period**. The final examination period is given at Ontario Tech University's Important dates and deadlines.

15. Professional Suitability (if applicable)

Ontario Tech University is a community that values and promotes respect, integrity, diversity and accountability among all members of the university. These values can only be achieved in an environment that supports and protects the safety and security of its members. The Ontario Tech University Policy on Student Conduct defines and guides standards of student behaviour at the university to uphold these values and ensure that behaviour contrary to these standards are dealt with in a manner that is fair, open and effective.

The Faculty of Business & IT has the following expectations related to professionalism for all its community members, including without limitation, students, Staff, and Faculty:

- **Respect, civility, and courtesy:** Community members are expected to treat each other with respect, civility, and courtesy both in and outside of the classroom. Rudeness, profanity, insults, harassment, and class disruptions are unacceptable.
- **Critique ideas, not the people who raise the ideas:** Discussions, debates, and the exchange of ideas are normal parts of life in an academic community. Community members are expected to engage in discussions, debates, and the exchange of ideas in respectful ways, even while vigorously advocating for one's perspective.
- **Talk *to* those with whom you have a complaint, not *about* them.** When community members have disputes, complaints, and/or concerns about another community member, they are expected to do their best to address the matter directly and informally with the other member, provided that it is safe to do so.

- **Special obligations:** Community members in positions of authority have special obligations to demonstrate respect, civility, and professionalism and to encourage the development of these values within the FBIT community.

The *Professional Suitability* policy can be found at Ontario Tech's Professional Suitability Policy and the related procedures are hosted at Ontario Tech's Professional Suitability Procedures.

16. Academic Integrity

Students and faculty at Ontario Tech University share an important responsibility to maintain the integrity of the teaching and learning relationship. This relationship is characterized by honesty, fairness and mutual respect for the aim and principles of the pursuit of education. Academic misconduct impedes the activities of the university community and is punishable by appropriate disciplinary action.

Students are expected to be familiar with and abide by Ontario Tech University's regulations on Academic Conduct which sets out the kinds of actions that constitute academic misconduct, including plagiarism, copying or allowing one's own work to copied, use of unauthorized aids in examinations and tests, submitting work prepared in collaboration with another student when such collaboration has not been authorized, among other academic offences. The regulations also describe the procedures for dealing with allegations, and the sanctions for any finding of academic misconduct, which can range from a resubmission of work to a failing grade to permanent expulsion from the university. A lack of familiarity with these regulations on academic conduct does not constitute a defense against its application. Please note that generative artificial intelligence (GAI) tools should not be utilized without advance, specific written approval by the faculty member teaching the course.

More information can be found at Ontario Tech's Academic Integrity Policy.

Extra support services are available to all Ontario Tech University students in academic development, study skills, counseling, and peer mentorship. More information on student support services can be found at Academic Support at Ontario Tech.

17. Turnitin (if applicable)

Ontario Tech University and faculty members reserve the right to use electronic means to detect and help prevent plagiarism. Students agree that by taking this course all assignments are subject to submission for textual similarity review by Turnitin.com. Assignments submitted to Turnitin.com will be included as source documents in Turnitin.com's restricted access database solely for the purpose of detecting plagiarism in such documents. The instructor may require students to submit their assignments electronically to Turnitin.com or the instructor may submit questionable text on behalf of a student. The terms that apply to Ontario Tech University's use of the Turnitin.com service are described on the Turnitin.com website.

Students who do not wish to have their work submitted to Turnitin.com must provide with their assignment at the time of submission to the instructor a signed Turnitin.com Assignment Cover sheet: Signed Turnitin Coversheet to Withdraw Permission to Submit Work.

18. Online Test and Exam Proctoring (Virtual Proctoring)

Ontario Tech University will conduct virtual monitoring of examinations in accordance with Ontario privacy legislation and all approved policy instruments.

19. Final Examinations (if applicable)

Final examinations are held during the final examination period at the end of the semester and may take place in a different room and on a different day from the regularly scheduled class. Check the published Examination Schedule for a complete list of days and times.

Students are required to show their valid physical or digital Ontario Tech University student photo ID card (campus ID), or a valid government issued photo ID that is in English when writing an **in-person examination.** Students are advised to obtain their Student ID Card well in advance of the examination period as they will not be able to write their examinations without it. More information on ID cards can be found at Information on Ontario Tech's Student ID Cards.

Students who are unable to write a final examination when scheduled due to religious publications may make arrangements to write a deferred examination. These students are required to submit an Academic Consideration form to the applicable Faculty as soon as possible and no later than three weeks prior to the first day of the final examination period.

Further information on final examinations can be found in the university's *Procedures for Final Examination Administration* Ontario Tech's Procedures for Final Examinations and in the Procedures for Consideration of Missed In-Term Course Work and Examinations.

20. Freedom of Information and Protection of Privacy Act

The following is an important notice regarding the process for submitting course assignments, quizzes, and other evaluative material in your courses in the Faculty of Business and IT.

Ontario Tech University is governed by the Freedom of Information and Protection of Privacy Act ("FIPPA"). In addition to providing a mechanism for requesting records held by the university, this legislation also requires that the University not disclose the personal information of its students without their consent.

FIPPA's definition of "personal information" includes, among other things, documents that contain both your name and your Banner (student) ID. For example, this could include graded test papers or assignments. To ensure that your rights to privacy are protected, the Faculty of Business and IT encourages you to use only your Banner ID on assignments or test papers being submitted for grading. This policy is intended to prevent the inadvertent disclosure of your information where graded papers are returned to groups of students at the same time. If you still wish to write both your name and your Banner ID on your tests and assignments, please be advised that Ontario Tech University will interpret this as an implied consent to the disclosure of your personal information in the normal course of returning graded materials to students.

If you have any questions or concerns relating to the new policy or the issue of implied consent addressed above, please contact accessandprivacy@ontariotechu.ca

Notice of Collection and Use of Personal Information
Throughout this course, personal information may be collected through the use of certain technologies under the authority of the *University of Ontario Institute of Technology Act, SO 2002, c. 8, Sch. O.* and will be collected, protected, used, disclosed and retained in compliance with Ontario's *Freedom of Information and Protection of Privacy Act R.S.O. 1990, c. F.31.*

This course will use the following technologies that may collect, use, disclose and retain personal information (including images) for the purposes described below: Instructors should edit this section according to the systems and technologies to be used in this specific course (e.g. If using Proctortrack, remove any reference to Respondus)

- Respondus Monitor and Proctortrack to maintain academic integrity for examinations;
- Google Meet and Kaltura Virtual Classroom to facilitate remote instruction and interactive learning;
- Peer-shared applications, services or technologies that may be reviewed, assessed, or used as part of coursework.
- Other applications, services, or technologies that support or enhance online learning that include, but are not limited to, the following: Instructor to list all relevant components.

For more information relating to these technologies, we encourage you to visit: Educational Technologies used at Ontario Tech.

Questions regarding personal information may be directed to: Ontario Tech University Access and Privacy Office, 2000 Simcoe Street North, Oshawa, ON L1G 0C5, email: accessandprivacy@ontariotechu.ca.

By remaining enrolled in this course, you acknowledge that you have read, understand, and agree to the terms and conditions under which the technology provider(s) may collect, use, disclose and retain your personal information. You agree to the university using the technologies and using your personal information for the purposes described in this course outline.

21. Human Rights and Respect

Ontario Tech University is committed to providing a campus environment in which all University Members are treated with dignity and to fostering a climate of understanding and mutual respect. The University will not tolerate, ignore or condone Discrimination or Harassment by or against anyone. Examples of Harassing behavior include, but are not limited to; bullying, taunting or mocking someone's race or creed, ridiculing an individual's disability, or targeting individuals with unwanted sexual or negative stereotypical comments about one's sex, gender, sexual orientation, gender identity and/or gender expression. Pursuant to Ontario Tech's Respectful Campus Policy, students are reminded of their role in ensuring an equitable and inclusive learning environment. Requirements to refrain from harassment and discrimination apply broadly to on campus activities, e.g., on University property, in the classroom, including in lectures, labs and practicums, and also apply to off-campus activities, e.g. during any organized Ontario Tech class or extra-curricular activity including experiential learning opportunities such as co-op, practicum or during research endeavors, during official Ontario Tech events or using University equipment and technological tools that facilitate remote learning, e.g., class and other chat functions, video conferencing, and electronic mail.

22. Freedom of Expression

Pursuant to Ontario Tech's Freedom of Expression Policy, all students are encouraged to express ideas and perspectives freely and respectfully in university space and in the online university environment, subject to certain limitations. Students are reminded that the limits on Freedom of Expression include speech or behaviour that: is illegal or interferes with the university's legal obligations; defames an individual or group; constitutes a threat, harassment or discrimination; is a breach of fiduciary, contractual, privacy or confidentiality obligations or commitments; and unduly disrupts and interferes with the functioning of the university. In the context of working online, different forms of communication are used. Where permitted, students using "chat" functions or other online forms of communication are encouraged to ensure that their communication complies with the Freedom of Expression Policy.

23. Copyright Notice

All Teaching Materials, as they are defined under Ontario Tech's Intellectual Property policy ("IP Policy"), provided by the instructor throughout the course, including, but not limited to, in whole or in part, course notes, teaching notes, custom books, tutorials, evaluation tools, presentations and examinations are subject to the Copyright Act, R.S.C., 1985, c. C-42 and the IP Policy. Subject to the IP Policy, Teaching Materials are owned by the faculty member, instructor or other third party who creates such works, with a license to the University. The copyright owner(s) reserves all intellectual property rights in and to the foregoing materials. Consistent with the IP Policy, Teaching Materials are intended to be used by Ontario Tech University students registered in the course that is the subject of this course outline for educational purposes only. Any distribution or publishing of this material (e.g., uploading material to a third-party website) by a student is strictly prohibited under the law unless the student has obtained the copyright owner's prior written consent. Any violation of copyright law or the IP Policy, if proven, may be subject to sanction as academic misconduct, and/or under the Student Conduct Policy.

24. Student Course Feedback Surveys

Student evaluation of teaching is a highly valued and helpful mechanism for monitoring the quality of Ontario Tech University's programs and instructional effectiveness. To that end, course evaluations are administered by an external company in an online, anonymous process during the last few weeks of classes. Students are encouraged to participate actively in this process and will be notified of the dates. Notifications about course evaluations will be sent via e-mail, and posted on Canvas, Weekly News, and signage around the campus.

25. AODA

The Accessibility for Ontarians with Disabilities Act (AODA) standards have been considered in the development of this model course template and it adheres to the principles outlined in the University's Accessibility Policy.

Ontario Tech University

Ontario Tech University acknowledges the lands and people of the Mississaugas of Scugog Island First Nation. We are thankful to be welcomed on these lands in friendship. The lands we are situated on are covered under the Williams Treaties and the traditional territory of the Mississaugas, a branch of the greater Anishinaabeg Nation, including Algonquin, Ojibway, Odawa and Pottawatomi. These lands remain home to a number of Indigenous nations and people.

We acknowledge this land out of respect for the Indigenous nations who have cared for Turtle Island, also called North America, from before the arrival of settler peoples until this day. Most importantly, we remember the history of these lands has been tainted by poor treatment and a lack of friendship with the First Nations who call them home.

This history is something we are all affected by as we are all treaty people in Canada. We all have a shared history to reflect on, and each of us is affected by this history in different ways. Our past defines our present, but if we move forward as friends and allies, then it does not have to define our future.

FACULTY OF BUSINESS AND IT

Cybersecurity in Critical Infrastructure
2024-25

1. Course Details & Important Dates*

Term	Course Type	Day	Time	Location	CRN#
2024-25	Online				

Classes Start	Classes End	**Last day to drop course without academic consequence**	Final Exam Period

* Visit Ontario Tech's Important Dates and Deadlines for other dates.

2. Instructor Contact Information

Instructor Name	Office	Phone	Email
Khalil El-Khatib			Canvas Email
Office Hours: by appointment			

Laboratory/Teaching Assistant Name	Office	Phone	Email
Office Hours: by appointment			

3. Course Description

Today, every nation has identified several critical infrastructures that are essential for national and economic security. The Canadian National Strategy has identified 10 CI sectors including information and communication technology, energy and utilities, water, manufacturing, food, government, health, safety, finance, and transportation. Ensuring the security and resiliency of these infrastructure is a key priority for the Canadian government and for every government around the world. The course will teach students about identifying physical and cybersecurity threats that can affect the security of a critical infrastructure, and also understanding and developing integrated risk management strategies

4. Learning Outcomes

On successful completion of the course, students will be able to:

- Understand the key concepts in critical infrastructure protection,
- Understand the security requirements and considerations for critical infrastructure.
- Understand interdependencies among critical infrastructures.
- Perform risk analysis for critical infrastructure protection.
- Develop an integrated risk management strategies for critical infrastructure protection.

5. Course Design

The lectures for the course are designed to include a fair amount of discussion with the necessary theory to meet the level of a graduate course. Students are expected to attend all lectures. To succeed in this course, it is highly advisable that students:

1. Read the notes/textbook/papers prior to the lecture to have an idea of the new concept(s) that will be introduced that day.
2. During the lecture, make sure the new topic(s) being introduced is understood. Ask questions.
3. Pay attention to lectures.
4. After the lecture, review the material studied during that session.
5. See the professor during office hours or schedule extra consultation time, if necessary.
6. Assignments are designed to provide students with hands-on learning on the concepts studied in the course.
7. The Final Project is designed so that students will become very familiar with a specific topic, and will be able to write a survey paper on that area as well as articulate a presentation to the class.

6. Outline of Topics in the Course

Week #	Date	Topics	Readings
1		Introduction to Critical Infrastructure	•
2		The convergence of Physical and cybersecurity	•
3		Industrial Control Systems	•

4		Critical Infrastructure Threats	•
5		Energy and Utilities Sector	•
6		finance and Government Sector	
7		Risk Assessments	•
8		Incident Response	•
9		Policy & Governance	•
10		Student Presentations	•
11		Student Presentations	
12			

***Important Notes:** Adjustment of scheduled lectures might be made in accordance with any unforeseen circumstances during the semester.*

7. Required Readings

Students will be assigned various up-to-date research papers to read on each topic. students might wish to read some of the following textbooks, including:

- Industrial Network Security: Securing Critical Infrastructure Networks for Smart Grid, Scada, and Other Industrial Control Systems, by Eric D. Knapp and Joel Thomas Langill
- Critical Infrastructure Protection A Complete Guide, by Gerardus Blokdyk

Additional readings may be assigned or recommended during the course.

8. Evaluation Method

The course has only a final term paper and presentation. Students are encouraged to pick a topic related to critical infrastructure protection, do a literature review about the topic, present it to the whole class, and finally write a report about it.

9. Assignments and Tests

There are no tests in this course.

10. Technology Requirements and Learning Management System Information

Ontario Tech uses *Canvas*™ as its learning management system (LMS). Access to the LMS is limited to students formally registered in courses. That access is for the duration of the semester **and for an additional 120 days once the semester is over**. Students are strongly encouraged to download any/all relevant course material during that access period. Any requests for access post this period must be made in writing to the instructor/faculty member responsible for the course.

To support online learning, the university recommends certain technology requirements for laptops, software and internet connectivity which are available at: Ontario Tech's Remote Learning Policies.

Students experiencing technical difficulties such that they are unable to meet the technology requirements may contact the IT Service Help Desk at: servicedesk@dc-uoit.ca
Students experiencing financial difficulties such that they are unable to meet the technology requirements may contact Student Awards and Financial Aid Office at: connect@ontariotehu.ca

By remaining enrolled in this course, you acknowledge that you have read, understand and agree to observe the Recommended Technology Requirements for accessing university online learning resources, including those minimum requirements that are specific to your faculty and program.

11. Sensitive/Offensive Subject Matter

The classroom (both physical and virtual) is intended to provide a safe, open space for the critical and civil exchange of ideas and opinions. Some articles, media and other course materials may contain sensitive content that is offensive and/or disturbing. For example, some articles or videos may contain graphical depictions of violence, profanity, human anatomy, sexual acts, matters pertaining to race, gender, or sexuality. The Course Instructor will try to identify such material and communicate warnings to students in advance of the distribution and use of such materials, affording students the choice to either emotionally prepare for, or not to view or interact with, the content.
Disclaimer: “The content you are about to view contains sensitive subject matter that may be considered offensive and/or disturbing to some viewers. By viewing and/or interacting with the content you acknowledge and agree that it is your decision to view and interact with the content and to take the risk that you will experience a negative emotional response or reaction to the nature of the content.”

12. Student Support

Any student who faces challenges securing their food or housing and believes this may affect their performance in the course is urged to contact studentlife@ontariotechu.ca for support. Furthermore, please notify your professor if you are comfortable in doing so. This will enable them to provide any resources and help that they can.

13. Student Sexual Violence Support and Education

Ontario Tech is committed to the prevention of sexual violence in all its forms. For any student who has experienced Sexual Violence, Ontario Tech can help. We will make accommodations to cater to the diverse backgrounds, cultures, and identities of students when dealing with individual cases.

If you think you have been subjected to or witnessed sexual violence:

- Reach out to the gender-based case specialist in the Human Rights office, a specially trained individual authorized to receive confidential disclosures about incidents of sexual violence. The Human Rights Office will make support services, including counselling, access or referrals to medical services, safety planning and accommodations, available to Students affected by an Incident of Sexual Violence. Book a consultation with the Case Specialist for more information.

Learn more about your options at: Ontario Tech's Policy on Sexual Violence and Support Information.

14. Students with Disabilities

Ontario Tech University is committed to promoting an environment where everyone has an equal opportunity to contribute to their fullest potential. Students who require accommodation for a disability are advised to contact Student Accessibility Services (SAS) as soon as possible. Accommodation decisions will be made in accordance with the Ontario Human Rights Code.

Accommodations will be consistent with and supportive of the essential requirements of courses and programs, and provided in a way that respects the dignity of students with disabilities and encourages integration and equality of opportunity. Reasonable academic accommodation may require instructors to exercise creativity and flexibility in responding to the needs of students with disabilities while maintaining integrity.

Disability-related and accommodation support is available for students with mental health, physical, mobility, sensory, medical, cognitive, or learning challenges. Office hours are 8:30am-4:30pm, Monday, Tuesday, Thursday, and Friday, Wednesday's 10:00 am to 4:30. Please note they are closed each day between noon and 1:00 pm. For more information on services provided, you can visit the SAS website at Ontario Tech's Student Accessibility Services (SAS). Students may contact Student Accessibility Services by calling 905-721-3266, or email studentaccessibility@ontariotechu.ca.

Students who require the use of the Test Centre to write tests, midterms, or quizzes MUST register online using the SAS test/exam sign-up module, found here Registration Link to write examinations in SAS at Ontario Tech. Students must sign up for tests, midterms, or quizzes **AT LEAST seven (7) working days before the date of the test.**

Students must register for final exams no later **than 3 weeks prior to the start of the final examination period**. The final examination period is given at Ontario Tech University's Important dates and deadlines.

15. Professional Suitability (if applicable)

Ontario Tech University is a community that values and promotes respect, integrity, diversity and accountability among all members of the university. These values can only be achieved in an environment that supports and protects the safety and security of its members. The Ontario Tech University Policy on Student Conduct defines and guides standards of student behaviour at the university to uphold these values and ensure that behaviour contrary to these standards are dealt with in a manner that is fair, open and effective.

The Faculty of Business & IT has the following expectations related to professionalism for all its community members, including without limitation, students, Staff, and Faculty:

- **Respect, civility, and courtesy:** Community members are expected to treat each other with respect, civility, and courtesy both in and outside of the classroom. Rudeness, profanity, insults, harassment, and class disruptions are unacceptable.
- **Critique ideas, not the people who raise the ideas:** Discussions, debates, and the exchange of ideas are normal parts of life in an academic community. Community members are expected to engage in discussions, debates, and the exchange of ideas in respectful ways, even while vigorously advocating for one's perspective.
- **Talk *to* those with whom you have a complaint, not *about* them.** When community members have disputes, complaints, and/or concerns about another community member, they are expected to do their best to address the matter directly and informally with the other member, provided that it is safe to do so.
- **Special obligations:** Community members in positions of authority have special obligations to demonstrate respect, civility, and professionalism and to encourage the development of these values within the FBIT community.

The *Professional Suitability* policy can be found at Ontario Tech's Professional Suitability Policy and the related procedures are hosted at Ontario Tech's Professional Suitability Procedures.

16. Academic Integrity

Students and faculty at Ontario Tech University share an important responsibility to maintain the integrity of the teaching and learning relationship. This relationship is characterized by honesty, fairness and mutual respect for the aim and principles of the pursuit of education. Academic misconduct impedes the activities of the university community and is punishable by appropriate disciplinary action.

Students are expected to be familiar with and abide by Ontario Tech University's regulations on Academic Conduct which sets out the kinds of actions that constitute academic misconduct, including plagiarism, copying or allowing one's own work to copied, use of unauthorized aids in examinations and tests, submitting work prepared in collaboration with another student when such collaboration has not been authorized, among other academic offences. The regulations also describe the procedures for dealing with allegations, and the sanctions for any finding of academic misconduct, which can range from a resubmission of work to a failing grade to permanent expulsion from the university. A lack of familiarity with these regulations on academic conduct does not constitute a defense against its application. Please note that generative artificial intelligence (GAI) tools should not be utilized without advance, specific written approval by the faculty member teaching the course.

More information can be found at Ontario Tech's Academic Integrity Policy.

Extra support services are available to all Ontario Tech University students in academic development, study skills, counseling, and peer mentorship. More information on student support services can be found at Academic Support at Ontario Tech.

17. Turnitin (if applicable)

Ontario Tech University and faculty members reserve the right to use electronic means to detect and help prevent plagiarism. Students agree that by taking this course all assignments are subject to submission for textual similarity review by Turnitin.com. Assignments submitted to Turnitin.com will be included as source documents in Turnitin.com's restricted access database solely for the purpose of detecting plagiarism in such documents. The instructor may require students to submit their assignments electronically to Turnitin.com or the instructor may submit questionable text on behalf of a student. The terms that apply to Ontario Tech University's use of the Turnitin.com service are described on the Turnitin.com website.

Students who do not wish to have their work submitted to Turnitin.com must provide with their assignment at the time of submission to the instructor a signed Turnitin.com Assignment Cover sheet: Signed Turnitin Coversheet to Withdraw Permission to Submit Work.

18. Online Test and Exam Proctoring (Virtual Proctoring)

Ontario Tech University will conduct virtual monitoring of examinations in accordance with Ontario privacy legislation and all approved policy instruments.

19. Final Examinations (if applicable)

Final examinations are held during the final examination period at the end of the semester and may take place in a different room and on a different day from the regularly scheduled class. Check the published Examination Schedule for a complete list of days and times.

Students are required to show their valid physical or digital Ontario Tech University student photo ID card (campus ID), or a valid government issued photo ID that is in English when writing an **in-person examination.** Students are advised to obtain their Student ID Card well in advance of the examination period as they will not be able to write their examinations without it. More information on ID cards can be found at Information on Ontario Tech's Student ID Cards.

Students who are unable to write a final examination when scheduled due to religious publications may make arrangements to write a deferred examination. These students are required to submit an Academic Consideration form to the applicable Faculty as soon as possible and no later than three weeks prior to the first day of the final examination period.

Further information on final examinations can be found in the university's *Procedures for Final Examination Administration* Ontario Tech's Procedures for Final Examinations and in the Procedures for Consideration of Missed In-Term Course Work and Examinations.

20. Freedom of Information and Protection of Privacy Act

The following is an important notice regarding the process for submitting course assignments, quizzes, and other evaluative material in your courses in the Faculty of Business and IT.

Ontario Tech University is governed by the Freedom of Information and Protection of Privacy Act ("FIPPA"). In addition to providing a mechanism for requesting records held by the university, this legislation also requires that the University not disclose the personal information of its students without their consent.

FIPPA's definition of "personal information" includes, among other things, documents that contain both your name and your Banner (student) ID. For example, this could include graded test papers or assignments. To ensure that your rights to privacy are protected, the Faculty of Business and IT encourages you to use only your Banner ID on assignments or test papers being submitted for grading. This policy is intended to prevent the inadvertent disclosure of your information where graded papers are returned to groups of students at the same time. If you still wish to write both your name and your Banner ID on your tests and assignments, please be advised that Ontario Tech University will interpret this as an implied consent to the disclosure of your personal information in the normal course of returning graded materials to students.

If you have any questions or concerns relating to the new policy or the issue of implied consent addressed above, please contact accessandprivacy@ontariotechu.ca

Notice of Collection and Use of Personal Information
Throughout this course, personal information may be collected through the use of certain technologies under the authority of the *University of Ontario Institute of Technology Act, SO 2002, c. 8, Sch. O.* and will be collected, protected, used, disclosed and retained in compliance with Ontario's *Freedom of Information and Protection of Privacy Act R.S.O. 1990, c. F.31.*

This course will use the following technologies that may collect, use, disclose and retain personal information (including images) for the purposes described below:

- Respondus Monitor and Proctortrack to maintain academic integrity for examinations;
- Google Meet and Kaltura Virtual Classroom to facilitate remote instruction and interactive learning;
- Peer-shared applications, services or technologies that may be reviewed, assessed, or used as part of coursework.
- Other applications, services, or technologies that support or enhance online learning that include, but are not limited to, the following: Internet and Webcam.

For more information relating to these technologies, we encourage you to visit: Educational Technologies used at Ontario Tech.

Questions regarding personal information may be directed to: Ontario Tech University Access and Privacy Office, 2000 Simcoe Street North, Oshawa, ON L1G 0C5, email: accessandprivacy@ontariotechu.ca.

By remaining enrolled in this course, you acknowledge that you have read, understand, and agree to the terms and conditions under which the technology provider(s) may collect, use, disclose and retain your personal information. You agree to the university using the technologies and using your personal information for the purposes described in this course outline.

21. Human Rights and Respect

Ontario Tech University is committed to providing a campus environment in which all University Members are treated with dignity and to fostering a climate of understanding and mutual respect. The University will not tolerate, ignore or condone Discrimination or Harassment by or against anyone. Examples of Harassing behavior include, but are not limited to; bullying, taunting or mocking someone's race or creed, ridiculing an individual's disability, or targeting individuals with unwanted sexual or negative stereotypical comments about one's sex, gender, sexual orientation, gender identity and/or gender expression. Pursuant to Ontario Tech's Respectful Campus Policy, students are reminded of their role in ensuring an equitable and inclusive learning environment. Requirements to refrain from harassment and discrimination apply broadly to on campus activities, e.g., on University property, in the classroom, including in lectures, labs and practicums, and also apply to off-campus activities, e.g. during any organized Ontario Tech class or extra-curricular activity including experiential learning opportunities such as co-op, practicum or during research endeavors, during official Ontario Tech events or using University equipment and technological tools that facilitate remote learning, e.g., class and other chat functions, video conferencing, and electronic mail.

22. Freedom of Expression

Pursuant to Ontario Tech's Freedom of Expression Policy, all students are encouraged to express ideas and perspectives freely and respectfully in university space and in the online university environment, subject to certain limitations. Students are reminded that the limits on Freedom of Expression include speech or behaviour that: is illegal or interferes with the university's legal obligations; defames an individual or group; constitutes a threat, harassment or discrimination; is a breach of fiduciary, contractual, privacy or confidentiality obligations or commitments; and unduly disrupts and interferes with the functioning of the university. In the context of working online, different forms of communication are used. Where permitted, students using "chat" functions or other online forms of communication are encouraged to ensure that their communication complies with the Freedom of Expression Policy.

23. Copyright Notice

All Teaching Materials, as they are defined under Ontario Tech's Intellectual Property policy ("IP Policy"), provided by the instructor throughout the course, including, but not limited to, in whole or in part, course notes, teaching notes, custom books, tutorials, evaluation tools, presentations and examinations are subject to the Copyright Act, R.S.C., 1985, c. C-42 and the IP Policy. Subject to the IP Policy, Teaching Materials are owned by the faculty member, instructor or other third party who creates such works, with a license to the University. The copyright owner(s) reserves all intellectual property rights in and to the foregoing materials. Consistent with the IP Policy, Teaching Materials are intended to be used by Ontario Tech University students registered in the course that is the subject of this course outline for educational purposes only. Any distribution or publishing of this material (e.g., uploading material to a third-party website) by a student is strictly prohibited under the law unless the student has obtained the copyright owner's prior written consent. Any violation of copyright law or the IP Policy, if proven, may be subject to sanction as academic misconduct, and/or under the Student Conduct Policy.

24. Student Course Feedback Surveys

Student evaluation of teaching is a highly valued and helpful mechanism for monitoring the quality of Ontario Tech University’s programs and instructional effectiveness. To that end, course evaluations are administered by an external company in an online, anonymous process during the last few weeks of classes. Students are encouraged to participate actively in this process and will be notified of the dates. Notifications about course evaluations will be sent via e-mail, and posted on Canvas, Weekly News, and signage around the campus.

25. AODA

The Accessibility for Ontarians with Disabilities Act (AODA) standards have been considered in the development of this model course template and it adheres to the principles outlined in the University’s Accessibility Policy.

OntarioTech UNIVERSITY

FACULTY OF BUSINESS AND IT

INFR 6110G: Global Cybersecurity Threats

Course outline for **Fall 2023**

1. Course Details & Important Dates*

Term	Course Type	Day	Time	Location	CRN #
FALL 2023					

Classes Start	Classes End	**Last day to drop course without academic consequence**	Final Exam Period
September 5, 2023	December 4, 2023	October 2, 2023	December 6 - 16, 2023

* Visit Ontario Tech's Important Dates and Deadlines for other dates.

2. Instructor Contact Information

Instructor Name	Office	Phone	Email
Office Hours:			

Laboratory/Teaching Assistant Name	Office	Phone	Email
Office Hours:			

3. Course Description

In a hyper connected world, threat actors see no limits or boundaries to their targets, and cybersecurity incidents can have major effects on individuals, organizations, and governments around the world. Cybersecurity managers find themselves obliged to learn about the latest cyber threats to protect their digital assets. The objective of this course is to learn about the global power dynamics, conflicts and risk factors in cyberspace; cyber-based sabotage, espionage and subversion activities; and major and recent cyber incidents that have unfolded internationally and to evaluate their implications. Students will also go over recent threat reports from various security organizations to learn about how the global cyberthreat landscape is evolving.

3. Learning Outcomes

On the successful completion of the course, students will be able to:

- Describe the nature of cyber threats at the global level

- Understand how leading organizations, regulators and governments around the world analyze and prepare for global threats.
- Analyze various threat reports from various sources to understand the cyber threat Landscape and develop cybersecurity strategies.
- Analyze the intrigued world of global cybersecurity threats, opportunities, risks, and policies.
- Develop some actionable information on emerging global cybersecurity threats.

5. Course Design

The course will be structured to include a variety of pedagogy exercises including case studies, reports analysis, guest speakers, lectures, classroom discussions, and student presentations. Students are expected to participate in all discussions in the classroom. For some activities, teams maybe be formed by the instructors, with each team assigned different activities,

6. Outline of Topics in the Course

Given the dynamic nature of the course that focuses on state-of-the-art threats, the topics in the course are determined on a year-to-year basis. Some core topics are included in the table below:

Lecture #	Date	Time	Topics	Details of topics to be covered in the course, by unit or by week
1			Fundamentals of Cyber warfare	
2			Global Cyber threats	
3			Analysis of cyber incidents	
4			Geopolitics and Cyber power	
	October 9, 2023		Thanksgiving Day, no scheduled academic activities.	
STUDY BREAK	October 10 to 15, 2023		Study Break, no scheduled academic activities.	
5			Hacktivism	
6			Cyber Deterrence and surveillance	
7			Global issues related to ethics and legality of cyber warfare	
			Student Presentations	
			Student Presentations	
	December 5, 2023		Study break, no scheduled academic activities.	

7. Required Texts/Readings

There is no textbook required for this course.
Students will be assigned various articles on each topic, including the latest threat reports from various security organizations.
Students will also be assigned cases and students finding weekly news cybersecurity nuggets.

Additional readings may be assigned or recommended during the course.

8. Evaluation Method

Students will be evaluated based on their participation in the class.
Students will also be required to submit a cumulative "portfolio" assignment of "what happened in the 12 weeks during the term." Here is a tentative percentage for each work:

- Class participation: 50%
- Presentation: 30%
- Peer evaluation 20%

Final course grades may be adjusted to conform to program or Faculty grade distribution profiles. Further information on grading can be found at: Ontario Tech's Academic regulations

9. Assignments and Tests

[Provide a schedule of term assignments (format, description, length, due dates, submission requirements, etc.), tests and examinations. If collaborative group work is component of the course, include a statement that sets out the roles and roles and responsibilities of members for their own work and for the work of the other members of the group. Detail also how missed/late assignment and medical excuses will be managed in accordance with Faculty rules.]

Step #1: If you have midterms/term tests in your course, you **MUST** include the "Missed Term Test" paragraph below.

Missed Term Test
Students who miss a midterm or term test may submit a request for deferral using an Academic Consideration form, along with supporting documentation to the Faculty Advising offices within three (3) working days. We do not require students to submit Ontario Tech University Medical Statements at this time. If a midterm or term test is missed for approved reasons, the weight of the missed component will be added to the final (or select this sentence: a make-up test will be offered at a date set by the course instructor). If you miss the midterm or term test and do not follow the procedure above, you will receive a score of zero on the missed component.

All forms can also be found through MyOntarioTech or on the Ontario Tech University website.

Step #2: If you have no midterms/term tests in your course, however have coursework/ quizzes/ assignments you **MUST select** Option #1 OR Option #2 of the "Missed Course Work" paragraphs (below).

If you also have a coursework/quiz/assignment component in addition to midterms/term tests you **MUST** include the "Missed Term Test" paragraph (above) AND select Option #1 OR Option #2 of the "Missed Course Work" paragraphs(below).

Select - Option #1: Missed Course Work
Coursework missed for medical or serious personal reasons must be documented and reported to the instructor within three (3) working days of the missed work using an Academic Consideration form. Coursework includes, but is not limited to, quizzes; written assignments; participation; case

studies; etc… If missed coursework totals more than 25% of the final grade, this must be documented through the FBIT Academic Advising office. The weight of the missed course component will be reweighted to … (or select this sentence: the instructor will contact you regarding a make-up assignment) If you miss coursework and do not notify the instructor within the three (3) working day deadline, you will receive a score of zero on the missed component.

Or Select - Option #2: Missed Course Work
To cover any coursework missed due to unexpected absences, the lowest (out of xx) quizzes/assignments/journals/seminars/etc… will be dropped. Please note that this provision is not a free ticket to skip coursework as there will be no make-up quizzes/assignments/journals/seminars/etc for the missed ones.

(**REMOVE** this paragraph **after you have read**): The object of these paragraphs is to note that any missed assignment/quiz/coursework that is worth LESS than 25% of the final grade in the course will be **handled by the course instructor NOT** the FBIT Advising Office. As in the past, any missed final exam or test/assignment/midterm worth 25% or more of the final grade will be administered through the FBIT Advising Office.

10. Technology Requirements and Learning Management System Information

Ontario Tech uses *Canvas*™ as its learning management system (LMS). Access to the LMS is limited to students formally registered in courses. That access is for the duration of the semester **and for an additional 120 days once the semester is over**. Students are strongly encouraged to download any/all relevant course material during that access period. Any requests for access post this period must be made in writing to the instructor/faculty member responsible for the course.

To support online learning, the university recommends certain technology requirements for laptops, software and internet connectivity which are available at: Ontario Tech's Remote Learning Policies.

Students experiencing technical difficulties such that they are unable to meet the technology requirements may contact the IT Service Help Desk at: servicedesk@dc-uoit.ca
Students experiencing financial difficulties such that they are unable to meet the technology requirements may contact Student Awards and Financial Aid Office at: connect@ontariotehu.ca

By remaining enrolled in this course, you acknowledge that you have read, understand and agree to observe the Recommended Technology Requirements for accessing university online learning resources, including those minimum requirements that are specific to your faculty and program.

11. Sensitive/Offensive Subject Matter

The classroom (both physical and virtual) is intended to provide a safe, open space for the critical and civil exchange of ideas and opinions. Some articles, media and other course materials may contain sensitive content that is offensive and/or disturbing. For example, some articles or videos may contain [Instructors should provide examples that are applicable to the course subject matter – e.g. graphical depictions of violence, profanity, human anatomy, sexual acts, matters pertaining to race, gender, or sexuality]. The Course Instructor will try to identify such material and communicate warnings to students in advance of the distribution and use of such materials, affording students the choice to either emotionally prepare for, or not to view or interact with, the content. [Instructors should publish a warning statement in advance so as to give students adequate opportunity to make a choice to avoid any such matter. The following is a sample disclaimer: "The content you are about to view contains sensitive subject matter that may be considered offensive and/or disturbing to some viewers. By viewing and/or interacting with the content you acknowledge and agree that it is your decision to view and interact with the content and to take the risk that you will experience a negative emotional response or reaction to the nature of the content."]

12. Student Support

Any student who faces challenges securing their food or housing and believes this may affect their performance in the course is urged to contact studentlife@ontariotechu.ca for support. Furthermore, please notify your professor if you are comfortable in doing so. This will enable them to provide any resources and help that they can.

13. Sexual Violence Support and Education

Ontario Tech is committed to the prevention of sexual violence in all its forms. For any student who has experienced Sexual Violence, Ontario Tech can help. We will make accommodations to cater to the diverse backgrounds, cultures, and identities of students when dealing with individual cases.

If you think you have been subjected to or witnessed sexual violence:

- Reach out to a Support Worker, a specially trained individual authorized to receive confidential disclosures about incidents of sexual violence. Support Workers can offer help and resolution options which can include safety plans, accommodations, mental health support, and more. To make an appointment with a Support Worker, call 905.721.3392 or email studentlife@ontariotechu.ca

- Learn more about your options at: Ontario Tech's Policy on Sexual Violence and Support Information

14. Students with Disabilities

Accommodating students with disabilities at Ontario Tech is a responsibility shared among various partners: the students themselves, SAS staff and faculty members. To ensure that disability-related concerns are properly addressed during this course, students with documented disabilities and who may require assistance to participate in this class are encouraged to speak with me as soon as possible. **Students who suspect they have a disability that may affect their participation in this course are advised to go to Student Accessibility Services (SAS) as soon as possible.** Maintaining communication and working collaboratively with SAS and faculty members will ensure you have the greatest chance of academic success.

When on campus access is allowed, students taking courses on North Oshawa campus can visit Student Accessibility Services in Shawenjigewining Hall. Students taking courses on the **downtown Oshawa campus** can visit Student Accessibility Services in Charles Hall, Room 225.

Disability-related and accommodation support is available for students with mental health, physical, mobility, sensory, medical, cognitive, or learning challenges. Office hours are 8:30am-4:30pm, Monday, Tuesday, Thursday, and Friday, Wednesday's 10:00 am to 4:30. Please note they are closed each day between noon and 1:00 pm. For more information on services provided, you can visit the SAS website at Ontario Tech's Student Accessibility Services (SAS). Students may contact Student Accessibility Services by calling 905-721-3266, or email studentaccessibility@ontariotechu.ca.

When on campus access is allowed, students who require the use of the Test Centre to write tests, midterms, or quizzes MUST register online using the SAS test/exam sign-up module, found here Registration Link to write examinations in SAS at Ontario Tech. Students must sign up for tests, midterms, or quizzes AT LEAST seven (7) days before the date of the test.

Students must register for final exams by the registration deadline, which is typically two (2) weeks prior to the start of the final examination period. SAS will notify students of the registration deadline date.

15. Professional Suitability (if applicable)

Ontario Tech University is a community that values and promotes respect, integrity, diversity and accountability among all members of the university. These values can only be achieved in an environment that supports and protects the safety and security of its members. The Ontario Tech University Policy on Student Conduct defines and guides standards of student behaviour at the university to uphold these values and ensure that behaviour contrary to these standards are dealt with in a manner that is fair, open and effective.

The Faculty of Business & IT has the following expectations related to professionalism for all its community members, including without limitation, students, Staff, and Faculty:

- **Respect, civility, and courtesy:** Community members are expected to treat each other with respect, civility, and courtesy both in and outside of the classroom. Rudeness, profanity, insults, harassment, and class disruptions are unacceptable.
- **Critique ideas, not the people who raise the ideas:** Discussions, debates, and the exchange of ideas are normal parts of life in an academic community. Community members are expected to engage in discussions, debates, and the exchange of ideas in respectful ways, even while vigorously advocating for one's perspective.
- **Talk *to* those with whom you have a complaint, not *about* them.** When community members have disputes, complaints, and/or concerns about another community member, they are expected to do their best to address the matter directly and informally with the other member, provided that it is safe to do so. (See Appendix A for more information about how students can raise concerns about academic matters.)
- **Special obligations:** Community members in positions of authority have special obligations to demonstrate respect, civility, and professionalism and to encourage the development of these values within the FBIT community.

The *Professional Suitability* policy can be found at Ontario Tech's Professional Suitability Policy and the related procedures are hosted at Ontario Tech's Professional Suitability Procedures.

16. Academic Integrity

Students and faculty at Ontario Tech University share an important responsibility to maintain the integrity of the teaching and learning relationship. This relationship is characterized by honesty, fairness and mutual respect for the aim and principles of the pursuit of education. Academic misconduct impedes the activities of the university community and is punishable by appropriate disciplinary action.

Students are expected to be familiar with and abide by Ontario Tech University's regulations on Academic Conduct which sets out the kinds of actions that constitute academic misconduct, including plagiarism, copying or allowing one's own work to copied, use of unauthorized aids in examinations and tests, submitting work prepared in collaboration with another student when such collaboration has not been authorized, among other academic offences. The regulations also describe the procedures for dealing with allegations, and the sanctions for any finding of academic misconduct, which can range from a resubmission of work to a failing grade to permanent expulsion from the university. A lack of familiarity with these regulations on academic conduct does not constitute a defense against its application. This information can be found at Ontario Tech's Academic Integrity Policy.

Extra support services are available to all Ontario Tech University students in academic development, study skills, counseling, and peer mentorship. More information on student support services can be found at Academic Support at Ontario Tech's Student Learning Centre.

17. Turnitin (if applicable)

Ontario Tech University and faculty members reserve the right to use electronic means to detect and help prevent plagiarism. Students agree that by taking this course all assignments are subject to submission for textual similarity review by Turnitin.com. Assignments submitted to Turnitin.com will be included as source documents in Turnitin.com's restricted access database solely for the purpose of detecting plagiarism in such documents. The instructor may require students to submit their assignments electronically to Turnitin.com or the instructor may submit questionable text on behalf of a student. The terms that apply to Ontario Tech University's use of the Turnitin.com service are described on the Turnitin.com website.

Students who do not wish to have their work submitted to Turnitin.com must provide with their assignment at the time of submission to the instructor a signed Turnitin.com Assignment Cover sheet: Signed Turnitin Coversheet to Withdraw Permission to Submit Work.

18. Online Test and Exam Proctoring (Virtual Proctoring)

Ontario Tech University will conduct virtual monitoring of examinations in accordance with Ontario privacy legislation and all approved policy instruments.

19. Final Examinations (if applicable)

Final examinations are held during the final examination period at the end of the semester and **when on campus access is allowed,** may take place in a different room and on a different day from the regularly scheduled class. Check the published Examination Schedule for a complete list of days and times.

Students are required to show their Student ID card (campus ID) when **in-person examinations are allowed.** Students are advised to obtain their Student ID Card well in advance of the examination period as they will not be able to write their examinations without it. More information on ID cards can be found at Information on Ontario Tech's Student ID Cards.

Students who are unable to write a final examination when scheduled due to religious publications may make arrangements to write a deferred examination. These students are required to submit a Request for Accommodation for Religious Obligations to the Faculty concerned as soon as possible and no later than three weeks prior to the first day of the final examination period.

Further information on final examinations can be found at Ontario Tech's Procedures for Final Examinations.

20. Freedom of Information and Protection of Privacy Act

The following is an important notice regarding the process for submitting course assignments, quizzes, and other evaluative material in your courses in the Faculty of Business and IT.

Ontario Tech University is governed by the Freedom of Information and Protection of Privacy Act ("FIPPA"). In addition to providing a mechanism for requesting records held by the university, this legislation also requires that the University not disclose the personal information of its students without their consent.

FIPPA's definition of "personal information" includes, among other things, documents that contain both your name and your Banner (student) ID. For example, this could include graded test papers or assignments. To ensure that your rights to privacy are protected, the Faculty of [Insert Faculty name] encourages you to use only your Banner ID on assignments or test papers being submitted for grading. This policy is intended to prevent the inadvertent disclosure of your information where graded papers are returned to groups of students at the same time. If you still wish to write both your name and your Banner ID on your tests and assignments, please be advised that Ontario Tech

University will interpret this as an implied consent to the disclosure of your personal information in the normal course of returning graded materials to students.

If you have any questions or concerns relating to the new policy or the issue of implied consent addressed above, please contact accessandprivacy@ontariotechu.ca

Notice of Collection and Use of Personal Information
Throughout this course, personal information may be collected through the use of certain technologies under the authority of the *University of Ontario Institute of Technology Act, SO 2002, c. 8, Sch. O.* and will be collected, protected, used, disclosed and retained in compliance with Ontario's *Freedom of Information and Protection of Privacy Act R.S.O. 1990, c. F.31.*

This course will use the following technologies that may collect, use, disclose and retain personal information (including images) for the purposes described below: [Instructors should edit this section according to the systems and technologies to be used in this specific course (e.g. If using Proctortrack, remove any reference to Respondus)]

- Respondus Monitor and Proctortrack to maintain academic integrity for examinations;
- Google Meet and Kaltura Virtual Classroom to facilitate remote instruction and interactive learning;
- Peer-shared applications, services or technologies that may be reviewed, assessed, or used as part of coursework.
- Other applications, services, or technologies that support or enhance online learning that include, but are not limited to, the following: [Instructor to list all relevant components].

For more information relating to these technologies, we encourage you to visit: Educational Technologies used at Ontario Tech. Questions regarding personal information may be directed to: Ontario Tech University Access and Privacy Office, 2000 Simcoe Street North, Oshawa, ON L1G 0C5, email: accessandprivacy@ontariotechu.ca.

By remaining enrolled in this course, you acknowledge that you have read, understand, and agree to the terms and conditions under which the technology provider(s) may collect, use, disclose and retain your personal information. You agree to the university using the technologies and using your personal information for the purposes described in this course outline.

21. Human Rights and Respect

Ontario Tech University is committed to providing a campus environment in which all University Members are treated with dignity and to fostering a climate of understanding and mutual respect. The University will not tolerate, ignore or condone Discrimination or Harassment by or against anyone. Examples of Harassing behavior include, but are not limited to; bullying, taunting or mocking someone's race or creed, ridiculing an individual's disability, or targeting individuals with unwanted sexual or negative stereotypical comments about one's sex, gender, sexual orientation, gender identity and/or gender expression. Pursuant to Ontario Tech's Respectful Campus Policy, students are reminded of their role in ensuring a campus environment that is equitable and inclusive. Requirements to refrain from harassment and discrimination apply broadly to the classroom, including in lectures, labs and practicums, as well as through the use of sanctioned and unsanctioned technological tools that facilitate remote learning, e.g. class and other chat functions, video conferencing, electronic mail and texts, and social media content amongst or about University students, faculty and staff.

22. Freedom of Expression

Pursuant to Ontario Tech's Freedom of Expression Policy, all students are encouraged to express ideas and perspectives freely and respectfully in university space and in the online university environment, subject to certain limitations. Students are reminded that the limits on Freedom of Expression include speech or behaviour that: is illegal or interferes with the university's legal obligations; defames an individual or group; constitutes a threat, harassment or discrimination; is a breach of fiduciary, contractual, privacy or confidentiality obligations or commitments; and unduly disrupts and interferes with the functioning of the university. In the context of working online, different forms of communication are used. Where permitted, students using "chat" functions or other online forms of communication are encouraged to ensure that their communication complies with the Freedom of Expression Policy.

23. Copyright Notice

All teaching materials provided by the instructor throughout the course, including, but not limited to, in whole or in part, recorded lectures, slides, videos, diagrams, case studies, assignments, quizzes, and examinations are subject to the Copyright Act, R.S.C., 1985, c. C-42. Teaching materials are owned by the faculty member, instructor or other third party who creates such works. The copyright owner(s) reserves all intellectual property rights in and to the teaching materials, including the sole right to copy, reproduce, distribute, and modify the teaching materials. Consistent with the university's Intellectual Property Policy, teaching materials are intended only for the educational use of Ontario Tech University students registered in the course that is the subject of this course outline. Any distribution or publishing of this material (e.g. uploading material to a third-party website) is strictly prohibited under the law unless the student has obtained the copyright owner's prior written consent. Any violation of copyright law or the Intellectual Property Policy, if proven, may be subject to sanction as academic misconduct, and/or under the Student Conduct Policy.

24. Student Course Feedback Surveys

Student evaluation of teaching is a highly valued and helpful mechanism for monitoring the quality of Ontario Tech University's programs and instructional effectiveness. To that end, course evaluations are administered by an external company in an online, anonymous process during the last few weeks of classes. Students are encouraged to participate actively in this process and will be notified of the dates. Notifications about course evaluations will be sent via e-mail, and posted on Canvas, Weekly News, and signage around the campus.

University Response to COVID-19

The government response to the COVID-19 pandemic is continually evolving. As new information becomes available from federal and provincial public health authorities, the Province of Ontario and the Regional Municipality of Durham, Ontario Tech University will remain nimble and prepared to respond to government orders, directives, guidelines and changes in legislation to ensure the health and safety of all members of its campus community. In accordance with public health recommendations, the university may need to adjust the delivery of course instruction and the availability and delivery mode of campus services and co-curricular opportunities. Ontario Tech University appreciates the understanding and flexibility of our students, faculty and staff as we continue to navigate the pandemic and work together to demonstrate our strong commitment to academic, research and service excellence during these challenging and unprecedented times.

The Accessibility for Ontarians with Disabilities Act (AODA) standards have been considered in the development of this model course template and it adheres to the principles outlined in the University's Accessibility Policy.

Ontario Tech University acknowledges the lands and people of the Mississaugas of Scugog Island First Nation. We are thankful to be welcomed on these lands in friendship. The lands we are situated on are covered under the Williams Treaties and the traditional territory of the Mississaugas, a branch of the greater Anishinaabeg Nation, including Algonquin, Ojibway, Odawa and Pottawatomi. These lands remain home to a number of Indigenous nations and people.

We acknowledge this land out of respect for the Indigenous nations who have cared for Turtle Island, also called North America, from before the arrival of settler peoples until this day. Most importantly, we remember the history of these lands has been tainted by poor treatment and a lack of friendship with the First Nations who call them home.

This history is something we are all affected by as we are all treaty people in Canada. We all have a shared history to reflect on, and each of us is affected by this history in different ways. Our past defines our present, but if we move forward as friends and allies, then it does not have to define our future.

FACULTY OF BUSINESS AND IT

INFR 6120G: Cybersecurity Leadership
Course outline for XXX

1. Course Details & Important Dates*

Term	Course Type	Day	Time	Location	CRN#
----				Online	

Classes Start	Classes End	**Last day to drop course without academic consequence**	Final Exam Period
----	----	----	----

* Visit Ontario Tech's Important Dates and Deadlines for other dates.

Important Note – Final Exams

There is no final exam for this course

2. Instructor Contact Information

Instructor Name	Office	Phone	Email
Office Hours:			

Laboratory/Teaching Assistant Name	Office	Phone	Email
Office Hours:			

3. Course Description

This course examines the concept of leadership, how it works and specifically how it may be applied to the specific needs of cybersecurity. This includes leadership in times of normalcy, crisis and continuance. The course includes case discussions, roleplaying exercises and input as available from external cybersecurity experts. The course will be held in a hybrid format, with online and face to face discussions and exercises according to the availability of students.

4. Learning Outcomes

On the successful completion of the course, students will be able to:

- Analyze different leadership styles in the context of cybersecurity
- Construct and justify different actions in response to cybersecurity activities and events
- Demonstrate how leadership makes a difference in cybersecurity events
- Debate the strengths and weaknesses of different leadership styles in context

5. Course Design

This course is largely discussion-based, with a few lectures on the concepts of leadership and how it is different or similar in different cybersecurity concepts. We will use a case-based and discussion method to tease out the ways in which different leadership styles and the actions of leaders have led to different outcomes. There may well be visiting presenters who will share their expertise of how and when the different styles and requirements of leadership make sense, in 'normal', crisis and post-crisis settings. There will be ample opportunity to discuss the governance and leadership issues associated with the cases, as well as in a final 'war game' scenario and subsequent debriefing in which students will participate.

6. Outline of Topics in the Course

Week #	Topics	Details of topics to be covered in the course, by unit or by week
1	What do we mean by leadership? From philosophy to sociology through psychology. From stoicism to authoritarianism and beyond.	The Romans, the Greeks, "Great Man" Theory, military leadership, civilian leadership.
2	Leadership rules. Leadership actions. Leadership versus management.	Leadership styles, how leadership works in context.
3	Why cybersecurity needs leadership. What is different about cybersecurity?	The different timescales of cybersecurity. The different people and tools of cybersecurity. The similarities between cybersecurity and other areas.
4	Communication	How, why, when and again, how.

5	Normalcy	How to lead in uncertain and normal times, in different kinds of environment.
6	Crisis	The requirements of a crisis: pro-action, reaction, availability, communication, understanding.
7	Post-crisis and return to normalcy	What happens next? Who knows?
8	Legal concerns	The law in Canada and elsewhere as it relates to cybersecurity and why it impacts leadership requirements.
9	Recognizing and building new leaders in our field and work	Coaching and encouraging.
10	Incompetency and worse: There is no I in team	How to fail. How to spot failing. Self-assessment and self-regulation.
11	"War game"	
12	Debriefing	

7. Required Texts/Readings

There is no specific text assigned for the course. Cases will be assigned on a weekly basis to help discuss the concepts presented. Readings from different texts and articles will be required. All of these will be available in or through the university library (no purchase of texts will be required.)

Additional readings may be assigned or recommended during the course.

8. Evaluation Method

This is a course that requires people to participate.

There are weekly case discussions. Students will be expected to prepare and present a case assigned to them at some point during the semester. The presentation and analysis is worth 25% of the final grade for the course.

The 'war game' will be a **full day** session in which all students are expected to take part in different roles – it is a reactive simulation that is designed to examine the different ways in which leadership makes a difference in various situations. A report on what transpired is required per student and participation in the debrief session is also required.

War game participation and activity: 20%
Report: 15%
Debrief: 15%

Participation in the weekly sessions/discussions is worth up to 15% of the final grade.

Contribution to the ongoing course educational resource (an OER created and maintained by the class) is worth up to 15% of the final grade and opportunities to contribute will present themselves throughout the course.

Final course grades may be adjusted to conform to program or Faculty grade distribution profiles. Further information on grading can be found under Academic Regulations at: Ontario Tech's Academic regulations

9. Assignments and Tests

Weekly cases (at least one per student group).
Online and in class discussions (generally, topics will be assigned but can be requested).
OER contributions (to be discussed in class, due by end of semester).

Attendance at the weekly sessions/discussions is therefore mandatory. Up to two may be missed for personal or other reasons without penalty, but given the unique nature of what we are discussing and how, further absences will result in the student being unable to complete the course.

For information on how missed/late assignments and medical excuses are managed, please refer to the university's revised *Procedures for Consideration of Missed In-Term Course Work and Examinations*

10. Technology Requirements and Learning Management System Information

Ontario Tech uses *Canvas*™ as its learning management system (LMS). Access to the LMS is limited to students formally registered in courses. That access is for the duration of the semester **and for an additional 120 days once the semester is over**. Students are strongly encouraged to download any/all relevant course material during that access period. Any requests for access post this period must be made in writing to the instructor/faculty member responsible for the course.

To support online learning, the university recommends certain technology requirements for laptops, software and internet connectivity which are available at: Ontario Tech's Remote Learning Policies.

Students experiencing technical difficulties such that they are unable to meet the technology requirements may contact the IT Service Help Desk at: servicedesk@dc-uoit.ca
Students experiencing financial difficulties such that they are unable to meet the technology requirements may contact Student Awards and Financial Aid Office at: connect@ontariotehu.ca

By remaining enrolled in this course, you acknowledge that you have read, understand and agree to observe the Recommended Technology Requirements for accessing university online learning resources, including those minimum requirements that are specific to your faculty and program.

11. Sensitive/Offensive Subject Matter

The classroom (both physical and virtual) is intended to provide a safe, open space for the critical and civil exchange of ideas and opinions. Some articles, media and other course materials may contain sensitive content that is offensive and/or disturbing. The Course Instructor will try to identify such material and communicate warnings to students in advance of the distribution and use of such materials, affording students the choice to either emotionally prepare for, or not to view or interact with, the content

12. Student Support

Any student who faces challenges securing their food or housing and believes this may affect their performance in the course is urged to contact studentlife@ontariotechu.ca for support. Furthermore, please notify your professor if you are comfortable in doing so. This will enable them to provide any resources and help that they can.

13. Student Sexual Violence Support and Education

Ontario Tech is committed to the prevention of sexual violence in all its forms. For any student who has experienced Sexual Violence, Ontario Tech can help. We will make accommodations to cater to the diverse backgrounds, cultures, and identities of students when dealing with individual cases.

If you think you have been subjected to or witnessed sexual violence:

- Reach out to the gender-based case specialist in the Human Rights office, a specially trained individual authorized to receive confidential disclosures about incidents of sexual violence. The Human Rights Office will make support services, including counselling, access or referrals to medical services, safety planning and accommodations, available to Students affected by an Incident of Sexual Violence. Book a consultation with the Case Specialist for more information.

Learn more about your options at: Ontario Tech's Policy on Sexual Violence and Support Information.

14. Students with Disabilities

Ontario Tech University is committed to promoting an environment where everyone has an equal opportunity to contribute to their fullest potential. Students who require accommodation for a disability are advised to contact Student Accessibility Services (SAS) as soon as possible. Accommodation decisions will be made in accordance with the Ontario Human Rights Code. Accommodations will be consistent with and supportive of the essential requirements of courses and programs, and provided in a way that respects the dignity of students with disabilities and encourages integration and equality of opportunity. Reasonable academic accommodation may require instructors to exercise creativity and flexibility in responding to the needs of students with disabilities while maintaining integrity.

Disability-related and accommodation support is available for students with mental health, physical, mobility, sensory, medical, cognitive, or learning challenges. Office hours are 8:30am-4:30pm, Monday, Tuesday, Thursday, and Friday, Wednesday's 10:00 am to 4:30. Please note they are closed each day between noon and 1:00 pm. For more information on services provided, you can visit the SAS website at Ontario Tech's Student Accessibility Services (SAS). Students may contact Student Accessibility Services by calling 905-721-3266, or email studentaccessibility@ontariotechu.ca.

Students who require the use of the Test Centre to write tests, midterms, or quizzes MUST register online using the SAS test/exam sign-up module, found here Registration Link to write examinations in SAS at Ontario Tech. Students must sign up for tests, midterms, or quizzes **AT LEAST seven (7) working days before the date of the test.**

Students must register for final exams no later **than 3 weeks prior to the start of the final examination period**. The final examination period is given at Ontario Tech University's Important dates and deadlines.

15. Professional Suitability (if applicable)

Ontario Tech University is a community that values and promotes respect, integrity, diversity and accountability among all members of the university. These values can only be achieved in an environment that supports and protects the safety and security of its members. The Ontario Tech University Policy on Student Conduct defines and guides standards of student behaviour at the university to uphold these values and ensure that behaviour contrary to these standards are dealt with in a manner that is fair, open and effective.

The Faculty of Business & IT has the following expectations related to professionalism for all its community members, including without limitation, students, Staff, and Faculty:

- **Respect, civility, and courtesy:** Community members are expected to treat each other with respect, civility, and courtesy both in and outside of the classroom. Rudeness, profanity, insults, harassment, and class disruptions are unacceptable.
- **Critique ideas, not the people who raise the ideas:** Discussions, debates, and the exchange of ideas are normal parts of life in an academic community. Community members are expected to engage in discussions, debates, and the exchange of ideas in respectful ways, even while vigorously advocating for one's perspective.
- **Talk *to* those with whom you have a complaint, not *about* them.** When community members have disputes, complaints, and/or concerns about another community member, they are expected to do their best to address the matter directly and informally with the other member, provided that it is safe to do so.
- **Special obligations:** Community members in positions of authority have special obligations to demonstrate respect, civility, and professionalism and to encourage the development of these values within the FBIT community.

The *Professional Suitability* policy can be found at Ontario Tech's Professional Suitability Policy and the related procedures are hosted at Ontario Tech's Professional Suitability Procedures.

16. Academic Integrity

Students and faculty at Ontario Tech University share an important responsibility to maintain the integrity of the teaching and learning relationship. This relationship is characterized by honesty, fairness and mutual respect for the aim and principles of the pursuit of education. Academic misconduct impedes the activities of the university community and is punishable by appropriate disciplinary action.

Students are expected to be familiar with and abide by Ontario Tech University's regulations on Academic Conduct which sets out the kinds of actions that constitute academic misconduct, including plagiarism, copying or allowing one's own work to copied, use of unauthorized aids in examinations and tests, submitting work prepared in collaboration with another student when such collaboration has not been authorized, among other academic offences. The regulations also describe the procedures for dealing with allegations, and the sanctions for any finding of academic misconduct, which can range from a resubmission of work to a failing grade to permanent expulsion from the university. A lack of familiarity with these regulations on academic conduct does not constitute a defense against its application. Please note that generative artificial intelligence (GAI) tools should not be utilized without advance, specific written approval by the faculty member teaching the course.

More information can be found at Ontario Tech's Academic Integrity Policy.

Extra support services are available to all Ontario Tech University students in academic development, study skills, counseling, and peer mentorship. More information on student support services can be found at Academic Support at Ontario Tech.

17. Turnitin (if applicable)

Ontario Tech University and faculty members reserve the right to use electronic means to detect and help prevent plagiarism. Students agree that by taking this course all assignments are subject to submission for textual similarity review by Turnitin.com. Assignments submitted to Turnitin.com will be included as source documents in Turnitin.com's restricted access database solely for the purpose of detecting plagiarism in such documents. The instructor may require students to submit their assignments electronically to Turnitin.com or the instructor may submit questionable text on behalf of a student. The terms that apply to Ontario Tech University's use of the Turnitin.com service are described on the Turnitin.com website.

Students who do not wish to have their work submitted to Turnitin.com must provide with their assignment at the time of submission to the instructor a signed Turnitin.com Assignment Cover sheet: Signed Turnitin Coversheet to Withdraw Permission to Submit Work.

18. Online Test and Exam Proctoring (Virtual Proctoring)

Ontario Tech University will conduct virtual monitoring of examinations in accordance with Ontario privacy legislation and all approved policy instruments.

19. Final Examinations (if applicable)

Final examinations are held during the final examination period at the end of the semester and may take place in a different room and on a different day from the regularly scheduled class. Check the published Examination Schedule for a complete list of days and times.

Students are required to show their valid physical or digital Ontario Tech University student photo ID card (campus ID), or a valid government issued photo ID that is in English when writing an **in-person examination.** Students are advised to obtain their Student ID Card well in advance of the examination period as they will not be able to write their examinations without it. More information on ID cards can be found at Information on Ontario Tech's Student ID Cards.

Students who are unable to write a final examination when scheduled due to religious publications may make arrangements to write a deferred examination. These students are required to submit an Academic Consideration form to the applicable Faculty as soon as possible and no later than three weeks prior to the first day of the final examination period.

Further information on final examinations can be found in the university's *Procedures for Final Examination Administration* Ontario Tech's Procedures for Final Examinations and in the Procedures for Consideration of Missed In-Term Course Work and Examinations.

20. Freedom of Information and Protection of Privacy Act

The following is an important notice regarding the process for submitting course assignments, quizzes, and other evaluative material in your courses in the Faculty of Business and IT.

Ontario Tech University is governed by the Freedom of Information and Protection of Privacy Act ("FIPPA"). In addition to providing a mechanism for requesting records held by the university, this legislation also requires that the University not disclose the personal information of its students without their consent.

FIPPA's definition of "personal information" includes, among other things, documents that contain both your name and your Banner (student) ID. For example, this could include graded test papers or assignments. To ensure that your rights to privacy are protected, the Faculty of Business and IT encourages you to use only your Banner ID on assignments or test papers being submitted for grading. This policy is intended to prevent the inadvertent disclosure of your information where graded papers are returned to groups of students at the same time. If you still wish to write both your name and your Banner ID on your tests and assignments, please be advised that Ontario Tech University will interpret this as an implied consent to the disclosure of your personal information in the normal course of returning graded materials to students.

If you have any questions or concerns relating to the new policy or the issue of implied consent addressed above, please contact accessandprivacy@ontariotechu.ca

Notice of Collection and Use of Personal Information
Throughout this course, personal information may be collected through the use of certain technologies under the authority of the *University of Ontario Institute of Technology Act, SO 2002, c. 8, Sch. O.* and will be collected, protected, used, disclosed and retained in compliance with Ontario's *Freedom of Information and Protection of Privacy Act R.S.O. 1990, c. F.31.*

This course will use the following technologies that may collect, use, disclose and retain personal information (including images) for the purposes described below:

- Google Meet and Kaltura Virtual Classroom to facilitate remote instruction and interactive learning;
- Peer-shared applications, services or technologies that may be reviewed, assessed, or used as part of coursework.
- Other applications, services, or technologies that support or enhance online learning that include, but are not limited to, the following: pressbooks, mentimeter.

For more information relating to these technologies, we encourage you to visit: Educational Technologies used at Ontario Tech.

Questions regarding personal information may be directed to: Ontario Tech University Access and Privacy Office, 2000 Simcoe Street North, Oshawa, ON L1G 0C5, email: accessandprivacy@ontariotechu.ca.

By remaining enrolled in this course, you acknowledge that you have read, understand, and agree to the terms and conditions under which the technology provider(s) may collect, use, disclose and retain your personal information. You agree to the university using the technologies and using your personal information for the purposes described in this course outline.

21. Human Rights and Respect

Ontario Tech University is committed to providing a campus environment in which all University Members are treated with dignity and to fostering a climate of understanding and mutual respect. The University will not tolerate, ignore or condone Discrimination or Harassment by or against anyone. Examples of Harassing behavior include, but are not limited to; bullying, taunting or mocking someone's race or creed, ridiculing an individual's disability, or targeting individuals with unwanted sexual or negative stereotypical comments about one's sex, gender, sexual orientation, gender identity and/or gender expression. Pursuant to Ontario Tech's Respectful Campus Policy, students are reminded of their role in ensuring an equitable and inclusive learning environment. Requirements to refrain from harassment and discrimination apply broadly to on campus activities, e.g., on University property, in the classroom, including in lectures, labs and practicums, and also apply to off-campus activities, e.g. during any organized Ontario Tech class or extra-curricular activity including experiential learning opportunities such as co-op, practicum or during research endeavors, during official Ontario Tech events or using University equipment and technological tools that facilitate remote learning, e.g., class and other chat functions, video conferencing, and electronic mail.

22. Freedom of Expression

Pursuant to Ontario Tech's Freedom of Expression Policy, all students are encouraged to express ideas and perspectives freely and respectfully in university space and in the online university environment, subject to certain limitations. Students are reminded that the limits on Freedom of Expression include speech or behaviour that: is illegal or interferes with the university's legal obligations; defames an individual or group; constitutes a threat, harassment or discrimination; is a breach of fiduciary, contractual, privacy or confidentiality obligations or commitments; and unduly disrupts and interferes with the functioning of the university. In the context of working online, different forms of communication are used. Where permitted, students using "chat" functions or other online forms of communication are encouraged to ensure that their communication complies with the Freedom of Expression Policy.

23. Copyright Notice

All Teaching Materials, as they are defined under Ontario Tech's Intellectual Property policy ("IP Policy"), provided by the instructor throughout the course, including, but not limited to, in whole or in part, course notes, teaching notes, custom books, tutorials, evaluation tools, presentations and examinations are subject to the Copyright Act, R.S.C., 1985, c. C-42 and the IP Policy. Subject to the IP Policy, Teaching Materials are owned by the faculty member, instructor or other third party who creates such works, with a license to the University. The copyright owner(s) reserves all intellectual property rights in and to the foregoing materials. Consistent with the IP Policy, Teaching Materials are intended to be used by Ontario Tech University students registered in the course that is the subject of this course outline for educational purposes only. Any distribution or publishing of this material (e.g., uploading material to a third-party website) by a student is strictly prohibited under the law unless the student has obtained the copyright owner's prior written consent. Any violation of copyright law or the IP Policy, if proven, may be subject to sanction as academic misconduct, and/or under the Student Conduct Policy.

24. Student Course Feedback Surveys

Student evaluation of teaching is a highly valued and helpful mechanism for monitoring the quality of Ontario Tech University's programs and instructional effectiveness. To that end, course evaluations are administered by an external company in an online, anonymous process during the last few weeks of classes. Students are encouraged to participate actively in this process and will be notified of the dates. Notifications about course evaluations will be sent via e-mail, and posted on Canvas, Weekly News, and signage around the campus.

25. AODA

The Accessibility for Ontarians with Disabilities Act (AODA) standards have been considered in the development of this model course template and it adheres to the principles outlined in the University's Accessibility Policy.

FACULTY OF BUSINESS AND IT

INFR6130G: Cybercrime

Course outline for ****** 20****

1. Course Details & Important Dates*

Term	Course Type	Day	Time	Location	CRN #
-	Lecture	-	3 hours	-	-

Classes Start	Classes End	**Last day to drop course without academic consequence**	Final Exam Period
-	-	-	-

* Visit Ontario Tech's Important Dates and Deadlines for other dates.

Important Note – Final Exams
The final exam for this course will be run ON CAMPUS during the regular final exam period. If a student cannot attend due to COVID-19 related international travel restrictions you **must email your course instructor ASAP** (as soon as possible) regarding the possibility of alternate arrangements.

2. Instructor Contact Information

Instructor Name	Office	Phone	Email
Dr. Fletcher Lu	UB3062	905-721-8668 ext. 3761	fletcher.lu@ontariotechu.ca
Office Hours: TBA*			

Teaching Assistant Name	Office	Phone	Email

*TBA = To Be Announced

3. Course Description

This course covers different manifestations of cybercrime including hacking, viruses and other forms of malicious software. It presents technical and social issues of cybercrime, covers the origins and extent of the cybercrime problem, ethical and legal issues as well as analytical techniques to detect cybercrime.

4. Learning Outcomes

On the successful completion of the course, students will be able to:

1. Identify and describe techniques for cyber-fraud, online deception and scams,

2. Distinguish between criminal hacking, and non-criminal hacking.
3. Describe how computer technologies have altered the ways in which theft, terrorism, ransoming, fraud, and identity crimes are committed.
4. Identify and distinguish the various types of viruses and malicious code.
5. Identify and define the primary security technologies used to protect information.
6. Explain the conflicting roles within law enforcement pertaining to investigation vs. intelligence gathering.
7. Identify the legal issues related to various cybercrime activities both domestically and internationally.
8. Describe social issues related to cybercrime including cyberbullying and harassment.

5. Course Design

Many of the topics covered in this course are contemporary in nature and not adequately covered by any single textbook. Due to this contemporary nature, extensive online reading and material are required. Students are strongly recommended to attend lectures as not all material necessary for exams and assignments may appear on printed lecture notes, but instead are drawn from articles and postings that are cited and discussed during lectures. Thus, students will need to take comprehensive notes during lectures or be prepared to obtain another student's notes for any missed lectures. For missed lectures, it is the responsibility of the student to obtain such notes from another student and NOT from the instructor.

Online interactive computer tools will be used during lectures, thus students must bring their laptop with them to lectures and it is strongly encouraged to bring an internet cable to help reduce lag time due to the slower wireless transfer speeds.

6. Outline of Topics in the Course

Week #	Date	Time	Topics*
1	-	-	1. Introduction and Overview • Introduction to course • Overview of assignments, grading • Defining cybercrime • Current events, issues
2	-	-	2. Online fraud, email spam and scams • Peer to peer network dangers • Who is tracking your online activities • Phishing, Pharming, Spams and scams • Misinformation, Deception & Deep Fakes
3	-	-	3. Analytics for Crime Detection • Modeling methods • Probabilistic Association Rules • Training & outlier techniques
4	-	-	4. Computer viruses, spyware and attacks • Approaches, techniques and medium • Protection methods and mechanisms • DOS attacks
5	-	-	5. Theft, piracy and security issues • Theft and protections of identity and data • Approaches to commit identity and data theft

			• Legal and technological protections • Smartphone and WiFi issues • Midterm Review
6	-	-	Midterm
7	-	-	6. Online Surveillance • Surveillance through mobile and computer devices • Government, individual and business surveillance tactics • Tracking systems
8	-	-	7. Bullying, pornography and sex crimes • Stalking, bullying and harassment • Definitions, laws and protections • Sexual predators • Security measures • Protections
9	-	-	8. Advanced Techniques • Misinformation, DeepFakes and AI in cybercrime • Techniques for detection and prevention
10	-	-	Project Presentations
11	-	-	Project Presentations
12	-	-	Final Exam

*topic schedule subject to change

7. Required Texts/Readings

There is no required textbook, however additional readings are assigned or recommended during the course.

8. Evaluation Method

	Due Date[1]	**Percentage of Final Grade***
Assignment 1	-	15%
Midterm	-	15%
Assignment 2	-	15%
Term Project	*Written Report portion:* -	20%
	Oral Presentation portion: -	20%
Final Exam	-	15%

1. Due dates are subject to change, be sure to check the course Canvas account for updates/changes.
2. TBD = to be determined

**Final course grades may be adjusted to conform to program or Faculty grade distribution profiles. Further information on grading can be found at: Ontario Tech's Academic regulations*

9. Assignments and Tests

All assignments must be submitted on or before the due date and time. No late submissions will be accepted unless accompanied by an acceptable excuse (medical or compassionate with supporting documentation) that has been approved by the instructor. All late submissions without an approved excuse by the instructor will receive a mark of zero. Note: technical difficulties due to such issues as a slow or dropped connection, lag on server, etc. are NOT approvable excuses. Students are strongly encouraged to avoid such difficulties by following a principle of submitting both early and often before the due date/time. The principle behind 'early and often' submission is that as soon as you have some work done such as part of one question, submit it so you always avoid getting a zero due to a missed or late assignment as you will have at least something submitted. And then keep resubmitting as you complete more of the assignment material.

Assignments will be posted on the Canvas system with submissions handed in electronically through Canvas. The term project has both a written and oral presentation component. The written component is due all on the same due date. For the project, students will work in groups and each group will be randomly assigned to a presentation date. Each group member is required to participate in the oral presentation. It is the responsibility of the group members to ensure that work is equitably shared among the group's members.

Missed Term Test
Students who miss a midterm or term test may submit a request for deferral using an Academic Consideration form, along with supporting documentation to the Faculty Advising offices within three (3) working days. We do not require students to submit Ontario Tech University Medical Statements at this time. If a midterm or term test is missed for approved reasons, the weight of the missed component will be added to the final. If you miss the midterm or term test and do not follow the procedure above, you will receive a score of zero on the missed component.

All forms can also be found through MyOntarioTech or on the Ontario Tech University website.

Missed Course Work
Coursework missed for medical or serious personal reasons must be documented and reported to the instructor within three (3) working days of the missed work using an Academic Consideration form. Coursework includes, but is not limited to, quizzes; written assignments; participation; case studies; etc… If missed coursework totals more than 25% of the final grade, this must be documented through the FBIT Academic Advising office. The weight of the missed course component will be reweighted to the final exam. If you miss coursework and do not notify the instructor within the three (3) working day deadline, you will receive a score of zero on the missed component.

10. Technology Requirements and Learning Management System Information

Ontario Tech uses *Canvas*™ as its learning management system (LMS). Access to the LMS is limited to students formally registered in courses. That access is for the duration of the semester **and for an additional 120 days once the semester is over**. Students are strongly encouraged to download any/all relevant course material during that access period. Any requests for access post this period must be made in writing to the instructor/faculty member responsible for the course.

To support online learning, the university recommends certain technology requirements for laptops, software and internet connectivity which are available at: Ontario Tech's Remote Learning Policies.

Students experiencing technical difficulties such that they are unable to meet the technology requirements may contact the IT Service Help Desk at: servicedesk@dc-uoit.ca
Students experiencing financial difficulties such that they are unable to meet the technology requirements may contact Student Awards and Financial Aid Office at: connect@ontariotehu.ca

By remaining enrolled in this course, you acknowledge that you have read, understand and agree to observe the Recommended Technology Requirements for accessing university online learning resources, including those minimum requirements that are specific to your faculty and program.

11. Sensitive/Offensive Subject Matter

The classroom (both physical and virtual) is intended to provide a safe, open space for the critical and civil exchange of ideas and opinions. Some articles, media and other course materials may contain sensitive content that is offensive and/or disturbing. For example, some articles or videos may contain depictions of violence, profanity, human anatomy, sexual acts, matters pertaining to race, gender, or sexuality. The Course Instructor will try to identify such material and communicate warnings to students in advance of the distribution and use of such materials, affording students the choice to either emotionally prepare for, or not to view or interact with, the content.

12. Student Support

Any student who faces challenges securing their food or housing and believes this may affect their performance in the course is urged to contact studentlife@ontariotechu.ca for support. Furthermore, please notify your professor if you are comfortable in doing so. This will enable them to provide any resources and help that they can.

13. Sexual Violence Support and Education

Ontario Tech is committed to the prevention of sexual violence in all its forms. For any student who has experienced Sexual Violence, Ontario Tech can help. We will make accommodations to cater to the diverse backgrounds, cultures, and identities of students when dealing with individual cases.

If you think you have been subjected to or witnessed sexual violence:

- Reach out to a Support Worker, a specially trained individual authorized to receive confidential disclosures about incidents of sexual violence. Support Workers can offer help and resolution options which can include safety plans, accommodations, mental health support, and more. To make an appointment with a Support Worker, call 905.721.3392 or email studentlife@ontariotechu.ca
- Learn more about your options at: Ontario Tech's Policy on Sexual Violence and Support Information

14. Students with Disabilities

Accommodating students with disabilities at Ontario Tech is a responsibility shared among various partners: the students themselves, SAS staff and faculty members. To ensure that disability-related concerns are properly addressed during this course, students with documented disabilities and who may require assistance to participate in this class are encouraged to speak with me as soon as possible. **Students who suspect they have a disability that may affect their participation in this course are advised to go to Student Accessibility Services (SAS) as soon as possible.** Maintaining communication and working collaboratively with SAS and faculty members will ensure you have the greatest chance of academic success.

When on campus access is allowed, students taking courses on North Oshawa campus can visit Student Accessibility Services in Shawenjigewining Hall. Students taking courses on the **downtown Oshawa campus** can visit Student Accessibility Services in Charles Hall, Room 225.

Disability-related and accommodation support is available for students with mental health, physical, mobility, sensory, medical, cognitive, or learning challenges. Office hours are 8:30am-4:30pm, Monday, Tuesday, Thursday, and Friday, Wednesday's 10:00 am to 4:30. Please note they are closed each day between noon and 1:00 pm. For more information on services provided, you can visit the SAS website at Ontario Tech's Student Accessibility Services (SAS). Students may contact Student Accessibility Services by calling 905-721-3266, or email studentaccessibility@ontariotechu.ca.

When on campus access is allowed, students who require the use of the Test Centre to write tests, midterms, or quizzes MUST register online using the SAS test/exam sign-up module, found here Registration Link to write examinations in SAS at Ontario Tech. Students must sign up for tests, midterms, or quizzes AT LEAST seven (7) days before the date of the test.

Students must register for final exams by the registration deadline, which is typically two (2) weeks prior to the start of the final examination period. SAS will notify students of the registration deadline date.

15. Professional Suitability (if applicable)

Ontario Tech University is a community that values and promotes respect, integrity, diversity and accountability among all members of the university. These values can only be achieved in an environment that supports and protects the safety and security of its members. The Ontario Tech University Policy on Student Conduct defines and guides standards of student behaviour at the university to uphold these values and ensure that behaviour contrary to these standards are dealt with in a manner that is fair, open and effective.

The Faculty of Business & IT has the following expectations related to professionalism for all its community members, including without limitation, students, Staff, and Faculty:

- **Respect, civility, and courtesy:** Community members are expected to treat each other with respect, civility, and courtesy both in and outside of the classroom. Rudeness, profanity, insults, harassment, and class disruptions are unacceptable.
- **Critique ideas, not the people who raise the ideas:** Discussions, debates, and the exchange of ideas are normal parts of life in an academic community. Community members are expected to engage in discussions, debates, and the exchange of ideas in respectful ways, even while vigorously advocating for one's perspective.
- **Talk *to* those with whom you have a complaint, not *about* them.** When community members have disputes, complaints, and/or concerns about another community member, they are expected to do their best to address the matter directly and informally with the other member, provided that it is safe to do so. (See Appendix A for more information about how students can raise concerns about academic matters.)
- **Special obligations:** Community members in positions of authority have special obligations to demonstrate respect, civility, and professionalism and to encourage the development of these values within the FBIT community.

The *Professional Suitability* policy can be found at Ontario Tech's Professional Suitability Policy and the related procedures are hosted at Ontario Tech's Professional Suitability Procedures.

16. Academic Integrity

Students and faculty at Ontario Tech University share an important responsibility to maintain the integrity of the teaching and learning relationship. This relationship is characterized by honesty, fairness and mutual respect for the aim and principles of the pursuit of education. Academic misconduct impedes the activities of the university community and is punishable by appropriate disciplinary action.

Students are expected to be familiar with and abide by Ontario Tech University's regulations on Academic Conduct which sets out the kinds of actions that constitute academic misconduct, including plagiarism, copying or allowing one's own work to copied, use of unauthorized aids in examinations and tests, submitting work prepared in collaboration with another student when such collaboration has not been authorized, among other academic offences. The regulations also describe the procedures for dealing with allegations, and the sanctions for any finding of academic misconduct, which can range from a resubmission of work to a failing grade to permanent expulsion from the university. A lack of familiarity with these regulations on academic conduct does not constitute a defense against its application. This information can be found at Ontario Tech's Academic Integrity Policy.

Extra support services are available to all Ontario Tech University students in academic development, study skills, counseling, and peer mentorship. More information on student support services can be found at Academic Support at Ontario Tech's Student Learning Centre.

17. Turnitin (if applicable)

Ontario Tech University and faculty members reserve the right to use electronic means to detect and help prevent plagiarism. Students agree that by taking this course all assignments are subject to submission for textual similarity review by Turnitin.com. Assignments submitted to Turnitin.com will be included as source documents in Turnitin.com's restricted access database solely for the purpose of detecting plagiarism in such documents. The instructor may require students to submit their assignments electronically to Turnitin.com or the instructor may submit questionable text on behalf of a student. The terms that apply to Ontario Tech University's use of the Turnitin.com service are described on the Turnitin.com website.

Students who do not wish to have their work submitted to Turnitin.com must provide with their assignment at the time of submission to the instructor a signed Turnitin.com Assignment Cover sheet: Signed Turnitin Coversheet to Withdraw Permission to Submit Work.

18. Online Test and Exam Proctoring (Virtual Proctoring)

Ontario Tech University will conduct virtual monitoring of examinations in accordance with Ontario privacy legislation and all approved policy instruments.

19. Final Examinations (if applicable)

Final examinations are held during the final examination period at the end of the semester and **when on campus access is allowed,** may take place in a different room and on a different day from the regularly scheduled class. Check the published Examination Schedule for a complete list of days and times.

Students are required to show their Student ID card (campus ID) when **in-person examinations are allowed.** Students are advised to obtain their Student ID Card well in advance of the examination period as they will not be able to write their examinations without it. More information on ID cards can be found at Information on Ontario Tech's Student ID Cards.

Students who are unable to write a final examination when scheduled due to religious publications may make arrangements to write a deferred examination. These students are required to submit a Request for Accommodation for Religious Obligations to the Faculty concerned as soon as possible and no later than three weeks prior to the first day of the final examination period.

Further information on final examinations can be found at Ontario Tech's Procedures for Final Examinations.

20. Freedom of Information and Protection of Privacy Act

The following is an important notice regarding the process for submitting course assignments, quizzes, and other evaluative material in your courses in the Faculty of Business and IT.

Ontario Tech University is governed by the Freedom of Information and Protection of Privacy Act ("FIPPA"). In addition to providing a mechanism for requesting records held by the university, this legislation also requires that the University not disclose the personal information of its students without their consent.

FIPPA's definition of "personal information" includes, among other things, documents that contain both your name and your Banner (student) ID. For example, this could include graded test papers or assignments. To ensure that your rights to privacy are protected, the Faculty of [Insert Faculty name] encourages you to use only your Banner ID on assignments or test papers being submitted for grading. This policy is intended to prevent the inadvertent disclosure of your information where graded papers are returned to groups of students at the same time. If you still wish to write both your name and your Banner ID on your tests and assignments, please be advised that Ontario Tech University will interpret this as an implied consent to the disclosure of your personal information in the normal course of returning graded materials to students.

If you have any questions or concerns relating to the new policy or the issue of implied consent addressed above, please contact accessandprivacy@ontariotechu.ca

Notice of Collection and Use of Personal Information
Throughout this course, personal information may be collected through the use of certain technologies under the authority of the *University of Ontario Institute of Technology Act, SO 2002, c. 8, Sch. O.* and will be collected, protected, used, disclosed and retained in compliance with Ontario's *Freedom of Information and Protection of Privacy Act R.S.O. 1990, c. F.31.*

This course will use the following technologies that may collect, use, disclose and retain personal information (including images) for the purposes described below:

- Respondus Monitor and Proctortrack to maintain academic integrity for examinations;
- Google Meet and Kaltura Virtual Classroom to facilitate remote instruction and interactive learning;
- Peer-shared applications, services or technologies that may be reviewed, assessed, or used as part of coursework.
- Other applications, services, or technologies that support or enhance online learning that include, but are not limited to, the following: Mentimeter (www.menti.com) for participation polling.

For more information relating to these technologies, we encourage you to visit: Educational Technologies used at Ontario Tech. Questions regarding personal information may be directed to: Ontario Tech University Access and Privacy Office, 2000 Simcoe Street North, Oshawa, ON L1G 0C5, email: accessandprivacy@ontariotechu.ca.

By remaining enrolled in this course, you acknowledge that you have read, understand, and agree to the terms and conditions under which the technology provider(s) may collect, use, disclose and retain your personal information. You agree to the university using the technologies and using your personal information for the purposes described in this course outline.

21. Human Rights and Respect

Ontario Tech University is committed to providing a campus environment in which all University Members are treated with dignity and to fostering a climate of understanding and mutual respect. The University will not tolerate, ignore or condone Discrimination or Harassment by or against anyone. Examples of Harassing behavior include, but are not limited to; bullying, taunting or mocking someone's race or creed, ridiculing an individual's disability, or targeting individuals with unwanted sexual or negative stereotypical comments about one's sex, gender, sexual orientation, gender identity and/or gender expression. Pursuant to Ontario Tech's Respectful Campus Policy, students are reminded of their role in ensuring a campus environment that is equitable and inclusive. Requirements to refrain from harassment and discrimination apply broadly to the classroom, including in lectures, labs and practicums, as well as through the use of sanctioned and unsanctioned technological tools that facilitate remote learning, e.g. class and other chat functions, video conferencing, electronic mail and texts, and social media content amongst or about University students, faculty and staff.

22. Freedom of Expression

Pursuant to Ontario Tech's Freedom of Expression Policy, all students are encouraged to express ideas and perspectives freely and respectfully in university space and in the online university environment, subject to certain limitations. Students are reminded that the limits on Freedom of Expression include speech or behaviour that: is illegal or interferes with the university's legal obligations; defames an individual or group; constitutes a threat, harassment or discrimination; is a breach of fiduciary, contractual, privacy or confidentiality obligations or commitments; and unduly disrupts and interferes with the functioning of the university. In the context of working online, different forms of communication are used. Where permitted, students using "chat" functions or other online forms of communication are encouraged to ensure that their communication complies with the Freedom of Expression Policy.

23. Copyright Notice

All teaching materials provided by the instructor throughout the course, including, but not limited to, in whole or in part, recorded lectures, slides, videos, diagrams, case studies, assignments, quizzes, and examinations are subject to the Copyright Act, R.S.C., 1985, c. C-42. Teaching materials are owned by the faculty member, instructor or other third party who creates such works. The copyright owner(s) reserves all intellectual property rights in and to the teaching materials, including the sole right to copy, reproduce, distribute, and modify the teaching materials. Consistent with the university's Intellectual Property Policy, teaching materials are intended only for the educational use of Ontario Tech University students registered in the course that is the subject of this course outline. Any distribution or publishing of this material (e.g. uploading material to a third-party website) is strictly prohibited under the law unless the student has obtained the copyright owner's prior written consent. Any violation of copyright law or the Intellectual Property Policy, if proven, may be subject to sanction as academic misconduct, and/or under the Student Conduct Policy.

24. Student Course Feedback Surveys

Student evaluation of teaching is a highly valued and helpful mechanism for monitoring the quality of Ontario Tech University's programs and instructional effectiveness. To that end, course evaluations are administered by an external company in an online, anonymous process during the last few weeks of classes. Students are encouraged to participate actively in this process and will be notified of the dates. Notifications about course evaluations will be sent via e-mail, and posted on Canvas, Weekly News, and signage around the campus.

University Response to COVID-19

The government response to the COVID-19 pandemic is continually evolving. As new information becomes available from federal and provincial public health authorities, the Province of Ontario and the Regional Municipality of Durham, Ontario Tech University will remain nimble and prepared to respond to government orders, directives, guidelines and changes in legislation to ensure the health and safety of all members of its campus community. In accordance with public health recommendations, the university may need to adjust the delivery of course instruction and the availability and delivery mode of campus services and co-curricular opportunities. Ontario Tech University appreciates the understanding and flexibility of our students, faculty and staff as we continue to navigate the pandemic and work together to demonstrate our strong commitment to academic, research and service excellence during these challenging and unprecedented times.

The Accessibility for Ontarians with Disabilities Act (AODA) standards have been considered in the development of this model course template and it adheres to the principles outlined in the University's Accessibility Policy.

Ontario Tech University acknowledges the lands and people of the Mississaugas of Scugog Island First Nation. We are thankful to be welcomed on these lands in friendship. The lands we are situated on are covered under the Williams Treaties and the traditional territory of the Mississaugas, a branch of the greater Anishinaabeg Nation, including Algonquin, Ojibway, Odawa and Pottawatomi. These lands remain home to a number of Indigenous nations and people.

We acknowledge this land out of respect for the Indigenous nations who have cared for Turtle Island, also called North America, from before the arrival of settler peoples until this day. Most importantly, we remember the history of these lands has been tainted by poor treatment and a lack of friendship with the First Nations who call them home.

This history is something we are all affected by as we are all treaty people in Canada. We all have a shared history to reflect on, and each of us is affected by this history in different ways. Our past defines our present, but if we move forward as friends and allies, then it does not have to define our future.

FACULTY OF BUSINESS AND IT
Financial Implications of Cyber Risk
2024-25

1. Course Details & Important Dates*

Term	Course Type	Day	Time	Location	CRN#
2024-25	Lecture				

Classes Start	Classes End	**Last day to drop course without academic consequence**	Final Exam Period

* Visit Ontario Tech's Important Dates and Deadlines for other dates.

2. Instructor Contact Information

Instructor Name	Office	Phone	Email
Dr. Julia Zhu	UB3036		Canvas Email
Office Hours: by appointment			

Laboratory/Teaching Assistant Name	Office	Phone	Email
Office Hours: by appointment			

3. Course Description

This course attempts to provide a comprehensive and integrated introduction to cyber risk. We use contemporary models in accounting, finance, and economics to analyze and understand financial costs and implications of cyber risk. The focus will be on various issues regarding the causes and determinants of data privacy breaches, and the adverse consequences of cyberattacks.

Prerequisite(s):

4. Learning Outcomes

On the successful completion of the course, students will be able to:

- Demonstrate financial costs and implications of cyber risk
- Identify causes and determinants of data privacy breaches
- Evaluate the adverse consequences resulting from cyberattacks
- Estimate economic importance and financial consequences of cyberattacks
- Improve communication, teamwork, analytical, academic writing skills

5. Course Design

The course will be presented in the format of lectures, discussions, case study, simulated research projects, presentations, and term papers. A good understanding of the research papers and contemporary academic concepts is necessary for successful completion of this course. Students are therefore urged to work conscientiously on all assigned problems, questions, and readings. The practical implications will be analyzed through case study.

Lectures focus on the material presented in the distributed academic papers and general discussion relating to the topic(s) outlined in the lecture schedule. Students are expected to read the assigned academic journal articles and readings before class, and be prepared for class discussion. *Your instructor may not necessarily cover all of the materials in the paper, but it is the responsibility of the student to understand the concepts presented in the paper and lectures. If you are unsure of any of the concepts, please take the initiative to ask the instructor during class.*

Students requiring assistance are encouraged to speak to their instructor during class or during office hours. Should you wish to meet with the instructor outside of office hours, please email first to make an appointment. Students should get into the habit of making and keeping business appointments. Should you fail to attend or cancel the appointment at least 24 hours in advance, you will lose the right to book another appointment.

Email is commonly used by students to communicate with their instructor. However, it does limit the effectiveness of the communications and may not be the best way for instructors to answer student questions, especially those requiring an explanation of concepts covered in this course or some personal concerns. Therefore, the instructor may request a telephone call or personal/online meeting. *Your instructor will inform you as to her expectations about emails.*

Any surfing of the Internet during lectures that is not directly related to the class discussion is distracting and strictly forbidden. Additionally, the use of any electronic devices (e.g., cellular phones, Blackberrys, iphones) for e-mailing, text-messaging, etc. is strictly prohibited. Please turn OFF your phone before the beginning of each lecture. The laptop is to be used in class for academic purposes only.

6. Outline of Topics in the Course

Tentative Course Schedule, 2024-2025

Lecture #	Date	Topics	Material Covered
Lecture 1		Overview	Course Outline
		Introduction	Freeze, 2019; Bank of Canada, 2019

Lecture 2		Cyber Risk in Accounting and Finance	Deloitte, 2016;
			Institute of Internal Auditors, 2018;
			Interpol, 2020

Lecture 3		Research methods in Finance	Amir et al., 2018; Richardson et al., 2019

Lecture 4		Data Breach Investigations Report and	AICPA, 2018;
			PSC, 2018;
			Verizon, 2019

		Case study	
Lecture 5		Accounting audits	Chichernea, Holder, Petkevich, and Robin, 2018
Lecture 6		Trade secrets	Ettredge, Guo, and Li, 2018
Family Day, no scheduled academic activities ***Study Break, no scheduled academic activities***			
Lecture 7		Board-level technology committees	Higgs, Pinkser, Smith, and Young, 2016

Lecture 8		Financial Costs of Cyber Risk	Deloitte Development LLC, 2018;
			Lloyd's, 2017;
			Rajgopal and Srinivasan, 2016

		Case study	
Lecture 9		Cyber risk disclosure	Amir et al., 2018; Hilary et al., 2016
Lecture 10		Financial reports and audit fees	Smith et al., 2019; Lawrence et al., 2018

Lecture 11		Mixed effects of cyberattacks on stock market	Gatzlaff and McCullough, 2010;
			Richardson et al., 2019;
			Spanos and Angelis, 2016

Lecture 12		Private-sector firms	Gordon et al., 2015; Gordon et al., 2018

***Important Notes:** Adjustment of scheduled lectures might be made in accordance with any unforeseen circumstances during the semester.*

7. Required Readings

1. AICPA (American Institute of Certified Public Accountants), 2018. Cybersecurity risk management reporting fact sheet. Available at: www.aicpa.org/content/dam/aicpa/interestareas/frc/assuranceadvisoryservices/downloadabledocuments/cybersecurity-fact- sheet.pdf

2. Amir, E., Levi, S. and Livne, T., 2018. Do firms underreport information on cyber-attacks? Evidence from capital markets. Review of Accounting Studies 23, 1177-1206.

3. BoC (Bank of Canada), 2019. Cyber security strategy: Reducing Risk Promoting Resilience. Available at: https://www.bankofcanada.ca/wp-content/uploads/2019/06/cyber-security-strategy-2019-2021.pdf

4. Chichernea, D., Holder, A., Petkevich, A., and Robin, A., 2018. Better audits, better cybersecurity? Available at http://www.fmaconferences.org/SanDiego/SanDiegoProgram.htm.

5. Deloitte, 2016. Beneath the surface of a cyberattack: A deeper look at business impacts. Oakland, CA: Deloitte Development LLC.

6. Deloitte Development LLC. 2018. Black market ecosystem: Estimating the cost of ownership. Available at: https://www2.deloitte.com/content/dam/Deloitte/us/Documents/risk/us-risk-black-marketecosystem.pdf.

7. Ettredge, M., Guo, F., and Li, Y., 2018. Trade secrets and cyber security breaches. Journal of Accounting and Public Policy 37, 564– 585.

8. Freeze, Di. 2019. Cybersecurity almanac: 100 facts, figures, predictions and statistics. Cisco/CybersecurityVentures 2019 Cybersecurity Almanac. Available at https://cybersecurityventures.com/cybersecurity-almanac-2019/

9. Gatzlaff, K.M., McCullough, K.A., 2010. The effect of data breaches on shareholder wealth. Risk Management and Insurance Review 13, 61-83.

10. Gordon, L.A., Loeb, M.P., Lucyshyn, W. and Zhou, L., 2015. Externalities and the magnitude of cybersecurity underinvestment by private sector firms: a modification of the Gordon-Loeb model. Journal of Information Security 6, 24-30.

11. Gordon, L.A., Loeb, M.P., Lucyshyn, W. and Zhou, L. 2018. Empirical evidence on the determinants of cybersecurity investments in private sector firms. Journal of Information Security 9,133-153.

12. Higgs, J., Pinkser, R., Smith, T., and Young, G. 2016. The relationship between board-level technology committees and reported security breaches. Journal of Information Systems 30, 79–98.

13. Hilary, G., Segal, B., Zhang, M.H., 2016. Cyber-risk disclosure: Who cares? Unpublished working paper, Georgetown University.

14. IIA (Institute of Internal Auditors), 2018. The future of cybersecurity in internal audit. A joint research report by the internal audit foundation and crowe Horwath. Available at: https://bookstore.theiia.org/the-future-of-cybersecurity-in-internal-audit

15. Interpol, COVID-19 Cybercrime Analysis Report - August 2020.

16. Lawrence, A., Minutti-Meza, M., Vyas, D., 2018. Is operational control risk informative of financial reporting deficiencies? Auditing 37, 139-165.

17. Lloyd's, 2017. Closing the gap. Insuring your business against evolving cyber threats, http://www.lloyds.com/lloyds/about-us/what-do-we-insure/what-lloyds-insures/cyber/cyber-riskinsight/closing-the-gap.

18. PSC (Public Safety of Canada), 2018. Canada's vision for security and prosperity in the digital age. Available at: https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ntnl-cbr-scrt-strtg/ntnl-cbr-scrt-strtg-en.pdf

19. Rajgopal, S., Srinivasan, S., 2016. Why the market Yawned when Yahoo was hacked. The Wall Street Journal. Available at: https://www.wsj.com/articles/why-the-market-yawned-when-yahoo-washacked-1475537076.

20. Richardson, V.J., Smith, R.E., and Warson, M.W., 2019. Much ado about nothing: the (lack of) economic impact of data privacy breaches. Journal of Information System, 33 (3): 227–265.

21. Smith, T., Higgs, J.L. and Pinsker, R., 2019. Do auditors price breach risk in their audit fees?" Journal of Information Systems 33, 177-204.

22. Spanos, G. and Angelis, L., 2016. The impact of information security events to the stock market: a systematic literature review. Computers and Security 58, 216-229.

23. Verizon, 2019. Data Breach Investigations Report. Available at https://enterprise.verizon.com/resources/executivebriefs/2019-dbir-executive-brief.pdf.

Additional readings may be assigned or recommended during the course.

8. Evaluation Method

Evaluations	Weights	Due dates
In class presentation	15%	
Paper summary	15%	
Simulated project 1	20%	
Simulated project 2	20%	
Term paper	30%	
	100%	

Final course grades may be adjusted to conform to program or Faculty grade distribution profiles. Further information on grading can be found under Academic Regulations at: Ontario Tech's Academic regulations

9. Assignments and Tests

Paper Summary, Simulated Projects, and Term Papers:

Paper summary, simulated projects, and term papers are **individual** assignments.

Late submissions for above assignments will be accepted with a 20% **per day** penalty. Late submissions (penalty or not) are NOT accepted 2 days after the due date.

Missed In-Term Course Work

A request for consideration for missed course work worth 20% or less of the final grade must be documented and reported to the instructor in writing within the deadlines specified in the Procedures for Consideration of Missed In-Term Course Work and Examinations. Course work includes, but is not limited to: quizzes, written assignments (problem set), participation, case studies, etc. If missed coursework totals more than 20% of the final grade, the request for consideration must be submitted to the Faculty of Business and IT Advising Office and to the course instructor in writing using the Academic Consideration Form, along with supporting documentation. The request must be submitted within the deadlines specified in the Procedures for Consideration of Missed In-Term Course Work and Examinations. If approved, the extended deadline of the missed course component will be granted. If a student misses coursework and does not follow the procedure above, they will receive a score of zero on the missed component.

All forms can also be found through MyOntarioTech or on the Ontario Tech University website.

For information on how missed/late assignments and medical excuses are managed, please refer to the university's revised ***Procedures for Consideration of Missed In-Term Course Work and Examinations***

10. Technology Requirements and Learning Management System Information

Ontario Tech uses *Canvas*™ as its learning management system (LMS). Access to the LMS is limited to students formally registered in courses. That access is for the duration of the semester **and for an additional 120 days once the semester is over**. Students are strongly encouraged to download any/all relevant course material during that access period. Any requests for access post this period must be made in writing to the instructor/faculty member responsible for the course.

To support online learning, the university recommends certain technology requirements for laptops, software and internet connectivity which are available at: Ontario Tech's Remote Learning Policies.

Students experiencing technical difficulties such that they are unable to meet the technology requirements may contact the IT Service Help Desk at: servicedesk@dc-uoit.ca
Students experiencing financial difficulties such that they are unable to meet the technology requirements may contact Student Awards and Financial Aid Office at: connect@ontariotehu.ca

By remaining enrolled in this course, you acknowledge that you have read, understand and agree to observe the Recommended Technology Requirements for accessing university online learning resources, including those minimum requirements that are specific to your faculty and program.

11. Sensitive/Offensive Subject Matter

The classroom (both physical and virtual) is intended to provide a safe, open space for the critical and civil exchange of ideas and opinions. Some articles, media and other course materials may contain sensitive content that is offensive and/or disturbing. For example, some articles or videos may contain graphical depictions of violence, profanity, human anatomy, sexual acts, matters pertaining to race, gender, or sexuality. The Course Instructor will try to identify such material and communicate warnings to students in advance of the distribution and use of such materials, affording students the choice to either emotionally prepare for, or not to view or interact with, the content.
Disclaimer: "The content you are about to view contains sensitive subject matter that may be considered offensive and/or disturbing to some viewers. By viewing and/or interacting with the content you acknowledge and agree that it is your decision to view and interact with the content and to take the risk that you will experience a negative emotional response or reaction to the nature of the content."

12. Student Support

Any student who faces challenges securing their food or housing and believes this may affect their performance in the course is urged to contact studentlife@ontariotechu.ca for support. Furthermore, please notify your professor if you are comfortable in doing so. This will enable them to provide any resources and help that they can.

13. Student Sexual Violence Support and Education

Ontario Tech is committed to the prevention of sexual violence in all its forms. For any student who has experienced Sexual Violence, Ontario Tech can help. We will make accommodations to cater to the diverse backgrounds, cultures, and identities of students when dealing with individual cases.

If you think you have been subjected to or witnessed sexual violence:

- Reach out to the gender-based case specialist in the Human Rights office, a specially trained individual authorized to receive confidential disclosures about incidents of sexual violence. The Human Rights Office will make support services, including counselling, access or referrals to medical services, safety planning and accommodations, available to Students affected by an Incident of Sexual Violence. Book a consultation with the Case Specialist for more information.

Learn more about your options at: Ontario Tech's Policy on Sexual Violence and Support Information.

14. Students with Disabilities

Ontario Tech University is committed to promoting an environment where everyone has an equal opportunity to contribute to their fullest potential. Students who require accommodation for a disability are advised to contact Student Accessibility Services (SAS) as soon as possible. Accommodation decisions will be made in accordance with the Ontario Human Rights Code. Accommodations will be consistent with and supportive of the essential requirements of courses and programs, and provided in a way that respects the dignity of students with disabilities and encourages integration and equality of opportunity. Reasonable academic accommodation may require instructors to exercise creativity and flexibility in responding to the needs of students with disabilities while maintaining integrity.

Disability-related and accommodation support is available for students with mental health, physical, mobility, sensory, medical, cognitive, or learning challenges. Office hours are 8:30am-4:30pm, Monday, Tuesday, Thursday, and Friday, Wednesday's 10:00 am to 4:30. Please note they are closed each day between noon and 1:00 pm. For more information on services provided, you can visit the SAS website at Ontario Tech's Student Accessibility Services (SAS). Students may contact Student Accessibility Services by calling 905-721-3266, or email studentaccessibility@ontariotechu.ca.

Students who require the use of the Test Centre to write tests, midterms, or quizzes MUST register online using the SAS test/exam sign-up module, found here Registration Link to write examinations in SAS at Ontario Tech. Students must sign up for tests, midterms, or quizzes **AT LEAST seven (7) working days before the date of the test.**

Students must register for final exams no later **than 3 weeks prior to the start of the final examination period**. The final examination period is given at Ontario Tech University's Important dates and deadlines.

15. Professional Suitability (if applicable)

Ontario Tech University is a community that values and promotes respect, integrity, diversity and accountability among all members of the university. These values can only be achieved in an environment that supports and protects the safety and security of its members. The Ontario Tech University Policy on Student Conduct defines and guides standards of student behaviour at the university to uphold these values and ensure that behaviour contrary to these standards are dealt with in a manner that is fair, open and effective.

The Faculty of Business & IT has the following expectations related to professionalism for all its community members, including without limitation, students, Staff, and Faculty:

- **Respect, civility, and courtesy:** Community members are expected to treat each other with respect, civility, and courtesy both in and outside of the classroom. Rudeness, profanity, insults, harassment, and class disruptions are unacceptable.
- **Critique ideas, not the people who raise the ideas:** Discussions, debates, and the exchange of ideas are normal parts of life in an academic community. Community members are expected to engage in discussions, debates, and the exchange of ideas in respectful ways, even while vigorously advocating for one's perspective.
- **Talk *to* those with whom you have a complaint, not *about* them.** When community members have disputes, complaints, and/or concerns about another community member, they are expected to do their best to address the matter directly and informally with the other member, provided that it is safe to do so.
- **Special obligations:** Community members in positions of authority have special obligations to demonstrate respect, civility, and professionalism and to encourage the development of these values within the FBIT community.

The *Professional Suitability* policy can be found at Ontario Tech's Professional Suitability Policy and the related procedures are hosted at Ontario Tech's Professional Suitability Procedures.

16. Academic Integrity

Students and faculty at Ontario Tech University share an important responsibility to maintain the integrity of the teaching and learning relationship. This relationship is characterized by honesty, fairness and mutual respect for the aim and principles of the pursuit of education. Academic misconduct impedes the activities of the university community and is punishable by appropriate disciplinary action.

Students are expected to be familiar with and abide by Ontario Tech University's regulations on Academic Conduct which sets out the kinds of actions that constitute academic misconduct, including plagiarism, copying or allowing one's own work to copied, use of unauthorized aids in examinations and tests, submitting work prepared in collaboration with another student when such collaboration has not been authorized, among other academic offences. The regulations also describe the procedures for dealing with allegations, and the sanctions for any finding of academic misconduct, which can range from a resubmission of work to a failing grade to permanent expulsion from the university. A lack of familiarity with these regulations on academic conduct does not constitute a defense against its application. Please note that generative artificial intelligence (GAI) tools should not be utilized without advance, specific written approval by the faculty member teaching the course.

More information can be found at Ontario Tech's Academic Integrity Policy.

Extra support services are available to all Ontario Tech University students in academic development, study skills, counseling, and peer mentorship. More information on student support services can be found at Academic Support at Ontario Tech.

17. Turnitin (if applicable)

Ontario Tech University and faculty members reserve the right to use electronic means to detect and help prevent plagiarism. Students agree that by taking this course all assignments are subject to submission for textual similarity review by Turnitin.com. Assignments submitted to Turnitin.com will be included as source documents in Turnitin.com's restricted access database solely for the purpose of detecting plagiarism in such documents. The instructor may require students to submit their assignments electronically to Turnitin.com or the instructor may submit questionable text on behalf of a student. The terms that apply to Ontario Tech University's use of the Turnitin.com service are described on the Turnitin.com website.

Students who do not wish to have their work submitted to Turnitin.com must provide with their assignment at the time of submission to the instructor a signed Turnitin.com Assignment Cover sheet: Signed Turnitin Coversheet to Withdraw Permission to Submit Work.

18. Online Test and Exam Proctoring (Virtual Proctoring)

Ontario Tech University will conduct virtual monitoring of examinations in accordance with Ontario privacy legislation and all approved policy instruments.

19. Final Examinations (if applicable)

Final examinations are held during the final examination period at the end of the semester and may take place in a different room and on a different day from the regularly scheduled class. Check the published Examination Schedule for a complete list of days and times.

Students are required to show their valid physical or digital Ontario Tech University student photo ID card (campus ID), or a valid government issued photo ID that is in English when writing an **in-person examination.** Students are advised to obtain their Student ID Card well in advance of the examination period as they will not be able to write their examinations without it. More information on ID cards can be found at Information on Ontario Tech's Student ID Cards.

Students who are unable to write a final examination when scheduled due to religious publications may make arrangements to write a deferred examination. These students are required to submit an Academic Consideration form to the applicable Faculty as soon as possible and no later than three weeks prior to the first day of the final examination period.

Further information on final examinations can be found in the university's *Procedures for Final Examination Administration* Ontario Tech's Procedures for Final Examinations and in the Procedures for Consideration of Missed In-Term Course Work and Examinations.

20. Freedom of Information and Protection of Privacy Act

The following is an important notice regarding the process for submitting course assignments, quizzes, and other evaluative material in your courses in the Faculty of Business and IT.

Ontario Tech University is governed by the Freedom of Information and Protection of Privacy Act ("FIPPA"). In addition to providing a mechanism for requesting records held by the university, this legislation also requires that the University not disclose the personal information of its students without their consent.

FIPPA's definition of "personal information" includes, among other things, documents that contain both your name and your Banner (student) ID. For example, this could include graded test papers or assignments. To ensure that your rights to privacy are protected, the Faculty of Business and IT encourages you to use only your Banner ID on assignments or test papers being submitted for grading. This policy is intended to prevent the inadvertent disclosure of your information where graded papers are returned to groups of students at the same time. If you still wish to write both your name and your Banner ID on your tests and assignments, please be advised that Ontario Tech University will interpret this as an implied consent to the disclosure of your personal information in the normal course of returning graded materials to students.

If you have any questions or concerns relating to the new policy or the issue of implied consent addressed above, please contact accessandprivacy@ontariotechu.ca

Notice of Collection and Use of Personal Information
Throughout this course, personal information may be collected through the use of certain technologies under the authority of the *University of Ontario Institute of Technology Act, SO 2002, c. 8, Sch. O.* and will be collected, protected, used, disclosed and retained in compliance with Ontario's *Freedom of Information and Protection of Privacy Act R.S.O. 1990, c. F.31.*

This course will use the following technologies that may collect, use, disclose and retain personal information (including images) for the purposes described below:

- Respondus Monitor and Proctortrack to maintain academic integrity for examinations;
- Google Meet and Kaltura Virtual Classroom to facilitate remote instruction and interactive learning;
- Peer-shared applications, services or technologies that may be reviewed, assessed, or used as part of coursework.
- Other applications, services, or technologies that support or enhance online learning that include, but are not limited to, the following: Internet and Webcam.

For more information relating to these technologies, we encourage you to visit: Educational Technologies used at Ontario Tech.

Questions regarding personal information may be directed to: Ontario Tech University Access and Privacy Office, 2000 Simcoe Street North, Oshawa, ON L1G 0C5, email: accessandprivacy@ontariotechu.ca.

By remaining enrolled in this course, you acknowledge that you have read, understand, and agree to the terms and conditions under which the technology provider(s) may collect, use, disclose and retain your personal information. You agree to the university using the

technologies and using your personal information for the purposes described in this course outline.

21. Human Rights and Respect

Ontario Tech University is committed to providing a campus environment in which all University Members are treated with dignity and to fostering a climate of understanding and mutual respect. The University will not tolerate, ignore or condone Discrimination or Harassment by or against anyone. Examples of Harassing behavior include, but are not limited to; bullying, taunting or mocking someone's race or creed, ridiculing an individual's disability, or targeting individuals with unwanted sexual or negative stereotypical comments about one's sex, gender, sexual orientation, gender identity and/or gender expression. Pursuant to Ontario Tech's Respectful Campus Policy, students are reminded of their role in ensuring an equitable and inclusive learning environment. Requirements to refrain from harassment and discrimination apply broadly to on campus activities, e.g., on University property, in the classroom, including in lectures, labs and practicums, and also apply to off-campus activities, e.g. during any organized Ontario Tech class or extra-curricular activity including experiential learning opportunities such as co-op, practicum or during research endeavors, during official Ontario Tech events or using University equipment and technological tools that facilitate remote learning, e.g., class and other chat functions, video conferencing, and electronic mail.

22. Freedom of Expression

Pursuant to Ontario Tech's Freedom of Expression Policy, all students are encouraged to express ideas and perspectives freely and respectfully in university space and in the online university environment, subject to certain limitations. Students are reminded that the limits on Freedom of Expression include speech or behaviour that: is illegal or interferes with the university's legal obligations; defames an individual or group; constitutes a threat, harassment or discrimination; is a breach of fiduciary, contractual, privacy or confidentiality obligations or commitments; and unduly disrupts and interferes with the functioning of the university. In the context of working online, different forms of communication are used. Where permitted, students using "chat" functions or other online forms of communication are encouraged to ensure that their communication complies with the Freedom of Expression Policy.

23. Copyright Notice

All Teaching Materials, as they are defined under Ontario Tech's Intellectual Property policy ("IP Policy"), provided by the instructor throughout the course, including, but not limited to, in whole or in part, course notes, teaching notes, custom books, tutorials, evaluation tools, presentations and examinations are subject to the Copyright Act, R.S.C., 1985, c. C-42 and the IP Policy. Subject to the IP Policy, Teaching Materials are owned by the faculty member, instructor or other third party who creates such works, with a license to the University. The copyright owner(s) reserves all intellectual property rights in and to the foregoing materials. Consistent with the IP Policy, Teaching Materials are intended to be used by Ontario Tech University students registered in the course that is the subject of this course outline for educational purposes only. Any distribution or publishing of this material (e.g., uploading material to a third-party website) by a student is strictly prohibited under the law unless the student has obtained the copyright owner's prior written consent. Any violation of copyright law or the IP Policy, if proven, may be subject to sanction as academic misconduct, and/or under the Student Conduct Policy.

24. Student Course Feedback Surveys

Student evaluation of teaching is a highly valued and helpful mechanism for monitoring the quality of Ontario Tech University's programs and instructional effectiveness. To that end, course evaluations are administered by an external company in an online, anonymous process during the last few weeks of classes. Students are encouraged to participate actively in this process and will be notified of the dates. Notifications about course evaluations will be sent via e-mail, and posted on Canvas, Weekly News, and signage around the campus.

25. AODA

The Accessibility for Ontarians with Disabilities Act (AODA) standards have been considered in the development of this model course template and it adheres to the principles outlined in the University's Accessibility Policy.

Course Outline

MITS 6810 - Adversarial Machine Learning

Course Description

This course introduces adversarial attacks and defenses against machine learning models. Covered topics include evasion attacks against learning-based schemes, causative attacks by perturbing training datasets, and an introduction to robust statistics. Additionally, the course provides an overview of attacks against learning-based schemes utilized in some of the cybersecurity applications, such as *Spam Detection* and *Intrusion Detection*. The course provides the latest overview of state-of-the-art Adverserial Machine Learning (AML) schemes, such as *Generative Adversarial Networks* (GAN) and *Adversarial Active Learning*.

Learning Outcomes

Upon successful completion of the course, students will be able to:

- Describe different categories of attacks against machine learning models.
- Outline different categories of defenses for the development of robust learning-based models.
- Identify vulnerabilities of adaptive learning-based schemes deployed in an adversarial environment.
- Explain the importance of robust statistics and the use of invariant features in developing robust learning-based schemes for different cybersecurity applications.

Course Design

Course content will be presented to students during assigned lecture periods. Lecture slides will shall be posted on Canvas; however, the lecture slides may not cover some hands-on content, discussions and Q/A discussed in the class. Therefore, students are expected to attend assigned lectures, participate in class discussions as well as take notes to gain the most out of this course.

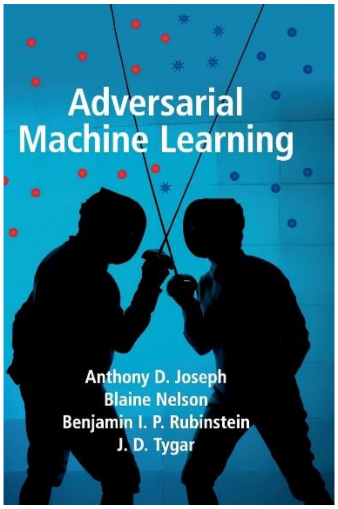
The two assignments and a final project constitute hands-on components and exercises related to the previously discussed topics during assigned lecture periods.

Outline of Topics in the Course

Week	Theme	Topics	Reading Assignments
1	A framework for Secure Learning	Overview of AML	Chapter 1
2		Characteristics of Adversarial Capabilities	Chapter 3
3		Exploratory vs. Causative Attacks	
4		Poisoning Hypersphere Learners	Chapter 4

5	Causative Attacks	Poisoning Retraining with Data Replacement	
6		Feature Space Attack: Red herring	*Selection of Research Papers*
7		Case Study – Causative Attack against Integrity and Availability	Chapter 5 and Chapter 6
8		Case Study – Active Learning and Malicious Labelers	*Selection of Research Papers*
9	Exploratory Attacks	Optimal Evasion Attacks	*Selection of Research Papers*
10		Evasion of Convex Inducing Classifiers	Chapter 8
11	Robust Learning	Robust Statistics for Learning	*Selection of Research Papers*
12		Generative Adversarial Networks	*Selection of Research Papers*
13		Randomized Classifiers (If time permits)	*Selection of Research Papers*

Required Texts/Readings



Textbook:

Title: Adversarial Machine Learning

Authors: Joseph, A., Rubinstein, B., Tygar, J.

ISBN-13: 9781107043466

Example of Papers:

- Brendel (2017) Decision-Based Adversarial Attacks: Reliable Attacks Against Black-Box Machine Learning Models
- Chen (2019) HopSkipJumpAttack: A Query-efficient Decision-based Adversarial Attack
- Guo (2019) Simple Black-box Adversarial Attacks
- Xiao (2018) Generating Adversarial Examples with Adversarial Networks
- Tramer (2018) Ensemble Adversarial Training: Attacks and Defenses
- Xu (2017) Feature Squeezing: Detecting Adversarial Examples in Deep Neural Networks
- Shafahi (2018) Poison Frogs! Targeted Clean-Label Poisoning Attacks on Neural Networks
- Zhang (2019) Theoretically Principled Trade-off between Robustness and Accuracy
- Belle (2020) Principles and Practice of Explainable Machine Learning
- Miller (2014) Adversarial Active Learning.

** Additional readings may be assigned or recommended during the course.*

Evaluation Method

Item	Weight (%)
Assignment 1 – (Coding & Report)	25%
Assignment 2 – (Coding & Report)	25%
Final Project – Outline	10%

Final Project – Report/Code	25%
Final Project – Presentation	15%

Assignments and Final Project

Assignments #1 and #2

For the two assignments (25% each), students will implement studied “causative” and “exploratory” attacks, and defenses methods utilizing different cybersecurity datasets. The students must implement the assignments using Python programming language and document their work (i.e. in report form) on Jupyter notebooks and must use common ML libraries, such as sci-kit learn and TensorFlow. The students may use free Jupyter notebooks provided by Google Colab (as their development environment) or choose to run a local Jupiter instance on their own machines.

Final Project

The students have the option to either: (a) select an AML research paper to implement or (b) define a learning-based application in cybersecurity that can be attacked/defended using the studied topics. Each student must prepare a project report explaining the selected problem statement, type of threats that selected learning-based scheme may face, demonstrate a successful attack, and present a viable defence. The report (25%) must be accompanied by a python implementation on the Juypyter notebook that can be shared with other students at the end of the term. Additionally, each student must prepare a presentation (15%) that shall be no more than 10 minutes long to discuss their project report with class.

Appendix D – Faculty Information

Please include here only those currently at the institution and affiliated with the program. Examples in purple to be removed. ***Where available, link each faculty name to their Research or Profile page on the website.***

Faculty members by home unit, rank, and supervisory privileges

Name and Faculty Status/Rank (Tenure/tenure-track, teaching-focused, continuing sessional, special appointment, emeritus, etc.)	Terminal Degree	Home Faculty/Unit	Areas of Expertise	Supervisory Privileges and Role in New Program (Note if faculty will be teaching and/or supervising in the program; indicate primary supervisor by asterisks)	Total Graduate Teaching (including New Program) (Note in bold type if faculty is a course developer for the program)
Patrick Hung, Professor	Ph.D.	FBIT	Privacy and Security	Teaching and Supervising	One course
Miguel Vargas Martin, Professor	Ph.D.	FBIT	Cryptography and Network Security	Teaching and Supervising	One course
Khalil El-Khatib, Professor	Ph.D.	FBIT	Privacy and Security	Teaching and Supervising	Two courses, Course developer
Salma Karray, Professor	Ph.D.	FBIT	Operational Research, Game Theory	Supervising	
Stephen Marsh, Professor	Ph.D.	FBIT	Information Trust and Privacy	Teaching and Supervising	Two courses Course developer
Julie Thorpe, Professor	Ph.D.	FBIT	Privacy and Security	Teaching and Supervising	One course Course developer
Andrea Slane, Professor	Ph.D., J.D.	FSSH	Legal and policy; privacy; intellectual Property	Teaching and Supervising	One course Course developer
Isabel Pedersen, Professor	Ph.D.	FSSH	Digital Life and Digital Media	Teaching and Supervising	One course Course developer
Shahram S. Heydari, Associate Professor	Ph.D.	FBIT	Communication networks and security	Teaching and Supervising	One course Course developer

Richard Pazzi, Associate Professor	Ph.D.	FBIT	Multimedia communication, Cloud networks	Supervising	
Amirali S. Abari, Associate Professor	Ph.D.	FBIT	Artificial Intelligence; IT Forensics	Teaching and Supervising	One course
Peter Lewis, Associate Professor	Ph.D.	FBIT	Trustworthy Artificial Intelligence	Teaching and Supervising	One course
Rajen Akalu, Associate Professor	Ph.D.	FBIT	Privacy and Artificial Intelligence; Information Privacy Law	Teaching and Supervising	One course
Fletcher Lu, Associate Professor	Ph.D.	FBIT	Cybercrime and online Fraud	Teaching and Supervising	One course
Hui Zhu, Associate Professor	Ph.D.	FBIT	Securities; Corporate Social responsibility; International Finance	Teaching and Supervising	One course, Course developer
Pooria Madani, Assistant Professor	Ph.D.	FBIT	Adversarial Machine Learning; Cybersecurity	Teaching and Supervising	One course Course developer
Li Yang, Assistant Professor	Ph.D.	FBIT	AI and data analytics; Cybersecurity	Teaching and Supervising	One course

Graduate Thesis supervisory records/experience by faculty member

Name	Completed (last 5 years)			Current		
	Master’s	Ph.D.	PDF	Master’s	Ph.D.	PDF
Miguel Vargas Martin	6	2		1	4	
Khalil El-Khatib	7	3			3	
Salma Karray		2		1	2	
Stephen Marsh	1	2		2		
Julie Thorpe	6	2		1	2	
Andrea Slane	5				1	
Isabel Pedersen	1	1				
Shahram S. Heydari	3	1	1	1	2	
Richard Pazzi	5	2				
Amirali S. Abari	7	1		3		
Peter Lewis		4	10	3	1	2
Pooria Madani				1		

Publication records at Ontario Tech by year and outlet (current and last 5 years)

Year	Faculty Members	Articles	Books	Book Chapters	Reports	Conference Presentations
2023	17	20	1			28
2022	16	22	1	1	1	20
2021	15	34	1	2	4	25
2020	14	13	1	4	4	15
2019	14	23		1	2	28
2018	14	17	1			28

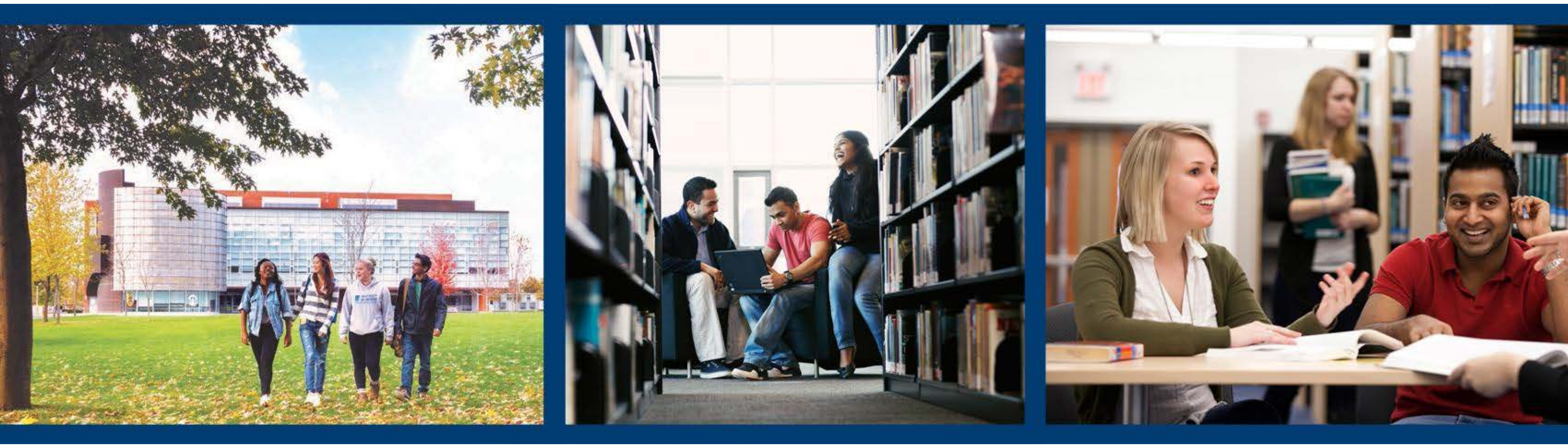
Research funding at Ontario Tech by source and year

Year	Faculty Members	Canadian Granting Councils	Canadian Government	International Government	Others
2023	17	$567000			$31000
2022	16	$611000	$95000		$24000
2021	15	$765000	$16000		$24000
2020	14	$483000	$16000		
2019	14	$406000	$5500		$80000
2018	14	$330000			$110000

Appendix E

Library Statement of Support for Proposed Doctor of Philosophy in Cybersecurity

Prepared by: Catie Sahadath, Associate University Librarian, Scholarly Resources, April 2024



OntarioTech
Library

Contents

Summary

Ontario Tech University Library's holdings in Business and Information Technology are strong.

The PhD in Cybersecurity program is a socio-technical, multidisciplinary research-intensive program that covers a broad range of themes related to cybersecurity; including technology, policy and governance, AI and human behaviour.

The Library's research holdings, as well as archives and special collections total more than 98, 000 print volumes and 167,892 journal subscriptions. In addition, our holdings include more than 1.3 million e-books, and primary source materials. Collection strengths support the research and instructional programs at Ontario Tech University.

Opportunities exist to incorporate information literacy directly into the PhD, Cybersecurity program. Student feedback from information literacy sessions overwhelmingly shows that students find the skills to be useful and that information literacy instruction should ideally be incorporated into foundational and methods courses. The following courses have been identified as ideal candidates for incorporating elements of library-delivered information, digital and data literacy instruction:

- INFR5010G: Fundamentals of IT Security
- CSCI 5010G: Survey of Computer Science Research Topics and Methods

Resource Requirements

Include a summary of any resource requirements to support the program, indicating one time startup or ongoing funding requests:

Resource	Rationale	Budget Requirement	OTO or Ongoing
Data Breach Chronology Database	This resource was identified by a faculty member as an important resource for the newly proposed course "Financial Implications of Cyber Risk."	$1 000	Ongoing
Total		$1000	

Introduction

The Library supports the teaching, learning and research missions of Ontario Tech University and Durham College. Ontario Tech students have access to a joint collection of more than 98, 000 print books. Additionally, our collections include extensive online resources such as e-books and online databases that are selected to meet curricular needs. Students and faculty are supported by a team of subject specialist librarians and trained library technicians who provide an array of research and teaching support services including information literacy instruction, workshops, research help and reference service.

Library Collections

The Library's collections support the PhD, Cybersecurity program. The existing collections that support similar and related programs, such as the BA, Information Technology, the MA and PhD in Computer Science, and the MA in IT Security, create a strong foundation of resources pertinent to the PhD, Cybersecurity program.

The Library's collections budget for 2023-24 was just under $2 M . Approximately 95% of this budget is directed to online resources, while the remainder is allocated to acquisition of other formats, including journals, print books, multimedia and other specialized material.

With respect to programs in the Faculty of Business and Information Technology, including the PhD, Cybersecurity program, our existing collection spans technology, policy, information, governance, IT security, AI, and human behaviour. Further, the collection covers topics of interdisciplinary relevance such as criminology and justice studies, social sciences, and business.

Suggestions for new resources are welcome and faculty and students are encouraged to contact their subject specialist. All recommended purchases are evaluated according to the Collection Development Policy and with consideration to budget constraints.

Consortial Licensing

Thanks to our participation in two consortia – the Ontario Council of University Libraries (OCUL) and the Canada Research Knowledge Network (CRKN) – Ontario Tech benefits from optimal pricing through licensing content as a collective, providing access to research published both open access and commercially through publishers such as Elsevier, Wiley, ACS, Taylor and Francis etc.

Journals

Our journal holdings in disciplines related to Cybersecurity is strong, including coverage related to engineering, computer science, criminology, critical policy studies, and artificial intelligence.

We provide access, through subscription, to most of the relevant journals with the highest impact factors, according to Clarivate's Journal Citation Reports (JCR) database and Google Scholar metrics.

By subject category:

JCR Subject Category	Ontario Tech Access	Select Titles
Computer Science, Interdisciplinary Applications	10/10	● Journal of Cybersecurity ● Cybersecurity ● Computers & Education
Criminology and Penology	10/10	● Annual Review of Criminology ● Criminology & Public Policy
Political Science	10/10	● Policy Review ● Social Science Quarterly
Law	10/10	● Internet Policy Review

Books & E-Books

As noted, we provide access to over 98,000 print books and over 1.3 million e-books that support teaching, learning and research across all programs and disciplines. Students and faculty have access to collections of books and e-books from major academic publishers.

Through our Omni Search, students and faculty have seamless access to holdings not just from Ontario Tech, but all Omni member libraries across Ontario universities. Articles and books that are not available through Omni Libraries can be requested through our interlibrary loan service.

The following table highlights Library holdings by subject heading for print books and e-books that encompass the Library's collections in Cybersecurity

Subject	# Print Books	# E-Books
Cybersecurity	186	3,332
Forensic Computing	74	5
Information Policy	32	5,293
Criminology	270	3,591

Search Tools

The Library subscribes to many research databases and indexes that provide access to the literature in Cybersecurity. Systematic searching of these resources enables students and faculty to access journals and other academic resources such as conference proceedings, theses and dissertations, trade publications and reports.

Highly Relevant Databases: Computer Science	Relevant Databases: Multidisciplinary	Relevant Databases: Related Disciplines
● IEEE Xplore Digital Library ● ACM Digital Library ● Computers and Applied Science Complete ● McGraw Hill Access Engineering	● Web of Science ● Scopus ● SpringerLINK Journals ● CBCA: Science and Technology	Forensic Science ● FORENSICnetBASE Criminology and Law ● Martin's Online Criminal Code ● National Criminal Justice Reference Service ● Proquest Criminal Justice

Standards and Codes

The Library provides access to Standards and Codes in print and online from the following sources:

- Canadian Standards Association (CSA)
- International Standards Organization (ISO)
- ASME
- ASTM
- IEEE
- Techstreet

Standards relating to Cybersecurity are available to faculty and students, as provisioned in the Library's Collection Development policy, for use in teaching, learning, and research. Faculty and students are encouraged to contact their subject specialist Librarian with suggestions for purchase.

Data Resources

To support research that requires statistics and datasets, the Library subscribes to three main resources:

- **Data Liberation Initiative (DLI):** Access to datasets from Statistics Canada surveys including public use microdata files (PUMF).
- **odesi**: A web-based data exploration, extraction and analysis tool that enables researchers to search for variables across thousands of datasets including Statistics Canada datasets and polling data.
- **Interuniversity Consortium for Political and Social Research (ICPSR):** Access to a data archive of more than 250,000 files of research in the social and behavioral sciences. Includes specialized collections of data in education, aging, criminal justice, substance abuse, terrorism, and other fields. Resources for teaching and learning include classroom exercises and materials to support

data literacy in the classroom.

In addition, we provide access to Borealis: The Canadian Dataverse Repository, which supports research data management and open access data requirements for Tri-Agency research funding compliance.

Multimedia Resources

The Library acquires DVD and streaming video resources that are relevant to the disciplines in the Cybersecurity program. Multimedia resources are selected individually or as part of standing subscriptions.

Omni retrieves over 350 results for videos available through the Library's streaming video subscriptions on the topic of cybersecurity.

Library Services

A range of library services support teaching, learning and research at the University. Students and faculty in the PhD, Cybersecurity program have access to services in-person, online and via email or telephone.

Research Support

The Library plays a vital role in supporting student and faculty research at Ontario Tech.

Reference Service & Research Consultations

Students and faculty have access to research support in-person and online, via telephone, email and through online chat help.

Librarians provide individualized research consultations with students and faculty, in person or online. These consultations are tailored to meet the needs of individual researchers and can cover a range of topics from basic introductions to more advanced search techniques and support for literature reviews.

Open Access & Research Data Management

We provide support to faculty and students in complying with the Tri-Agency Open Access Policy (SSHRC, NSERC, CIHR). Faculty and students can make their work open by publishing in an open access or hybrid journal, by depositing their work in a subject repository, or by depositing their work in Ontario Tech's institutional repository, eScholar (https://ir.library.ontariotechu.ca).

We also provide direct support to Faculties through dedicated subject specialist/liaison librarians and online guidance with the Library's Open Access Guide (http://guides.library.ontariotechu.ca/openaccess). The Library has a Research Data Management guide (http://guides.library.ontariotechu.ca/rdm) to support faculty and students in creating data management plans and sharing research data.

Research Metrics & Impact

The Library supports various departments on campus by fielding requests for reports on author, article, journal and institutional metrics. Subscribed tools include: Web of Science, Scopus and Journal Citation Reports (JCR).

Our Research Metrics guide (http://guides.library.ontariotechu.ca/researchmetrics) provides background information and support for these tools.

Theses & Dissertations

To ensure that the Ontario Tech community has access to national and international thesis and dissertation databases, we provide access to PQDT (ProQuest Dissertations and Theses) and the Theses Canada Portal. The Library plays a key role in the dissemination and preservation of Ontario Tech theses, managing copies in the institutional open-access digital repository, E-Scholar, as well as maintaining print copies in the Library archives.

Teaching & Learning Support

As partners in teaching and learning at Ontario Tech, we provide a range of instructional and curriculum supports, both in person and online.

Information Literacy Instruction

In collaboration with teaching faculty, Librarians deliver customized information literacy instruction that support the development of students' 21st century skills to successfully search, evaluate and ethically use scholarly resources in their course requirements. These library services are aligned with the Association of College and Research Libraries (ACRL) Framework for Information Literacy for Higher Education. Information literacy sessions are tailored to the specific requirements of the course or assignment. Information literacy may be delivered synchronously or asynchronously to classes, in person or online. Library information literacy modules are available in the Canvas Learning Management System and can be adapted and added direct into courses, or instructors can opt for asynchronous recordings.

Students may also receive Information Literacy instruction from a Librarian in their elective or communications courses.

Ideally, Information Literacy instruction is scaffolded across the required curriculum, enabling students to build increasingly sophisticated research skills throughout their program of study. Student feedback from information literacy sessions indicates that 78% of students felt more confident using the library after receiving library instruction, 84% if students felt that they learned something new, and that students often wish they would have received this training earlier in their program. Some comments include:

- "Definitely could have used this tutorial in prior classes for research"
- "I wish I had known about this stuff in first year"
- "I wish I had learned about this 3 years ago"
- "I wish this was mandatory for all first year students"
- "I think this course would be great for all first year students"

The following courses have been identified as potential Information Literacy touchpoints, due to the research skills outcomes built into the curriculum:

- INFR5010G: Fundamentals of IT Security
- CSCI 5010G: Survey of Computer Science Research Topics and Methods

Co-curricular Workshops

In addition to Information Literacy instruction that is integrated into the curriculum, the library offers a number of co-curricular workshops that help develop student and faculty skills. Some examples of workshops offered to Ontario Tech students in the past include:

- 3D Printing
- Managing Your Research Identity
- Citation Management
- Finding and Using Open Educational Resources
- Research Data management and Data Management Plans

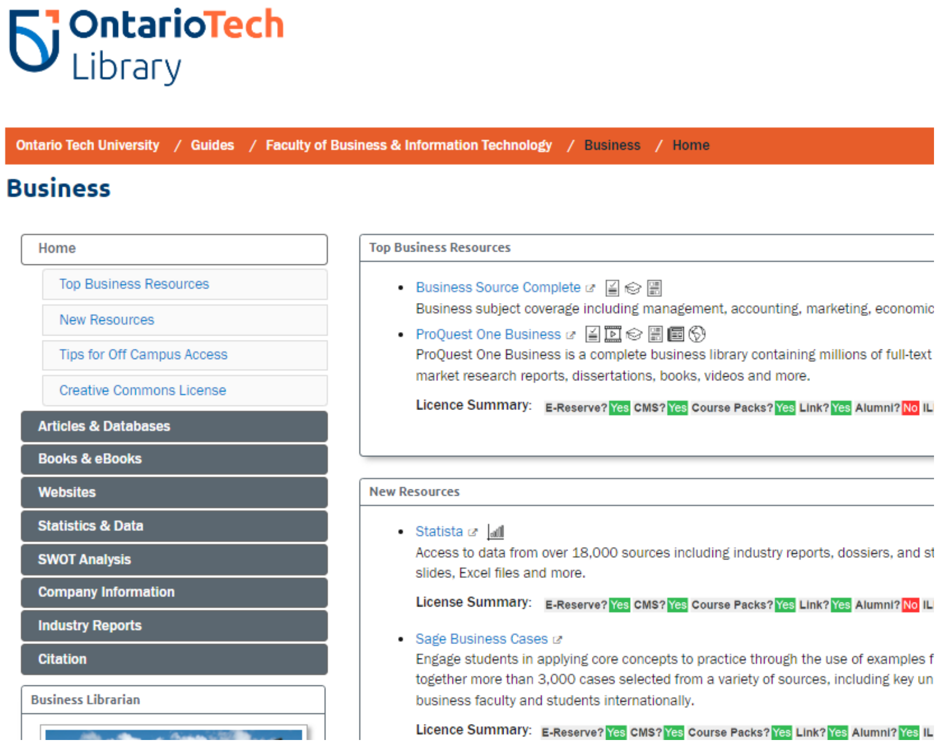
Workshop offerings are regularly updated in response to the changing needs of the community.

We also are regular contributors to the University's Grad Pro Skills offerings.

Online Research Guides

Subject specialist librarians create custom Research Guides for each subject area that are available from the Library website. Research Guides include program and course guides that are directly related to the program and course curriculum, as well as topic guides that have cross-disciplinary relevance. Research Guides of particular importance to students in the PhD, Cybersecurity program include:

- Business: https://guides.library.ontariotechu.ca/business
- Network & IT Security: https://guides.library.ontariotechu.ca/networkingITsecurity
- Citation Guide: https://guides.library.ontariotechu.ca/citation



OntarioTech Library

Ontario Tech University / Guides / Faculty of Business & Information Technology / Business / Home

Business

Home
- Top Business Resources
- New Resources
- Tips for Off Campus Access
- Creative Commons License

Articles & Databases

Books & eBooks

Websites

Statistics & Data

SWOT Analysis

Company Information

Industry Reports

Citation

Business Librarian

Top Business Resources

- Business Source Complete
  Business subject coverage including management, accounting, marketing, economic
- ProQuest One Business
  ProQuest One Business is a complete business library containing millions of full-text market research reports, dissertations, books, videos and more.

  Licence Summary: E-Reserve? Yes CMS? Yes Course Packs? Yes Link? Yes Alumni? No IL

New Resources

- Statista
  Access to data from over 18,000 sources including industry reports, dossiers, and st slides, Excel files and more.

  License Summary: E-Reserve? Yes CMS? Yes Course Packs? Yes Link? Yes Alumni? No IL
- Sage Business Cases
  Engage students in applying core concepts to practice through the use of examples f together more than 3,000 cases selected from a variety of sources, including key un business faculty and students internationally.

  Licence Summary: E-Reserve? Yes CMS? Yes Course Packs? Yes Link? Yes Alumni? Yes IL

Copyright & Academic Integrity

The Library provides copyright guidance for faculty and students. Library staff advise on license terms and the integration of content into the Learning Management System (LMS). We also help faculty find, evaluate and integrate Open Educational Resources into their courses.

Our research support services including our citation guides help students avoid plagiarism and comply with the University's Academic Conduct policy.

Course Reserves

Instructors can place materials on course reserve in the library, or make course materials available online through our electronic course reserves system. Online course reserves can include the library's print holdings, as well as digitized chapters, and links to journals, e-book chapters, videos and more. We are dedicated to providing equitable access to resources, and our online reserves are subject to copyright compliance and licensing restrictions.

3D Printing & Equipment Loans

Students have access to 3D printers and 3D printing workshops and can borrow equipment such as laptops and device chargers.

Library Staffing

The anticipated enrollment for students in the PhD, Cybersecurity program for years 1-5 is as follows:

2024-2025:	4
2025-2026:	9
2026-2027:	14
2027-2028:	19
2028-2029:	20

We anticipate that there will be additional staffing requirements associated with growth in graduate and undergraduate degree programs across the University. These requests will be part of the regular budget planning process, following a fulsome and strategic analysis of our staffing needs.

Conclusion

Supports for Graduate Students

Graduate students are encouraged to take advantage of all of the Library supports that are available to them. Their subject specialist librarian can help them identify the best databases for their research questions, as well as to define effective search strategies to make the best use of their time in locating articles, books, datasets etc. We can also assist in understanding the current publishing landscape, open access, open educational resources as well as managing research profiles, depositing research into eScholar, our institutional repository and determining research impact.

To conclude, the Library is very well-positioned to support the Faculty of Business and IT's proposed PhD in Cybersecurity and we look forward to a positive outcome and future launch of the program.

REVIEWERS' REPORT FOR NEW PROGRAMS

Reviewers' Report on the Proposed PhD-Cybersecurity Program at Ontario Tech University

Ali Dehghantanha
School of Computer Science
University of Guelph
ON, Canada

Isaac Woungang
Department of Computer Science
Toronto Metropolitan University
ON, Canada

1. OUTLINE OF THE REVIEW

Please indicate whether this review was conducted by desk audit or site visit. For those reviews that included a site visit, please indicate the following:

- Who was interviewed
- What facilities were seen
- Any other activities relevant to the appraisal

The program review was initially intended to be hosted in-person, but due to unforeseen circumstance, it was rescheduled to happen virtually in the form of desk audit and adjusted to avoid any substantial delay.

This report is based on the findings from the desk audit and an intensive review of the following documents that were made accessible to the review team (Professor Dehghantanha and Professor Woungang) via a Google drive folder:

- New Program Proposal
- Template for External Reviewers' Report
- Ontario Tech University's Institutional Quality Assurance Process Policy (IQAP)
- Information about Ontario Tech University
- Faculty and full curriculum information
- Strategic Research Plan
- Integrated Academic-Research Plan Summary
- Graduate Viewbook

During the desk audit online, we met with the following people:

- Deputy Provost
- Associate Dean, Graduate and Postdoctoral Studies
- Dean, Faculty of Business and IT
- Associate Dean, Academic Strategy
- Chair of Internal Assessment Team
- Graduate Program Assistant
- Director of Ontario Tech's Institute for Cyber Security and Resilient Systems
- Program and Curriculum Analyst-Centre for Institutional Quality Enhancement
- Manager, Graduate and Postdoctoral Studies
- Graduate Academic Affairs Specialist
- Graduate Admissions and Registration Coordinator
- Graduate Program Assistant
- Faculty Program Assistant
- Executive Assistant
- Faculty members & Staff
- A sampling of students
- Representatives from Student Life & School of Graduate and Postdoctoral Studies (SGPS)
- Faculty of Business and Information Technology Networking and IT Security Laboratory Managers

We also had Labs Virtual Tour, https://ontariotechu.ca/virtualtour/ of the following:

- *Networking lab (for teaching)* - which has leading-edge equipment (such as routers, switches, IP phones, wireless access points, and more, including remotely accessible ones) to teach concepts from fundamental networking skills to enterprise-level network engineering.
- *Biometric Access Control Lab* - for students to gain an understanding of biometric security concepts.
- *Hackers Research Lab* - for students to gain hands-on training in IT security
- *Security Operation Centre (SOC) Lab* - with appraise infrastructure and relevant applications.
- *Faculty of Business and Information* Technology *(FBIT) Cybersecurity and Resilience Testing Infrastructure (CRTI)* - currently under construction thanks to the recently obtained CFI/JELF grants. This will host the relevant equipment such as Spirent CyberFlood Security and Performance Testing Platform, ufiSpace programmable P4 switches, to support the envisaged research projects.
- *FBIT Research Labs/Groups* - which make use of the Cybersecurity-Related Research Facilities of the Institute for Cybersecurity and Resilient Systems (ICRS). These labs are:
  - Advanced Networking and Security (ANTS) Lab
  - Human Machine Lab
  - Security, Artificial Intelligence and Networks (SAIN) Lab
  - Trustworthy AI Lab
  - Business Analytics and AI Group
  - Interactive Media and Virtual Reality Research Group

2. EVALUATION CRITERIA

NOTE: Reviewers are asked to provide feedback on each of the following Evaluation Criteria (Quality Assurance Framework 2021, Section 2.1.2).

2.1 Program Objectives

- Clarity of the program's objectives
- Appropriateness of degree nomenclature given the program's objectives
- Consistency of the program's objectives with the institution's mission and academic plans

The objectives of the proposed PhD in Cybersecurity program at Ontario Tech University are consistent with the institution's mission and academic plans. Here are the key points that illustrate this alignment:
Institution's Mission and Vision: Ontario Tech's mission includes advancing the application of knowledge to address societal needs, fostering innovation, and nurturing a technology-enriched learning environment. The proposed PhD program, being multidisciplinary and research-intensive, focuses on technology, policy, and human behavior within cybersecurity, aiming to develop specialized socio-technical academics. This aligns well with the university's goals of advancing scientific and technical knowledge and addressing complex societal issues through a "Tech with a Conscience" approach.

- *Strategic and Academic Plans*: The program supports Ontario Tech's strategic priorities, including partnership and intellectual resilience. The affiliation with the Institute for Cybersecurity and Resilient Systems (ICRS) facilitates connections with industry, government, and research institutes, promoting interdisciplinary research and collaboration. These elements align with the university's emphasis on partnership and innovation as stated in its strategic plans.
- *Integrated Academic and Research Plan*: The PhD program contributes to areas identified as strengths or growth within the university's strategic mandate, such as digital technologies and artificial intelligence. By building on the successful Master of IT Security program and expanding into cybersecurity, the program supports the university's focus on developing programs that meet market demands and enhance its research capacity in emerging, impactful areas.

Thus, the proposed PhD program in Cybersecurity is well-aligned with the Ontario Tech University's mission, stated strategic priorities, and academic plans, reflecting a commitment to excellence and innovation in education and research in the field of cybersecurity. It is also consistent with the Graduate Degree Level Expectations (GDLEs).

2.2 Program requirements

- Appropriateness of the program's structure and the requirements to meet its objectives and program-level learning outcomes
- Appropriateness of the program's structure, requirements and program-level learning outcomes in meeting the undergraduate or graduate Degree Level Expectations
- Appropriateness of the proposed mode(s) of delivery to facilitate students' successful completion of the program-level learning outcomes
- Ways in which the curriculum addresses the current state of the discipline or area of study

The structure of the proposed PhD in Cybersecurity program at Ontario Tech University and the requirements to meet program objectives and program-level learning outcomes are appropriately designed. Here's a detailed look at how the program structure and requirements align with and support the achievement of its objectives and learning outcomes:

- *Coursework:* The program includes a combination of prerequisite and specialized courses, ensuring a comprehensive understanding of both fundamental and advanced topics in cybersecurity. This includes courses on IT security, law and ethics, AI in cybersecurity, and more.
- *Research Components*: The PhD program emphasizes research with components like a seminar course, thesis proposal, candidacy exam, and a final dissertation. This structure supports deep research engagement and innovation, critical for a doctoral level program.
- *Interdisciplinary Approach:* The program's affiliation with the Institute for Cybersecurity and Resilient Systems (ICRS) promotes interdisciplinary research, enhancing the breadth and depth of students' academic and professional development.
- *Admission Requirements:* Admission criteria are stringent, requiring a thesis-based Master's degree and a strong academic record, ensuring that incoming students are well-prepared and capable of high-level research. The multidisciplinary nature of the program suggests that some students may come to the program with more or less Science, Technology, Engineering, and Mathematics (STEM) in their background, the program is designed to move these students to an equal footing in the same way as any other graduate programs in cybersecurity.
- *Learning Outcomes:* The program defines clear learning outcomes related to knowledge of cybersecurity threats, risk management practices, the application of AI in cybersecurity, and the social, economic, and business aspects of the field. These outcomes are assessed through exams, defense presentations, and the thesis, ensuring that students achieve a deep and practical understanding of the field.
- *Supporting Activities:* The program includes activities like seminars and workshops that are critical for developing communication skills and professional capabilities, further supporting the learning outcomes aimed at preparing students for academia, industry, and policy-making roles.

The structure and requirements are designed to ensure that graduates:

- Have a deep and broad understanding of cybersecurity, from technical aspects to policy implications.
- Are capable of conducting independent, impactful research.
- Can effectively communicate complex ideas and research findings to a variety of audiences, crucial for roles in academia, industry, and government.

In summary, the program's structure and the requirements are well-tailored to meet its stated objectives and learning outcomes, preparing students for high-level careers in cybersecurity and related fields. This alignment supports Ontario Tech University's mission to foster knowledge and innovation in areas of societal importance.

2.3 Program requirements for graduate programs only

- Clear rationale for program length that ensures that students can complete the program level learning outcomes and requirements within the proposed time
- Evidence that each graduate student in the program is required to take a minimum of two-thirds of the course requirements from among graduate-level courses
- For research-focused graduate programs, clear indication of the nature and suitability of the major research requirements for degree completion

Yes, the structure, requirements, and program-level learning outcomes of the proposed PhD in Cybersecurity at Ontario Tech University are designed to meet the institution's Graduate Degree Level Expectations (GDLEs). Here's how the program aligns with these expectations:

Alignment with Graduate Degree Level Expectations

- *Depth and Breadth of Knowledge*: The program offers specialized coursework and interdisciplinary research opportunities that provide comprehensive knowledge in cybersecurity. Courses like "Fundamentals of IT Security" and "AI in Cybersecurity" ensure depth and breadth of knowledge in the field.
- *Research and Scholarship*: A strong emphasis on research is evident in the structure of the program, which includes a research thesis, candidacy exam, and dissertation defense. These components aim to foster the ability to generate new knowledge and satisfy peer review, key aspects of the GDLEs.
- *Level of Application of Knowledge*: The program is designed to train students to apply their knowledge in practical settings, addressing complex cybersecurity issues. This application is supported through specialized courses and the research thesis, where students tackle real-world problems.
- *Professional Capacity and Autonomy*: The PhD program encourages intellectual independence and ethical behavior in research. Program requirements such as the development of a personal research statement and the need for a faculty supervisor support the development of professional skills and autonomy.
- *Communication Skills*: Students are expected to communicate their research findings effectively, a requirement that is directly assessed during the thesis and candidacy defenses. Additionally, the program includes seminars where students can refine their presentation and communication skills.
- *Awareness of Limits of Knowledge*: The curriculum and research components of the program are designed to cultivate an appreciation of the complexity and limits of knowledge within the cybersecurity domain. This is achieved through critical analysis tasks and discussions on the ethical, social, and legal implications of cybersecurity technologies and practices.

Supporting Activities and Outcomes

- *Interdisciplinary Learning*: The program's affiliation with the Institute for Cybersecurity and Resilient Systems promotes interdisciplinary collaboration, enhancing students' ability to integrate knowledge from various fields into their cybersecurity research.
- *Practical and Ethical Training*: Courses on law, ethics, and governance in IT security ensure that students are well-versed in the practical and ethical aspects of cybersecurity, aligning with professional capacity expectations.
- *Research Opportunities and Innovation*: Opportunities for innovative research are supported by the program's structure, which encourages collaboration with industry and government agencies, fostering real-world impact and innovation.

In conclusion, the PhD in Cybersecurity program at Ontario Tech University is well-structured to meet the Graduate Degree Level Expectations by ensuring that graduates are knowledgeable, capable researchers, effective communicators, and ethically aware professionals prepared to contribute significantly to the field of cybersecurity and beyond.

2.4 Assessment of teaching and learning

- Appropriateness of the methods for assessing student achievement of the program-level learning outcomes and degree level expectations

- Appropriateness of the plans to monitor and assess:
  i. The overall quality of the program
  ii. Whether the program is achieving in practice its proposed objectives
  iii. Whether its students are achieving the program-level learning outcomes
  iv. How the resulting information will be documented and subsequently used to inform continuous program improvement

The methods used to assess student achievement of the program-level learning outcomes and degree level expectations. These methods also aim to monitor and assess the overall quality of the program, its achievement of proposed objectives, and whether students are meeting the program-level learning outcomes. Here's how the program plans to achieve these assessments:

Assessment of Learning Outcomes:

- *Examinations and Coursework*: Courses within the program utilize exams, projects, and presentations to assess students' understanding and application of knowledge. These assessments directly relate to specific learning outcomes outlined in the course syllabi.
- *Thesis Proposal and Defense*: The research proposal and final thesis defense are critical components where students must demonstrate their depth of knowledge, research skills, and the ability to contribute original insights to the field of cybersecurity.
- *Candidacy Exam*: This serves as a formal assessment of students' preparedness to conduct doctoral-level research, testing their knowledge and research plans against program objectives and learning outcomes.

Monitoring Program Quality and Objectives:

- *Annual Reviews*: The program plans to conduct annual reviews involving faculty assessments, student feedback, and program outcome analyses. These reviews help evaluate the effectiveness of the teaching methods and curriculum structure.
- *External Reviews*: Regular external assessments by academic peers and industry stakeholders provide objective insights into the program's relevance and effectiveness in meeting current cybersecurity challenges.

Assessing Achievement of Program Objectives:

- *Alumni Surveys and Employment Data*: By tracking graduates' career progress and obtaining feedback on their professional achievements, the program can assess how effectively it prepares students for roles in academia, industry, or policy-making.
- *Research Output and Impact*: Evaluations of students' research contributions to peer-reviewed journals and conferences provide measurable outcomes that reflect the program's success in achieving its academic objectives.

Documentation and Use of Assessment Information:

- *Continuous Improvement Process*: Assessment results are documented systematically and reviewed by the program committee to identify areas for improvement. This ongoing process ensures that the curriculum remains current and aligned with industry and academic advancements.
- *Strategic Adjustments*: Findings from these assessments inform curriculum revisions, teaching methods, and student support services, enhancing the program's overall effectiveness and its alignment with Degree Level Expectations.

The proposed PhD in Cybersecurity program at Ontario Tech University utilizes a comprehensive and structured approach to assess and monitor student achievements and the program's overall quality. The use of varied and rigorous assessment tools, combined with a clear mechanism for using the resulting data to drive continuous improvement, ensures that the program remains effective in meeting its objectives and adapting to the evolving field of cybersecurity. These measures are aligned with the standards set by the Quality Assurance Framework, ensuring that the program not only meets academic and industry standards but also prepares graduates to effectively contribute to and lead in the cybersecurity domain.

2.5 Admission requirements

- Appropriateness of the program's admission requirements given the program's objectives and program-level learning outcomes
- Sufficient explanation of alternative requirements, if applicable, for admission into a graduate, second-entry or undergraduate program, e.g., minimum grade point average, additional languages or portfolios, and how the program recognizes prior work or learning experience

The admission requirements for the PhD in Cybersecurity program at Ontario Tech University are well-structured and appropriately aligned with the program's objectives and program-level learning outcomes. The requirements ensure that incoming students possess the necessary academic background and research potential to succeed in this multidisciplinary, research-intensive program.

- *Educational Background*: Applicants are expected to have completed a four-year undergraduate degree and a thesis-based Master's degree in a relevant field. This ensures that students have a strong foundational knowledge and research experience in fields pertinent to cybersecurity. The requirement of an overall academic standing of at least 3.5 on a 4.0/4.3 scale underscores the program's commitment to academic excellence and ensures that students are well-prepared for the rigors of doctoral-level study.
- *Letters of Reference*: A minimum of two letters of reference from individuals who have direct knowledge of the applicant's academic competence is required. This allows the admissions committee to assess the applicant's suitability for the program based on feedback from credible sources who can attest to their research abilities and academic performance.
- *English Proficiency*: Proof of English proficiency for applicants whose first language is not English ensures that all students can effectively communicate and engage with the program's content, facilitating a productive learning environment.
- *Prospective Supervisor*: Applicants must find a prospective faculty supervisor from the list of graduate faculty members and receive formal acceptance from the supervisor. This requirement ensures that students have a clear research direction and mentorship from the outset, which is crucial for success in a research-intensive program.
- *Personal Research Statement*: The requirement of a minimum 3000-word personal research statement allows applicants to articulate their research interests and proposed academic research plan. This helps in assessing the applicant's alignment with the program's research objectives and their preparedness for undertaking significant research projects.
- *Sufficient Explanation of Alternative Requirements*: Graduates of Ontario Tech University's Master of IT Security (MITS) program can apply to the PhD program if they have an overall academic standing of at least 3.5/4.3. This provides a clear and accessible pathway for students from a related master's program to advance to doctoral studies.
- *Waiver Requests for Prerequisites*: Students who demonstrate sufficient proficiency through prior graduate-level coursework or extensive related work experience can request a waiver for certain prerequisite courses. This flexibility recognizes prior learning and professional experience, ensuring that students are not required to repeat content they have already mastered.

The admission requirements for the PhD in Cybersecurity program are comprehensive and appropriately tailored to the program's objectives and learning outcomes. They ensure that students have the requisite academic preparation, research potential, and language proficiency to succeed in the program. The inclusion of alternative requirements and pathways, such as the MITS pathway and waiver requests, demonstrates a thoughtful and inclusive approach to recognizing diverse educational backgrounds and professional experiences. Overall, these admission criteria are well-designed to attract and admit highly qualified candidates who are well-prepared to contribute to the field of cybersecurity research.

2.6 Resources for all programs

Given the program's planned /anticipated class sizes and cohorts as well as its program-level learning outcomes:

- Participation of a sufficient number and quality of core faculty who are competent to teach and/or supervise in and achieve the goals of the program and foster the appropriate academic environment
- If applicable, discussion/explanation of the role and approximate percentage of adjunct and part-time faculty/limited term appointments used in the delivery of the program and the associated plans to ensure the sustainability of the program and quality of the student experience
- If required, provision of supervision of experiential learning opportunities
- Adequacy of the administrative unit's planned utilization of existing human, physical and financial resources, including implications for the impact on other existing programs at the university
- Evidence that there are adequate resources to sustain the quality of scholarship and research activities produced by students, including library support, information technology support, and laboratory access
- If necessary, additional institutional resource commitments to support the program in step with its ongoing implementation

The resources available to sustain the quality of scholarship and research activities for the proposed PhD in Cybersecurity at Ontario Tech University are adequately provided, covering aspects such as library support, information technology support, and laboratory access:

- *Library Support*: The Library Report details a robust collection of resources that support the cybersecurity field, including over 98,000 print volumes and 167,892 journal subscriptions. Additionally, there are more than 1.3 million e-books and substantial electronic resources accessed through consortia licensing with major academic publishers. This provides a strong foundation for research and scholarship needs of PhD students.
- *Information Technology Support*: The university has committed resources to ensure that IT support is sufficiently robust to handle the specialized needs of cybersecurity research. This includes access to high-performance computing resources and secure data storage solutions, which are essential for handling the large datasets and complex simulations often required in cybersecurity research.
- *Laboratory Access*: The program proposal outlines access to specialized laboratories and research facilities that are part of the Institute for Cybersecurity and Resilient Systems. These facilities are designed to support advanced research in cybersecurity, including practical experiments and simulations, providing a crucial resource for doctoral research activities.

These resources collectively ensure that students have access to the necessary tools and environments to conduct high-level research, fostering innovation and maintaining a high standard of academic rigor within the program.

2.7 Resources for graduate programs only

Given the program's planned /anticipated class sizes and cohorts as well as its program-level learning outcomes:

- Evidence that faculty have the recent research or professional/clinical expertise needed to sustain the program, promote innovation, and foster an appropriate intellectual climate
- Where appropriate to the program, evidence that financial assistance for students will be sufficient to ensure adequate quality and numbers of students
- Evidence of how supervisory loads will be distributed, in light of qualifications and appointment status of the faculty

The faculty associated with the proposed PhD in Cybersecurity program at Ontario Tech University have the requisite recent research expertise and professional credentials to sustain the program, foster innovation, and maintain an appropriate intellectual climate. The Faculty CVs highlight diverse research activities and professional experience in areas critical to cybersecurity, including but not limited to, network security, AI, information trust, ethical hacking, and data privacy. Moreover, many faculty members have active research projects and collaborations that not only align with the program's focus but also ensure ongoing contributions to cutting-edge developments in the field. This active engagement in current research ensures that the program remains at the forefront of technological and academic advancements, which is essential for promoting innovation and fostering an intellectual climate conducive to advanced study and research in cybersecurity. The faculty's alignment with the program's multidisciplinary approach also supports a robust intellectual climate, where knowledge from different sub-fields of cybersecurity is integrated, offering students a comprehensive and nuanced understanding of the subject. This approach not only enriches the students' learning experience but also prepares them to tackle complex challenges in the cybersecurity landscape.

The financial assistance provided to students in the proposed PhD in Cybersecurity at Ontario Tech University appears sufficient to ensure the quality and numbers of students are maintained. The self-study document outlines various scholarships, awards, and funding opportunities that are available to graduate students. Specifically, students have access to scholarships like the Ontario Graduate Scholarship and Canada Graduate Scholarships, along with various internal awards provided by the university. Additionally, research assistantships funded by faculty grants can also provide financial support to students. The document also mentions the university's commitment to ensuring competitive funding packages to attract high-quality students. It acknowledges that the ability to offer competitive funding is crucial for attracting and retaining the best students, which directly impacts the program's quality and success.

The supervisory loads for the proposed PhD in Cybersecurity at Ontario Tech University are adequately distributed, considering the qualifications and appointment status of the faculty involved. The document details that faculty members from various departments and specializations will contribute to supervising students, ensuring a broad base of expertise and support. Furthermore, the faculty's qualifications, including their academic backgrounds, research accomplishments, and practical cybersecurity experience, align with the program's multidisciplinary approach. This diversity allows for a more enriching supervisory experience for students and ensures that supervisory duties are not concentrated among a few faculty members, thus preventing overloading. Additionally, the program plans to leverage industry partnerships and external collaborations, which could further distribute supervisory responsibilities and enhance the learning experience by integrating real-world perspectives and expertise into student supervision.

2.8 Quality and other indicators

- Evidence of quality of the faculty (*e.g.*, qualifications, funding, honours, awards, research, innovation and scholarly record; appropriateness of collective faculty expertise to contribute substantively to the program and commitment to student mentoring)
- Any other evidence that the program and faculty will ensure the intellectual quality of the student experience

NOTE: Reviewers are urged to avoid using references to individuals. Rather, they are asked to assess the ability of the faculty as a whole to deliver the program and to comment on the appropriateness of each of the areas of the program (fields) that the university has chosen to emphasize, in view of the expertise and scholarly productivity of the faculty.

The faculty involved in the proposed PhD program in Cybersecurity at Ontario Tech University appears well-equipped to deliver a comprehensive and research-intensive program based on their qualifications, research achievements, and commitment to mentoring students.

- *Qualifications and Expertise*: The faculty members hold advanced degrees in relevant fields, including computer science, cybersecurity, and information technology, among others. This educational background is essential for delivering the multidisciplinary aspects of the cybersecurity program which includes technology, policy and governance, artificial intelligence, and human behavior.

- *Research and Scholarly Record*: The faculty members are, as expected, diverse in their research interests and have a range of expertise from deep specialization through to tangential interests, but they are actively involved in cutting-edge research, contributing to areas critical to the program such as cyber-physical systems security, data privacy, and the applications of AI in cybersecurity. Their work is well-circulated in reputable academic journals, indicating a strong scholarly output which is critical for a PhD-level program. The faculty members are qualified to deliver various aspects of the proposed program and provide a solid foundation to initiate the program.
- *Funding, Honours, and Awards*: Many faculty members have secured significant research grants and awards from national and international bodies, enhancing the program's profile and providing ample research opportunities for students. Such funding is crucial for sustaining high-level research activities and for students to engage in funded projects.
- *Commitment to Student Mentoring*: The faculty have a demonstrated commitment to mentoring, with several members having received accolades for their teaching and student guidance. This mentorship is vital in a PhD program for fostering a supportive and productive learning environment.
- *Program Delivery and Teaching Methods*: The program uses a diverse set of delivery methods, including traditional lectures, seminars, and hybrid formats, which cater to different learning preferences and enhance student engagement. This variety helps in addressing complex cybersecurity topics comprehensively. The delivery modality is consistent with most modern graduate programs in cybersecurity.
- *Research Opportunities*: The program provides extensive research opportunities that are integrated into the curriculum through thesis work, specialized courses, and direct involvement with the Institute for Cybersecurity and Resilient Systems (ICRS). This exposure to active research projects under the guidance of experienced faculty ensures that students are at the cutting edge of cybersecurity developments.
- *Student Support and Resources*: The university ensures that cybersecurity PhD students have access to substantial academic resources, including a robust library system with specialized journals and databases in cybersecurity, and support for data management and open access publishing. These resources are critical for supporting high-level academic work and innovation in the field.
- *Mentorship and Professional Development*: The program emphasizes mentorship and the development of professional skills through seminars and personalized guidance from faculty. This approach not only enhances the academic rigor of student projects but also prepares them for future roles in academia, industry, or government.
- *Interdisciplinary Collaboration*: The program's structure encourages interdisciplinary collaboration, which is crucial for addressing the multifaceted challenges in cybersecurity. This interdisciplinary approach is supported by collaborations between faculties and departments, enriching the student learning experience by integrating diverse perspectives and expertise.
- The PhD program in Cybersecurity at Ontario Tech University has established strong criteria and support systems for student success, which are evident in several key areas.
- *Grade-Level for Admission*: Students applying to the program are expected to have a strong academic background, typically requiring a minimum GPA of 3.5 on a 4.0/4.3 scale in their last two years of a thesis-based master's degree in a relevant field. This high standard ensures that incoming students can engage deeply with the program's advanced content.
- *Scholarly Output and Awards*: The program is designed to enhance students' research capabilities, which is reflected in their scholarly output. While specific data on publications and conference presentations by current students were not detailed, the program's structure and faculty support are oriented towards producing high-quality research, which likely contributes to student success in these areas.

- *Success Rates in Scholarships and Competitions*: The students in the program are encouraged and supported in applying for provincial and national scholarships, with the structured mentorship and resources aimed at improving their competitiveness in these arenas.
- *Commitment to Professional and Transferable Skills*: The program incorporates professional development through seminars and workshops that focus on both the specific skills needed for cybersecurity and transferable skills such as communication, project management, and ethical considerations in technology. This commitment is critical for preparing students for diverse career paths in academia, industry, or government.
- *Times-to-Completion and Retention Rates*: The program aims for a completion time of around four to five years for full-time students, reflecting a structured and efficient pathway through coursework, research, and thesis completion. Retention rates are supported by comprehensive academic and personal support systems, although specific statistics on retention were not provided.

3. EQUITY, DIVERSITY, INCLUSION, AND DECOLONIZATION

Please comment on any consideration of the principles of equity, diversity, inclusion, and decolonization in the new program.

The proposed PhD program in Cybersecurity at Ontario Tech University demonstrates a commitment to the principles of equity, diversity, inclusion, and decolonization (EDID). These principles are integrated into various aspects of the program to ensure a supportive, inclusive, and equitable environment for all students. Here are some key points highlighting how these principles are considered in the new program:

- *Admissions Process*: The program has clear, transparent admission criteria that consider diverse academic backgrounds and professional experiences. By allowing waiver requests for certain prerequisite courses, the program recognizes prior learning and work experience, ensuring equitable access for students from various educational pathways.
- *Support for Underrepresented Groups*: The program encourages applications from underrepresented groups in the field of cybersecurity. This includes specific outreach efforts to attract a diverse applicant pool, ensuring that all students have equal opportunities to access the program.
- *Inclusive Curriculum*: The program covers a broad range of themes related to cybersecurity, including technology, business, policy, governance, AI, and human behavior. This multidisciplinary approach ensures that diverse perspectives are integrated into the curriculum, enriching the learning experience for all students.
- *Diverse Faculty*: The program is affiliated with the Institute for Cybersecurity and Resilient Systems (ICSR), which brings together a multidisciplinary team of researchers and faculty members. This diversity in expertise and background provides students with a wide range of perspectives and mentorship opportunities.
- *Support Services*: The program offers various support services to ensure an inclusive learning environment. This includes access to academic support, counseling services, and mentorship programs designed to help all students succeed, regardless of their background.
- *Library Resources*: The library provides extensive resources, including e-books, journals, and databases that cover diverse topics and perspectives in cybersecurity. Additionally, the library offers information literacy instruction tailored to the needs of students, ensuring they can effectively utilize these resources.
- *Curriculum Content*: The program includes a critical examination of the social and ethical implications of technology, which encompasses discussions on decolonization and the impact of cybersecurity on indigenous communities. This ensures that students are aware of and can critically engage with these important issues.
- *Research Opportunities*: Students are encouraged to undertake research that addresses the needs and concerns of marginalized and indigenous communities. This approach not only contributes to decolonization efforts but also broadens the scope and impact of cybersecurity research.

The PhD program in Cybersecurity at Ontario Tech University incorporates the principles of equity, diversity, inclusion, and decolonization in a comprehensive manner. From the admissions process to curriculum content and support services, the program is designed to provide an inclusive and equitable educational environment. These efforts ensure that students from diverse backgrounds can thrive and contribute to the field of cybersecurity, ultimately enriching the academic community and the society.

4. OTHER ISSUES

- Please highlight any unique curriculum or program innovation, creative components, or significant high-impact practices
- Please identify any other issues that may not be covered above

The PhD program in Cybersecurity at Ontario Tech University offers several unique and innovative elements that distinguish it from other programs in the field. These innovations and high-impact practices are designed to enhance the educational experience and ensure that graduates are well-prepared for both academic and industry roles in cybersecurity. One of the standout features of the PhD in Cybersecurity program is its multidisciplinary approach. The program integrates themes from technology, business, policy, governance, artificial intelligence, and human behavior. This broad perspective ensures that students gain a comprehensive understanding of cybersecurity, which is essential for addressing the complex and interconnected challenges in this field. By covering a wide range of topics, the program prepares students to tackle issues from various angles, fostering innovation and critical thinking.

Another innovative aspect of the program is its affiliation with the Institute for Cybersecurity and Resilient Systems (ICSR). This affiliation provides students with access to a multidisciplinary, global center for cybersecurity research, innovation, teaching, and outreach. The ICSR's resources and networks offer students unparalleled opportunities to engage in cutting-edge research and collaborate with leading experts in the field. This connection enhances the program's academic rigor and provides students with valuable industry connections and practical experience.

The program also includes a strong emphasis on real-world applications and high-impact practices. For example, the curriculum incorporates specialized courses that address current and emerging topics in cybersecurity, such as artificial intelligence in cybersecurity, usable security, information trust, and blockchain technologies. These courses ensure that students are not only learning the theoretical foundations but also gaining practical skills that are directly applicable to contemporary cybersecurity challenges. Moreover, the program's structure includes seminars, a thesis proposal, and a final thesis, which are designed to foster research skills and academic excellence. The requirement for students to present seminars and defend their thesis proposals and final dissertations in oral examinations ensures that they develop strong communication and presentation skills, which are crucial for both academic and professional success.

One of the key strengths of the PhD in Cybersecurity program is its flexibility in recognizing prior learning and professional experience. The program allows students to request waivers for certain prerequisite courses if they can demonstrate sufficient proficiency through prior graduate-level coursework or extensive related work experience. This flexibility is important for accommodating students from diverse educational and professional backgrounds, ensuring that the program is accessible to a wider range of applicants. The program's admission requirements, which include finding a prospective faculty supervisor and submitting a detailed personal research statement, ensure that students have a clear research direction and are well-prepared for the demands of the program. However, it is crucial to ensure that prospective students receive adequate guidance and support in identifying potential supervisors and developing their research proposals, as this can be a challenging process for applicants. Additionally, while the program's multidisciplinary approach and broad range of topics are strengths, it is important to ensure that the curriculum remains coherent and focused. Maintaining a balance between breadth and depth in the curriculum is essential to ensure that students gain a comprehensive yet detailed understanding of cybersecurity.

Overall, the PhD program in Cybersecurity at Ontario Tech University is well-designed, innovative, and aligned with current trends and challenges in the field. Its multidisciplinary approach, strong industry connections, and emphasis on practical skills and high-impact practices make it a standout program that is well-equipped to prepare students for successful careers in cybersecurity. By continuing to support students throughout the admission process and maintaining a balanced curriculum, the program can ensure that it remains at the forefront of cybersecurity education and research.

5. SUMMARY AND RECOMMENDATIONS

Please provide a summary of your conclusions and include a numbered list of each of your recommendations.

The proposed PhD program in cybersecurity at Ontario Tech University is designed to meet the growing global demand for advanced research and practical skills in the cybersecurity field. This program is expected to provide a robust curriculum that equips students with both theoretical and practical knowledge needed to address and mitigate modern cybersecurity challenges effectively. Key aspects of the program likely include a strong focus on interdisciplinary learning, which integrates insights from fields such as artificial intelligence, law, ethics, and business with core cybersecurity principles. This approach not only broadens the students' understanding, but also enhances their ability to innovate and solve complex problems across different sectors. Hands-on learning experiences are anticipated to be a cornerstone of the program, with students gaining practical skills through labs, simulations, and real-world projects. These activities are crucial for translating theoretical knowledge into practical, actionable skills in a real-world context. Collaboration with industry is expected to play a significant role in the program, providing students with exposure to the latest challenges and innovations in the field. These collaborations are also vital for networking, job placement, and practical insights into the cybersecurity industry. The program aims to continuously evolve by incorporating cutting-edge research, technology, and teaching methods. This ensures that graduates are not only well-prepared to enter the workforce but are also capable of leading the way in innovation and best practices in cybersecurity.
To further improve the program, in the long-term, following actions can be taken:

- *Funding for Research Chairs in the field*: Seek external funding to establish research chairs in cybersecurity including industry chairs, Canada Research Chairs, Canada Excellence Research Chairs to attract top-tier faculty and researchers.
- *Enhance Interdisciplinary Opportunities*: The program should further integrate interdisciplinary courses and projects that involve fields such as AI, law, and business ethics. This can be achieved by developing new courses or modifying existing ones to include interdisciplinary perspectives and problem-solving experiences.
- *Industry Collaboration and Partnerships*: Strengthen ties with the cybersecurity industry to facilitate ongoing student engagement through internships, guest lectures, and live project collaborations. This requires reaching out to potential industry partners and setting up agreements that benefit both the students and the companies involved.

Overall, the proposed PhD program at Ontario Tech University represents a significant step forward in cybersecurity education, aligning academic rigor with industry needs and future technological advancements. The program's success will rely on its ability to adapt, innovate, and maintain relevance in the rapidly changing landscape of global cybersecurity challenges.

NOTE: The responsibility for arriving at a recommendation on the final classification of the program belongs to the Appraisal Committee. Individual reviewers are asked to refrain from making recommendations in this respect.

Signature:

Date: July 3, 2024

Signature:

Date: July 3, 2024

Faculty Response to the External Review for the

____

Ph.D. in CyberSecurity

Submitted By:

Shahram Heydari

Date 13 August, 2024

Carolyn McGregor, FBIT Dean

13 August, 2024

Introduction

We thank the external reviewers Dr. Ali Dehghantanha (University of Guelph) and Dr. Isaac Woungang (Toronto Metropolitan University) for their positive and constructive comments. Dr. Dehghantanha and Dr. Woungang have prior experience in directing relevant graduate programs at their respective institutions. They conducted a thorough analysis of the program, identified our strengths, and concluded that the proposed program "is well-designed, innovative, and aligned with current trends and challenges in the field. Its multidisciplinary approach, strong industry connections, and emphasis on practical skills and high-impact practices make it a standout program that is well-equipped to prepare students for successful careers in cybersecurity. By continuing to support students throughout the admission process and maintaining a balanced curriculum, the program can ensure that it remains at the forefront of cybersecurity education and research."

They also note that the proposed program "represents a significant step forward in cybersecurity education, aligning academic rigor with industry needs and future technological advancements. The program's success will rely on its ability to adapt, innovate, and maintain relevance in the rapidly changing landscape of global cybersecurity challenges."

They have also kindly pointed out the areas to be considered for improvement and long term success of the program. We greatly appreciate their vote of confidence and recommendations and will address them to improve the program.

Summary of Recommendations and Faculty Responses

- *Restate the recommendations summarized in the external reviewers' report and provide the Program's comments and responses*
- *The Dean should then provide summative comments/responses from an overarching Faculty perspective for each recommendation and program response*

Recommendation 1
Funding for Research Chairs in the field: Seek external funding to establish research chairs in cybersecurity including industry chairs, Canada Research Chairs, Canada Excellence Research Chairs to attract top-tier faculty and researchers.

Program's Response
This is an excellent idea and will certainly bring expertise and recognition to the program. The proposal will be updated to recommend prioritizing research chair positions in the field of cybersecurity.

Dean's response
Within Ontario Tech University, allocation of Canada Research Chairs (CRC)s is managed centrally by the Office of Research Services and faculties have the option to bid for CRC. Cybersecurity is one of the four key research priority areas within FBIT and we will work to ensure we bid for a CRC in Cybersecurity (or related area) position within our faculty at any opportunity in the coming years.

In addition, I am currently working with Advancement to create opportunities for donor funds to support a research chair position in Cybersecurity (or related area).

Recommendation 2

Enhance Interdisciplinary Opportunities: The program should further integrate interdisciplinary courses and projects that involve fields such as AI, law, and business ethics. This can be achieved by developing new courses or modifying existing ones to include interdisciplinary perspectives and problem-solving experiences.

Program's Response
We agree that including of interdisciplinary courses are essential to the success of the program. In addition to the existing courses in these areas, several new courses have been proposed by the affiliated faculty members in the program and will be sent for approval to FBIT faculty council.

Dean's response
This recommendation is well received and we will work to ensure that new courses are proposed and receive Faculty Council so they can then continue through the remaining governance structure of approvals. Actual course offerings year on year will be managed within the context of the overall budget of courses offered within the faculty and specifically for this program based on enrolment.

Recommendation 3
Industry Collaboration and Partnerships: Strengthen ties with the cybersecurity industry to facilitate ongoing student engagement through internships, guest lectures, and live project collaborations. This requires reaching out to potential industry partners and setting up agreements that benefit both the students and the companies involved.

Program's Response
We agree. Our initial plan includes accelerating such partnerships through the Institute for CyberSecurity and Resilient Systems (ICRS) and the National Cybersecurity Consortium (NCC). Once the program is approved, an industry advisory board will be established to provide further directions and contacts for FBIT cybersecurity programs

Dean's response
We will capitalise on our partnerships through the Institute for CyberSecurity and Resilient Systems (ICRS) and the National Cybersecurity Consortium (NCC) to create such student engagement opportunities.

Suggested Revisions for the Proposal following External Review

- *Program to list all suggested revisions to the proposal*
- *For each suggested revision, the Dean should include a comment indicating whether the revision will proceed. If the revision will not proceed, please indicate a rationale*

Added in Section 4.b:

“As recommended in the external reviewers report, it is recommended that the university prioritize hiring or appointing research chairs (NSERC CRC, Industry chairs or university research chairs) in cybersecurity, particularly in areas related to social and business aspects of cybersecurity. This is an important area of growth in the faculty and a differentiating factor that would enhance the multidisciplinary nature of the program.”

OntarioTech UNIVERSITY

ACADEMIC COUNCIL REPORT

SESSION:		**ACTION REQUESTED:**	
Public	☒	**Decision**	**X**
		Discussion/Direction	□
		Information	□
Financial Impact	□ **Yes X No**	**Included in Budget**	□ **Yes** □ **No**

TO:	**Academic Council**
DATE:	**November 26, 2024**
FROM:	**Research Committee**
PRESENTED BY:	**Les Jacobs, Vice-President, Research and Innovation**
SUBJECT:	**Mindful Artificial Intelligence Research Institute (MAIRI) Centre**

COMMITTEE MANDATE:

In accordance with Article 1.4(b) of By-law No. 2 and the Procedures for the Creation of Research Entities, Academic Council makes recommendations to the Board on matters including the establishment of research centres.

Recommendation: The Research Committee, at its November 19, 2024 meeting, reviewed the proposal to create the Mindful Artificial Intelligence Research Institute (MAIRI) Centre proposed by six Faculty Members from the Faculty of Business and Information Technology, Faculty of Science, Faculty of Health Science, Faculty of Social Science and Humanities, Faculty of Education and the Faculty of Engineering and Applied Science.

We request that Academic Council review the Mindful Artificial Intelligence Research Institute (MAIRI) Centre proposal and find it appropriate to recommend to the Board of Governors for approval.

BACKGROUND/CONTEXT & RATIONALE:

Ontario Tech University encourages and provides a mechanism for the formal establishment of research entities such as research institutes. Research institutes should be cross faculty, and proposals are sponsored by the leading Faculty's Dean. The process for the establishment of research entities is outlined in the Procedures for the Establishment of Research Groups, Units, Centres and Institutes.

There is a desire among faculty to create a new interdisciplinary, cross-faculty research entity in the broad area of Artificial Intelligence. Thorough consultation and concept development by faculty from across the university has led to the creation of a proposal for the **Mindful AI Research Institute (MAIRI)**, as described in the accompanying documentation.

RESOURCES REQUIRED:

There are already several existing research labs across all the faculties that are carrying out excellent research in this area and are well supported, e.g., through CFI and ORF funding. As a connector, MAIRI's value lies in supporting, connecting, and enhancing the capacity in these existing labs, as well as supporting the growth of new ones. We therefore propose that MAIRI be used to provide a consistent identity that complements but does not diminish the strong visibility and reputation these labs already enjoy. Where appropriate, these spaces be enhanced with visible branding, for example on corridor walls and doors.

The Institute is proposed as a new, highly visible 'shop front' location, primarily aimed at visitors, partners, and students, that can also serve as a collision space for researchers from different labs and faculties. This physical space is at the concept stage, and a separate request to this proposal will be made at a later date, through the normal space planning procedures.

In terms of equipment, the University already enjoys substantial resources in this area, including high performance computing, maker spaces, labs, and collaboration spaces, thanks to several external grants. It is envisaged that future CFI bids (including those associated with future CRCs) can be used to enhance this. Members of the Institute Leadership Team and other parts of the University's administration are in parallel exploring options for future equipment purchases (such as high-performance computing / data centre facilities), and these will continue in parallel to the establishment of MAIRI. However, MAIRI's establishment is not dependent on these efforts, rather complementary.

Initial resources for Institute launch include computing equipment for the Institute Manager, a marketing and events budget for a visible launch, and annual conferences, Some pump-priming funds to support the development of novel internal collaborations, likely through match funding, will unlock and incentivize new interdisciplinary funding opportunities.

8.1. Staffing Requirements and Governance Structure

Reflecting the socio-technical nature of AI, **the institute will be interdisciplinary and cross-faculty by design**. It will be led by an Institute Leadership Team (ILT) comprised of a Director and two theme co-leads for each research theme, from different faculties. The Director role may also overlap with a theme co-lead. In the event that a Faculty is not represented, a representative from that Faculty will also be appointed to the ILT. It is envisaged that the Institute is supported by an Research Project Manager who will report to the Director. The Director will be responsible for chairing the ILT, and for overall strategic direction and financial accountability for the Institute. The theme co-leads will be responsible for advancing and connecting research and related activity in their respective thematic areas. The Institute Manager will be responsible for day-to-day management and coordination, media and publicity, event management, partnerships, and supporting the ILT.

The Institute will draw on the whole Ontario Tech research community to form its membership; any faculty members with an interest in AI research will be invited to join, along with graduate student and postdoctoral researchers, and undergraduate students directly working as part of faculty research projects. In addition, the broader MAIRI community will comprise a diversity of industrial and academic partners, various facets of the public sector and levels of government, the broader student and alumni community at Ontario Tech University, plus civic society and our local community in Durham region. This is sketched in the following diagram.

8.2. Budget and Financial Requirements

MAIRI's operational budget proposal is based on the ILT being formed from extant faculty, plus a new full-time Research Project Manager. The budget also supports activities to ensure an effective and visible launch, capacity-building events including an annual conference, and pump-priming funds to seed and support new interdisciplinary collaborative projects that can unlock new external funds.

Additional operating funds will initially be supported by seed funds from the Office of the VPRI, Deans, and Advancement. Over a three-year time horizon, we plan for MAIRI to be self-sufficient through grants, grant overheads, service contracts, and Advancement-led fund-raising activities. It is anticipated that with the critical mass of the Institute, our capacity to win larger grants will increase to support this. The initial Director will be able to commit time thanks to course releases associated with their current CRC, and this represents a strategic use of CRC resources within the University. At this time, it should be noted that Advancement are already actively pursuing funding opportunities to support and grow the Institute.

The planned initial budget is attached. Years 1 and 2 include start-up funds from the University as mentioned above, Year 3 and beyond assume operation based on research grant overheads and fund-raising.

ALIGNMENT WITH MISSION, VISION, VALUES & STRATEGIC PLAN:

Ontario Tech University's Strategic Research Plan, 2020-2025 aims to foster interdisciplinary research collaborations that address complex global challenges. One of the strategic priority areas is Data science, artificial intelligence and new technologies. The MAIRI initiative clearly aligns with this priority area.

-

CONSULTATION:

- Consultation and feedback on the establishment of the Mindful Artificial Intelligence Research Institute (MAIRI) Centre were carried out at different levels among all Faculties starting from March 2024 to October 2023. The proposal of the MAIRI Centre was presented in the FBIT Faculty Council in June 2024. Then, the proposal was discussed with the University Research Committee on October 7, 2024, where it was agree upon, in principle, with the request for full proposal at the November 19, 2024.

COMPLIANCE WITH POLICY/LEGISLATION:

The establishment of the MAIRI Centre aligns with Ontario Tech University's Procedure for the Creation of Research Units, Centres, and Institutes.

NEXT STEPS:

Board of Governors for approval.

MOTION FOR CONSIDERATION:

That pursuant to the recommendation of the Research Committee, Academic Council hereby recommends the Establishment of Mindful Artificial Intelligence Research Institute (MAIRI) Centre for approval by the Board of Governors, as presented.

SUPPORTING REFERENCE MATERIALS:

- MAIRI proposal documentation, including two appendices.

Research Entity Proposal: The Mindful Artificial Intelligence Research Institute (MAIRI)

1. Name of the Entity

The Mindful Artificial Intelligence Research Institute (MAIRI)

2. Proposers – including name, title, and contact information

Sponsoring Dean:
Dr. Carolyn McGregor, Dean, FBIT
carolyn.mcgregor@ontariotechu.ca

Lead Proposer:
Dr. Peter Lewis, Associate Professor & Canada Research Chair, FBIT
peter.lewis@ontariotechu.ca

Other Faculty Proposers:
Dr. Steven Livingstone, Associate Professor, Faculty of Science
steven.livingstone@ontariotechu.ca

Dr. Isabel Pedersen, Professor & Former Canada Research Chair, FSSH
Isabel.pedersen@ontariotechu.ca

Dr. David Rudoler, Associate Professor, FHS and Research Chair, Ontario Shores
David.rudoler@ontariotechu.ca

Dr. Janette Hughes, Professor & Canada Research Chair, Faculty of Education
janette.hughes@ontariotechu.ca

Dr. Qusay Mahmoud, Professor, Faculty of Engineering and Applied Science
qusay.mahmoud@ontariotechu.ca

3. Background Description and Justification

One of the great stories of the 2020s will undoubtedly be the accelerating development and pervasive use of Artificial intelligence (AI) technology, along with its profound impact on humanity. AI systems, intended to reproduce human intelligent behaviour, are transforming businesses, many professions, and society at large. In doing so, new questions are raised almost daily around this technology's capabilities, potential uses, and possibilities, as well as its limitations, potential for harm, and trustworthiness. At the same time, intelligent machines based on principles from living systems and ecosystems are inspiring a new wave of intelligent socio-cyber-physical systems embedded in the digital platforms, cities, agriculture, and infrastructure of the 21st century. Furthermore, new research is giving rise to novel forms of intelligence in machines that go beyond human capabilities in many ways. Yet such 'superhuman' capabilities in specific domains are usually accompanied by an absence of many features of human minds, such as social intelligence, reflection, and common sense, that we are used to taking for granted. **This leads to a number of complex challenges that must be viewed from an interdisciplinary, socio-technical perspective.**

Taken together, these emerging technologies require us to understand the current and possible forms of intelligent machines we can create, how to develop them purposefully, collaboratively, and well, and how to harness them for benefit of humanity and the planet. **By nature of our vision, existing expertise, partnerships, and agility, Ontario Tech University is uniquely positioned to rise to this research challenge.** Existing research strengths around trustworthy and responsible AI, software quality, data science, smart devices, critical study of technology and society, and the development of human-centred technology in business, civil society, healthcare, and education, can combine to provide a platform for a new research agenda for Ontario Tech into the 2030s and beyond.

Within the next decade, the pervasiveness of intelligent machines in society will only grow. This will bring challenges, both technical and social, that we are only beginning to understand. *How* we integrate these new technologies within organizations and society, what we expect of them, and how we build them to meet these new challenges and expectations are all still unclear. **This is a major area of opportunity and differentiated growth in research for Ontario Tech University, both within Canada and globally. By establishing a new cross-faculty and interdisciplinary research institute in this emerging area, we will position the University to be competitive for larger opportunities and enjoy a national and international presence that firmly establishes the University as a leader in this space, further attracting leading researchers.**

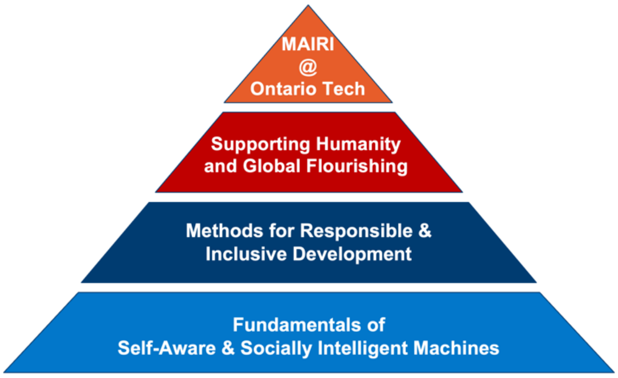
4. Research Mandate

Fundamentally, the mandate of the new **Mindful Artificial Intelligence Research Institute (MAIRI)** will be to ask: what *could* and what *should* intelligent machines be in 10-20 years' time, *when* and *how* should they be used, and *how* will we get there?

As a vision unique to the institute and university, we propose a future where Intelligent Machines…
have **rich and balanced cognitive abilities**,
are developed in **participatory and responsible** ways,
are used **intentionally, carefully, and opportunistically,**
in ways that **empower people** and tackle **global challenges**.

Thus, '*mindful'* intentionally carries simultaneous meanings. On the one hand, mindful means being *careful* and *thoughtful*, before acting. In this sense, being mindful in this space evokes the university's mission of **"tech with a conscience"**, representing the antithesis of the "move fast and break things" culture that is no longer appropriate when considering technology sensitively across society at large. On the other hand, mindful means being *conscious* or *aware* of something, especially context, self, and consequences. At a fundamental level, these are the cognitive abilities that future intelligent machines will need to possess to enhance their trustworthiness and act with social intelligence. Many of the pathologies of today's AI systems can be attributed to imbalanced forms of intelligence that lack broader social context and self-awareness. The term *mindful* originates from the notion of "having a good mind".

There is already substantial excellent research in AI, ML, and intelligent systems across the university. Nevertheless, this research is often fractured into silos. **We envisage MAIRI to be a connector** that brings this together, adding value, community, capacity, and critical mass. It will be structured in three research themes:


MAIRI
@
Ontario Tech
Supporting Humanity and Global Flourishing
Methods for Responsible & Inclusive Development
Fundamentals of Self-Aware & Socially Intelligent Machines

Theme 1: Fundamentals of Self-Aware & Socially Intelligent Machines. This draws on insights and understanding from social science as well as technical research in computer science, IT, cognitive science, and artificial life, and includes contributions to architectures & algorithms for reflective self-awareness, mechanisms for social & emotional intelligence, and new capabilities for machines to cooperate and act collectively.

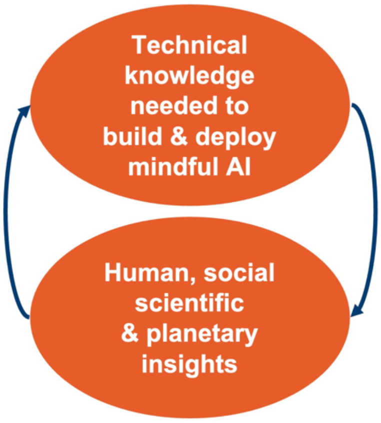
Theme 2: Methods for Responsible & Inclusive Development. This draws on software engineering, human-computer interaction, socio-technical systems, participatory co-design, business (including HR, leadership, organizational ecosystems), and sustainability, and includes contributions to responsible design practices, rigorous & repeatable development, democratizing co-design processes, privacy by design, and sustainable and low-energy AI systems and models.

Theme 3: Supporting Humanity & Global Flourishing. This draws on expertise in the application of intelligent machines in a diverse and open-ended set of domains, initially envisaged to include health and wellbeing, accessibility, education, sustainability, robotics, virtual agents and avatars, business, and community action. Targeted contributions include new technologies for social good that are by-design socially & culturally sensitive, safe, ethical, privacy-preserving, that support the empowerment of individuals & communities, new opportunities for social & planetary benefit, and education and AI literacy for all.

In summary, our research creates the technical contributions needed to realize the vision of intelligent machines that empower humanity, built on a deep understanding of personal, social, organizational, and planetary context.

The **Mindful Artificial Intelligence Research Institute** represents an opportunity to build on Ontario Tech's strengths, commitments, purpose, and strategic objectives:

- Centering the idea of AI *'with a conscience',*
- Advancing the University's research and societal mission,
- Furthering strategic industry, academic, and civic society partnerships.
- Empowering people and organizations with and through technology.


Technical knowledge needed to build & deploy mindful AI
Human, social scientific & planetary insights

By:

- Leading with a creative, ambitious, and distinctive research vision, in line with the University's objective of *differentiated growth*.
- Taking a holistic perspective on intelligent machines and their ecosystems.
- Taking a People, Society, and Planet-first approach to AI and smart technologies, embedding the University's commitments to furthering social good and sustainability.

As is hopefully clear from the mandate outlined above, MAIRI does not represent a single research project or group of related projects, but a vision of a multi-faceted interdisciplinary program of research, that will emerge based on a sustainable platform connecting AI research across Ontario Tech University and with its partners, and in doing so, unlocking a potential that is already present.

Please see the attached slide deck for more detail on the research themes, vision, and success criteria.

5. Student Involvement and Training

Graduate students, postdoctoral fellows, and undergraduate students engaged in research projects under the supervision of a professor who is a member of MAIRI, will also be invited to be members of MAIRI. As a connecting institute, it is envisaged that students' home lab and program will remain their primary disciplinary community and source of training. It is expected that students from many programs across the University will be members.

MAIRI presents an opportunity to go beyond this, complementing students' 'home' training with new interdisciplinary and community opportunities. It is envisaged that the institute will run a number of events to foster development and collegiality among the student AI research community. These include:

- Dedicated student and postdoc sessions as part of MAIRI events, especially the annual conference.
- An online Discord community to enable networking, sharing of information and advice, collaboration, and socializing, amongst MAIRI student members.
- Regular networking events to support students to find further research positions and jobs, such as the successful *'AI Networking Barbecue'* hosted as a pilot at 2200 North in Summer 2024, which featured a round of lightning talks from students and faculty.
- As MAIRI's research portfolio and expertise develops, the ILT will consider the desire and appropriateness of additional or shared courses, to support interdisciplinary working across labs and faculties, for students at MAIRI.
- A potential MAIRI summer school for students both at Ontario Tech and perhaps externally.
- Open invitation to the broader student community (including undergraduates not currently involved, but with an interest in AI) to campus events, including the annual conference.
- Support and encouragement to attend conferences, and identification of opportunities for cohort-level attendance. This also has the added benefit of increasing the University's visibility at key relevant conferences.
- Students will be able to avail themselves of unique opportunities arising from the increasingly interconnected nature of faculty research.
- The ILT and relevant Deans and Associate Deans may wish to consider new interdisciplinary programs at the graduate level to support MAIRI's growth.

6. Research Dissemination and Service Plan

Dissemination of MAIRI research will occur at multiple levels. First, existing dissemination activity through discipline-specific conferences, journals, and outreach will continue. This will continue to be the primary method of publishing research outputs for MAIRI members, and as MAIRI grows, we hope to be in a position to be able to support this activity to broaden accessibility of these opportunities (especially conferences) to our researchers.

As an institute, MAIRI will seek to amplify this output, through web and social media channels, public media appearances, and a newsletter. The content for these channels will be designed such that research from MAIRI members can be understood by other researchers and the public, in a way that is accessible to non-experts. We will leverage the expertise and resources of the Communications and Marketing team to do this.

The MAIRI website and social channels should at all times represent a vibrant and diverse set of research projects and strengths, and sourcing and maintaining this will be a core task of the Research Project Manager, to avoid overloading professors with more service.

A core part of MAIRI's dissemination will be through events, and these will take two forms. First, internal events aimed at capacity building and experience sharing across the University. These are an important form of dissemination that operates cross-university and with existing partners and is instrumental in unlocking the untapped interdisciplinary capacity we believe to exist. Second, external conferences (for which we may charge a fee) will be targeted externally, and will provide a showcase of MAIRI research, with the aim of both building our reputation and establishing new partnerships. These partnerships will take the form of new external research projects, and also new opportunities to connect with government and civic society, in order to inform and shape the debate concerning AI in Canada and the world, in the years and decades beyond 2025. As outlined in the budget, we plan for a capacity-building conference in Y1, a more open conference aimed at partnership building in Y2, and a highly visible public conference in Y3 and beyond.

Finally, dissemination will be a core part of MAIRI projects that collaborate with industry and civic society. For example, we already enjoy strong relationships with large firms (Meta, Microsoft, OPG, GM) as well as smaller firms (particularly in Durham Region), with public bodies (DDSB, DRDC, etc.), and the non-profit sector (e.g., CNIB, The Pamoja Institute). As we seek to continue to partner with these organizations through future research projects, these partners become key dissemination and knowledge mobilization channels, and spheres of influence.

7. Membership List, CVs and Affiliations

In addition to the members of the proposal team, at launch MAIRI already comprises a proposed membership base from across the University. **At this stage, over 50 faculty members from across all six Ontario Tech Faculties will be members at launch. This initial membership comprises faculty at all career stages and includes five current and two former Canada Research Chairs, as well as three other currently active Research Chairs.**

Further, MAIRI will operate an open membership model, where any Faculty with an interest in AI, broadly speaking, may join the institute, and graduate students and postdocs may also become members and so benefit from networking, collaborative, and potential funding opportunities. Additionally, research labs may also affiliate to the institute, forming a collective that preserves the uniqueness and reputation of individual labs, while also forming part of a critical mass to support larger opportunities and sense of community.

A full list of all proposed initial members, with abbreviated CVs for each, is in the appendix.

8. Resource Requirements

There are already several existing research labs across all the faculties that are carrying out excellent research in this area and are well supported, e.g., through CFI and ORF funding. As a connector, MAIRI's value lies in supporting, connecting, and enhancing the capacity in these existing labs, as well as supporting the growth of new ones. We therefore propose that MAIRI be used to provide a consistent identity that complements but does not diminish the strong visibility and reputation these labs already enjoy. Where appropriate, these spaces be enhanced with visible branding, for example on corridor walls and doors.

We propose that the Institute has a new, highly visible 'shop front' location, primarily aimed at visitors, partners, and students, that can also serve as a collision space for researchers from different labs and faculties. This physical space is at the concept stage, and a separate request to this proposal will be made at a later date, through the normal space planning procedures.

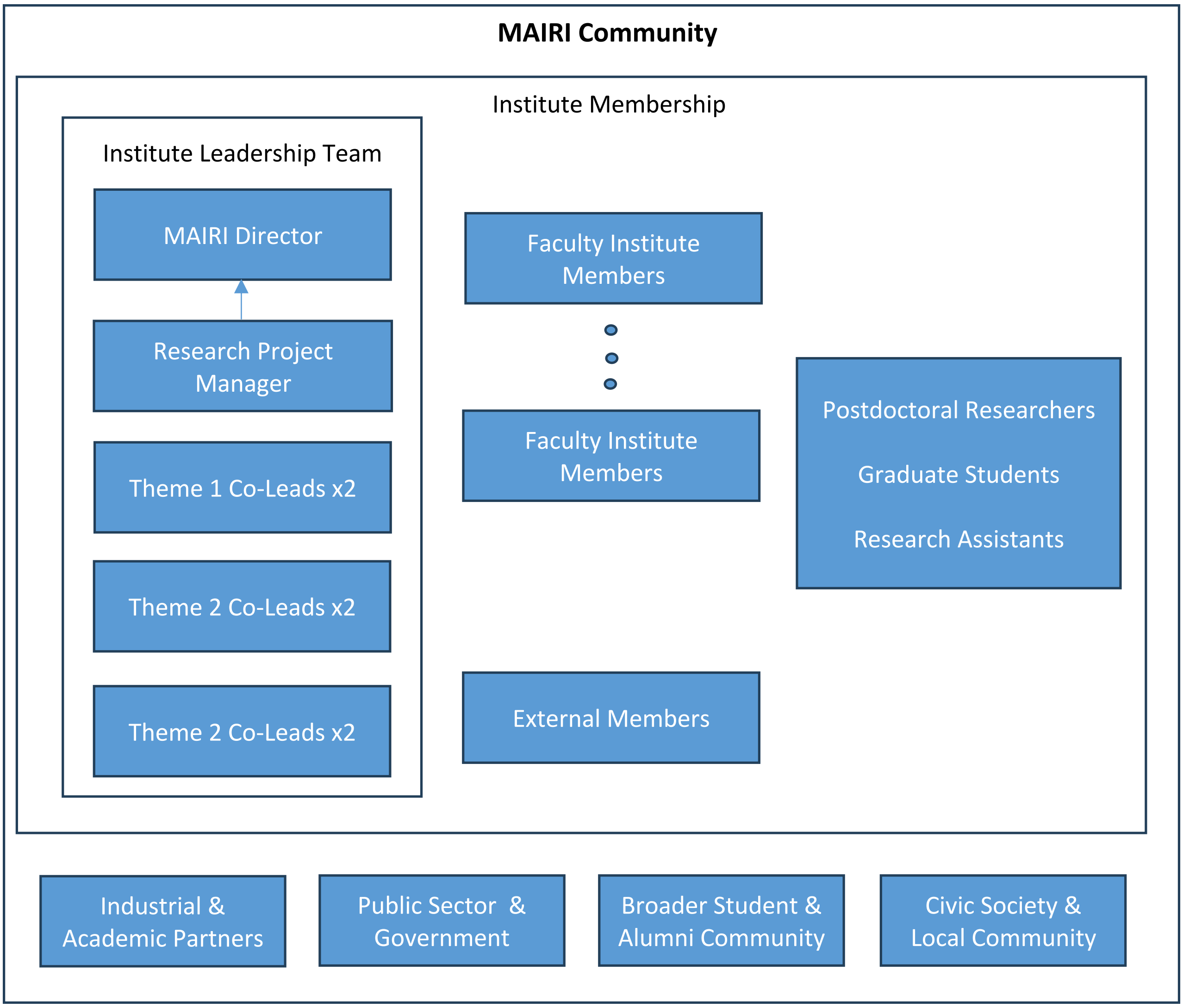
In terms of equipment, the University already enjoys substantial resources in this area, including high performance computing, maker spaces, labs, and collaboration spaces, thanks to several external grants. It is envisaged that future CFI bids (including those associated with future CRCs) can be used to enhance this. Members of the Institute Leadership Team and other parts of the University's administration are in parallel exploring options for future equipment purchases (such as high-performance computing / data centre facilities), and these will continue in parallel to the establishment of MAIRI. However, MAIRI's establishment is not dependent on these efforts, rather complementary.

Initial resources for Institute launch include computing equipment for the Institute Manager, a marketing and events budget for a visible launch, and annual conferences, Some pump-priming funds to support the development of novel internal collaborations, likely through match funding, will unlock and incentivize new interdisciplinary funding opportunities.

8.1. Staffing Requirements and Governance Structure

Reflecting the socio-technical nature of AI, **the institute will be interdisciplinary and cross-faculty by design**. It will be led by an Institute Leadership Team (ILT) comprised of a Director and two theme co-leads for each research theme, from different faculties. The Director role may also overlap with a theme co-lead. In the event that a Faculty is not represented, a representative from that Faculty will also be appointed to the ILT. It is envisaged that the Institute is supported by an Research Project Manager who will report to the Director. The Director will be responsible for chairing the ILT, and for overall strategic direction and financial accountability for the Institute. The theme co-leads will be responsible for advancing and connecting research and related activity in their respective thematic areas. The Institute Manager will be responsible for day-to-day management and coordination, media and publicity, event management, partnerships, and supporting the ILT.

The Institute will draw on the whole Ontario Tech research community to form its membership; any faculty members with an interest in AI research will be invited to join, along with graduate student and postdoctoral researchers, and undergraduate students directly working as part of faculty research projects. In addition, the broader MAIRI community will comprise a diversity of industrial and academic partners, various facets of the public sector and levels of government, the broader student and alumni community at Ontario Tech University, plus civic society and our local community in Durham region. This is sketched in the following diagram.



At launch, MAIRI membership will be comprised only of Ontario Tech employees and students. Following an initial launch campaign, the ILT will identify existing and new collaborators from the broader MAIRI community who may be invited to join the institute as External Members. For example, Ontario Tech already enjoys many productive partnerships with outside organizations in this area, including Microsoft, Meta, the Government of Ontario, CNIB, Ontario Power Generation, The Pamoja Institute, Ontario Shores, and Lakeridge Health.

Decision making at the Institute-level will be normally made by Committee decision at the ILT. The Director will have responsibility for executive action on behalf of the ILT, for sound financial management of the Institute, and will line manage the Research Project Manager. More broadly, MAIRI will operate in a federated model, where labs that are affiliated to the Institute will operate independently in line with normal University practice, able to draw on the strength and network of the Institute, as appropriate and as it is advantageous to do so. Further, theme leads will coordinate activity within their respective themes, and will report to the ILT on their strategy, activity, and outcomes.

8.2. Budget and Financial Requirements

MAIRI's operational budget proposal is based on the ILT being formed from extant faculty, plus a new full-time Research Project Manager. The budget also supports activities to ensure an effective and visible launch, capacity-building events including an annual conference, and pump-priming funds to seed and support new interdisciplinary collaborative projects that can unlock new external funds.

Additional operating funds will initially be supported by seed funds from the Office of the VPRI, Deans, and Advancement. Over a three-year time horizon, we plan for MAIRI to be self-sufficient through grants, grant overheads, service contracts, and Advancement-led fund-raising activities. It is anticipated that with the critical mass of the Institute, our capacity to win larger grants will increase to support this. The initial Director will be able to commit time thanks to course releases associated with their current CRC, and this represents a strategic use of CRC resources within the University. At this time, it should be noted that Advancement are already actively pursuing funding opportunities to support and grow the Institute.

The planned initial budget is attached. Years 1 and 2 include start-up funds from the University as mentioned above, Year 3 and beyond assume operation based on research grant overheads and fund-raising.

9. Intellectual Property and Commercialization

As a broad research institute capturing many different disciplinary norms and pathways to impact, MAIRI will not take a specific position on intellectual property and commercialization beyond that already captured in policy and practice at the University level. It is expected that specific projects and professors will engage in the IP and commercialization processes as before. However, MAIRI may provide opportunities to share best practice on doing this, and new opportunities for partnership to achieve commercialization or other forms of impact (for example, through commercialization workshops). MAIRI members may engage in contract work as they currently do, but it is not foreseen at this stage that MAIRI will, as an entity in itself, engage in contract work.

Appendix A: Faculty Membership of MAIRI at the time of proposal.
Presented in alphabetical order by first name.

Aaron Yurkewich

Assistant Professor, Faculty of Engineering and Applied Science

I am an Assistant Professor in Mechatronics Engineering with a focus on assistive and rehabilitation technology development and evaluation. I have 10 years of experience developing and evaluating stroke rehabilitation technology, such as a lower limb robot for foot drop exercise and gait training (University of Western Ontario), a hand exoskeleton for hand and upper limb motion assistance and home and clinic rehabilitation (University of Toronto, Toronto Rehabilitation Institute), and a hybrid electrical stimulation and exoskeleton system for accelerated strengthening and motor learning (Imperial College London). I have conducted clinical rehabilitation trials in clinic and home settings in Canada and globally utilizing exoskeletons and soft robots and human robot interaction, haptics, neuroscience and neurorehabilitation principles. I work with international partners in transdisciplinary teams to create accessible and affordable evidence-based rehabilitation solutions for in-clinic and at-home settings.

Key Publications:

- Yixing Lei, Zhiqun Ding, Aaron Yurkewich. (2023). Computer Vision-based Automated Functional Electrical Stimulation Calibration System for Inducing Functional Hand Postures. International Functional Electrical Stimulation Society (IFESS). RehabWeek 2023, Singapore
- Aaron Yurkewich, Illya Kozak, Andrei Ivanovic, Daniel Rossos, Debbie Hebert, Rosalie Wang, Alex Mihailidis. (2020). Myoelectric Untethered Robotic Glove Enhances Hand Function and Performance on Daily Living Tasks after Stroke. Journal of Rehabilitation and Assistive Technologies Engineering (RATE). 7: 1-14.

Alyson King

Professor, Political Science; Associate Dean, Faculty of Social Science and Humanities

My research focuses on the success strategies and experiences of university students and adult learners. I am a co-investigator for an on-going Partnership Grant called Partnership on University Plagiarism Prevention (PUPP) that aims to develop an international strategy to prevent plagiarism. As Principal Investigator for a completed Social Sciences and Humanities Research Council (SSHRC) Partnership Development grant, I worked with a team of researchers from across Canada to better understand how underrepresented university students are successful in their university studies. As a co-investigator on a completed SSHRC

Insight Grant, I conducted research with Dr. Shanti Fernando, Dr. Allyson Eamer and Dr. Tyler Frederick on supported education for adults living with mental illness.
Other research has included an oral history project collecting the stories of the founding members of Ontario Tech University (with Dr. Shirley Van Nuland) and a project on multiliteracies and graphic novels (with Dr. Janette Hughes). Currently, I am exploring the intersections with emerging GenAI technology and education, in particular around critical thinking, writing and learning.

Key Publications (forthcoming):

- King, A. & Garramone, P. (accepted). Teaching writing in the time of ChatGPT: Rethinking what counts as learning. In A. E. King (Ed.). Artificial Intelligence, Assessments and Academic Integrity. Switzerland: Springer Nature.

- King, A. E. (Ed.) (accepted) Artificial Intelligence, Assessments and Academic Integrity. Full manuscript submitted to and under review, Springer Nature, Sept. 2024. Symposium

Ana Duff

Associate Teaching Professor, Faculty of Business and IT

Dr. Ana Duff is an Associate Teaching Professor with the Faculty of Business and Information Technology at Ontario Tech University. Her research background is in mathematics in which she holds a Ph.D. from the University of Ottawa. She began her studies in mathematics at the University of Zagreb in Croatia, continuing at York University in Toronto, from which she received her B.Sc. (Honours), and followed by an M.Sc. from the University of Toronto. Her original research background is in Lie superalgebras, mathematical structures that hold an important role in quantum physics and the mathematics of supersymmetry.

She has been with Ontario Tech University since September 2017, where she teaches first year courses in mathematics and has been active in the practice of responsible management education in the context of people, planet and prosperity. Her efforts in teaching novices in advanced studies has refocused her research interests to that of problem-solving and, specifically, teaching problem-solving. Within the context of AI and its emergent role in the area of education, Dr. Duff is interested in the potential of using AI to support the growth of human, i.e., non-artificial intelligence. She is interested in the question of whether and how machine learning algorithms and AI can help individuals grow their capability in analytical, logical and holistic reasoning. Specifically, she is interested in how these systems and the underlying algorithms can mindfully yet rigorously challenge the user through questions rather than providing answers. At the same time, aware of the immense drain these systems put on natural environments and human systems, she is interested in the question of balance and the need for critical introspective when choosing to develop and/or use an AI-based tool for a particular task when such a task can be potentially accomplished with a comparatively lower negative impact on nature and/or society.

Prior to Ontario Tech University, Dr. Duff taught mathematics at the University of Ottawa, Royal Military College of Canada and the International School of Belgrade in Serbia. She also has extensive experience in developing and managing large-scale community mobilization and education programs in Canada and overseas within non-government and government sectors. She has received multiple recognitions, including teaching awards from the University of Ottawa and the Royal Military College of Canada, and was nominated and has received numerous awards for her teaching at Ontario Tech.

Andrea Slane

Professor, Legal Studies, Faculty of Social Science and Humanities

Dr. Andrea Slane J.D. PhD (she/her) is a Professor of Legal Studies in the Faculty of Social Science and Humanities, Ontario Tech University, Canada. Her research focuses on law's interface with digital communication and information technologies, including the nature of privacy interests and appropriate limits to privacy protection; legal approaches to addressing sexual exploitation and other wrongdoing online; and legal and ethical methods to protect and promote autonomy, dignity and identity in the face of rapidly evolving technological advancements in artificial intelligence. Dr. Slane is currently engaged in two projects - one aiming to promote informed public dialogue about the governance of police use of facial recognition technology, and another on the ways legal approaches to AI used for social support and companionship struggle to make principled distinctions between humans, companies/platforms, and autonomous AI entities. Her work and teaching centrally concern the social impacts of technologies and the legal and policy protections needed to ensure both redress for wrongs and means to build an environment able to support safe, equitable and principled use.

Key Publications:

- Andrea Slane and Isabel Pedersen, "Older People's Ethical Framing of Autonomy in Relation to Current and Future Consumer Technologies: The Case of Socially Assistive Robots" International Journal of Social Robotics (forthcoming 2025).

- Andrea Slane and Isabel Pedersen, "Bringing Older People's Perspectives on Consumer Socially Assistive Robots into Debates about the Future of Privacy Protection and AI Govern-ance" (2024) AI & Society: Journal of Knowledge, Culture and Communication, https://doi.org/10.1007/s00146-024-01894-3.

- Dallas Hill, Christopher O’Connor, and Andrea Slane, “Police Use of Facial Recognition Technology: The Potential for Engaging the Public through Co-Constructed Policy-Making” (2022) 24:3 International Journal of Police Science and Management, 325-335, https://doi.org/10.1177/14613557221089558.

- Andrea Slane, “Privacy Protective Roadblocks and Speedbumps Restraining Law Enforcement Use of Facial Recognition Software in Canada” (2021) 69:2 Criminal Law Quarterly 216-236. Available at SSRN: https://ssrn.com/abstract=4275241

Andrew Hogue

Associate Professor, Game Development and Interactive Media, Faculty of Business and IT

Dr. Andrew Hogue is an Associate Professor in the Game Development and Interactive Media program. Since joining Ontario Tech in 2007, Dr. Hogue has attracted over $7.6M in research and development funds, bolstering the study and application of new technologies in digital media. Dr. Hogue's main research interests currently revolve around the development of new technologies and experiences that utilize Volumetric Video and his team are currently exploring the implications of varying visual realism in XR and its effects on user experience, self-efficacy, and knowledge retention in interactive experiences. Dr. Hogue is currently co-authoring the forthcoming 4th edition of Rick Parent’s acclaimed textbook, "Computer Animation: Algorithms and Techniques". He has supervised more than 120 undergraduate R&D projects, 15 graduate, and 1 post-doctoral fellow. Dr. Hogue was the Technical Program Committee Chair for IEEE GEM 2023 and Dr. Hogue's work has been widely recognized with over 60 peer-reviewed journal and conference articles, and has co-authored a patent on Telepresence Management for Remote Aid for Surgery while consulting with a tech startup.

Annie En-Shiun Lee

Assistant Professor, Computer Science, Faculty of Science

Professor Annie En-Shiun Lee is an assistant professor at OntarioTech University and the University of Toronto (status-only). Professor Lee’s goal is to make language technology as inclusive and accessible to as many people as possible. She runs the Lee Langauge Lab (L^3) with research focusing on language diversity and multilingualism.

Professor Lee’s research has been published in Nature Digital Medicine, ACM Computing Survey, ACL, SIGCSE, IEEE TKDE, and Bioinformatics. Professor Lee has contributed significant expertise to industry and government through a track record of successful technology transfer over the past decade with 14 partners. She serves as the demo co-chair for NAACL and has extensive experience transferring technology to industry.

Key Publications:

- Surangika Ranathunga, En-Shiun Annie Lee, Marjana Prifti Skenduli, Ravi Shekhar, Mehreen Alam, and Rishemjit Kaur. 2023. Neural Machine Translation for Low-resource Languages: A Survey. ACM Comput. Surv. 55, 11, Article 229 (November 2023), 37 pages. https://doi-org.myaccess.library.utoronto.ca/10.1145/3567592

- En-Shiun Lee, Sarubi Thillainathan, Shravan Nayak, Surangika Ranathunga, David Adelani, Ruisi Su, and Arya McCarthy. 2022. Pre-Trained Multilingual Sequence-to-Sequence Models: A Hope for Low-Resource Language Translation?. In Findings of the Association for Computational Linguistics: ACL 2022, pages 58–67, Dublin, Ireland. Association for Computational Linguistics.

- David Adelani, Hannah Liu, Xiaoyu Shen, Nikita Vassilyev, Jesujoba Alabi, Yanke Mao, Haonan Gao, and En-Shiun Lee. 2024. SIB-200: A Simple, Inclusive, and Big Evaluation Dataset for Topic Classification in 200+ Languages and Dialects. In Proceedings of the 18th Conference of the European Chapter of the Association for Computational Linguistics (Volume 1: Long Papers), pages 226–245, St. Julian's, Malta. Association for Computational Linguistics.

- Wong, A.K.C., Zhou, PY. & Lee, A.ES. Theory and rationale of interpretable all-in-one pattern discovery and disentanglement system. npj Digit. Med. 6, 92 (2023). https://doi.org/10.1038/s41746-023-00816-9

- Franke, B., Plante, J.F., Roscher, R., Lee, E.S.A., Smyth, C., Hatefi, A., Chen, F., Gil, E., Schwing, A., Selvitella, A. and Hoffman, M.M., 2016. Statistical inference, learning and models in big data. International Statistical Review, 84(3), pp.371-389.

Asifa Aamir

Associate Teaching Professor, Faculty of Business and IT

I have master's degrees in Information Systems Engineering and Business administration (Tech. Management). I have been in academia for over 14 years. My teaching approach focuses on applied learning, where students gain hands-on experience in current IT/IS topics including artificial intelligence. My academic background and teaching experience provides me with a robust understanding of information technology applications within business contexts, helping me fuel my learning interests around the ethical and operational implications of emerging technologies in business environments. I am also working with Continuous Learning at Ontario Tech. In this capacity, I have facilitated specialized workshops for industry professionals, focusing on foundational AI concepts with an emphasis on ethical and security considerations relevant to business contexts.

Bobby Stojanoski

Assistant Professor, Faculty of Social Science and Humanities

The overarching aim of my research program is to understand the links between social and cognitive development and the underlying changes in the structure and function of the brain in neurotypical and neurodiverse youth populations, in particular, autistic children. My research places the environment front and center by incorporating factors such as socioeconomic status, adverse life experiences, and elements of lifestyle, such as sleep habits in his work examining the developing mind and brain.

I use various neuroimaging methods, including functional magnetic resonance imaging but also electroencephalography and functional near-infrared spectroscopy, which he recently received two large operating grants to bring this equipment to Ontario Tech. My research incorporates in-lab and online cognitive tests, and movie watching paradigms and applies computational analytic approaches to examine social and cognitive functioning in neurotypical and autistic children and adolescents.

Key Publications:

- Pho, B., Stevenson, R., Mohsenzadeh, Y., & Stojanoski, B. (2024). Using Machine Learning To Identify Neural Mechanisms Underlying the Development of Cognition in Children and Adolescents With ADHD. Developmental Cognitive Neuroscience

- Deng, Z., Li, Z., Gao, J., Stojanoski, B., & Chen, J. (under review). Differential representation of “toolness” and the elongated shape of tools revealed by continuous flash suppression and backward masking. Scientific Advances

Carolyn McGregor

Professor and Dean,
Research Chair in Artificial Intelligence for Health and Wellness,
Director, Joint Research Centre in AI for Health and Wellness,
Two-time Canada Research Chair in Health Informatics,
Faculty of Business and IT

Professor Carolyn McGregor AM is a two-time Canada Research Chair. She is the Founding Director and Research Chair of the Joint Research Centre in AI for Health and Wellness between Ontario Tech University in Canada and the University of Technology Sydney in Australia. Dr McGregor has led pioneering research in artificial intelligence, big data analytics, stream computing, deep learning, internet of things, temporal data mining, edge computing and cloud computing. She progresses research within the context of critical care medicine, precision public health, mental health, astronaut health together with military and civilian tactical training. She is the inventor of two internationally leading big data/AI based platforms Artemis and Athena used to improve health, wellness, resilience and adaptation. She has been awarded over $15 million in research funding and has led multiple large research programs including a highly acclaimed multi-million dollar First-of-A-Kind (FOAK) research program with IBM and a $3M project within the FedDev Ontario Health Ecosphere Innovation Pipeline project. She has over 190 refereed publications, 3 patents in multiple jurisdictions and has established two startup companies resulting from her research. She has extensive research collaborations in Canada, USA, Australia and India. She serves on government committees in Australia, Canada, France and Germany. She has received many awards for her research. In 2014 she was awarded membership in the Order of Australia for her significant service to science and innovation through health care information systems. In 2017 she was featured in the 150 Stories series commissioned by the Lieutenant Governor of Ontario and the Government of Canada to commemorate the 150th year anniversary of Ontario. In 2018 she was named as a Women Leader in Digital Health by Digital Health Canada. In 2022 she led a research study performed on the AXIOM Ax-1 all private astronaut mission to the ISS.

Key Publications:

- McGregor, C, and Rastpour, A., Predicting Patient Wait Times by Using Highly Deidentified Data in Mental Health Care: Enhanced Machine Learning Approach, JMIR Mental Health 9 (8), e38428, 2022

- McGregor, C., 2018, “Using Constructive Research to Structure the Path to Transdisciplinary Innovation and Its Application for Precision Health with Big Data Analytics, Technology Innovation Management Review, 8(8): 7–15. http://doi.org/10.22215/timreview/1174

- Kamaleswaran R., McGregor, C., 2016, “A Review of Visual Representations of Physiologic Data”, JMIR Medical Informatics, 4(4), e31 , doi:10.2196/medinform.5186
- Khazaei, H., McGregor, C., Eklund, J.M., El-Khatib, K., 2015, “Real-time and Retrospective Health Analytics as a Service”, JMIR Medical Informatics, 3(4), e36
- Khazaei, H., Mench-Bressan, N., McGregor, C., Pugh, J.E., 2015, “Health Informatics for Neonatal Intensive Care Units: an Analytical Modeling Perspective”, IEEE Journal of Translational Engineering in Health and Medicine, 3, pp 1-9

David Rudoler

Associate Professor, Faculty of Health Sciences,
and
Research Chair, Population Health and Innovation in Mental Health,
Ontario Shores Centre for Mental Health Sciences

David Rudoler is an applied health services researcher with expertise in health policy, health economics, econometrics, health economic evaluation, administrative data analysis, and mixed methods. He holds a Research Chair in Population Health and Innovation in Mental Health at Ontario Shores Centre for Mental Health Sciences, and is also an Assistant Professor in the Faculty of Health Sciences at Ontario Tech University. David is also an Adjunct Scientist at ICES in the Mental Health & Addictions Research Program. His research interests include health human resources, including the supply of community-based primary and mental health services; the evaluation of policy interventions, including provider responses to payment models and incentives; the evaluation of community-based interventions for people with serious mental illness; and the application of methods in data science to issues in population health and mental health care services.

Key Publication:

- Jamieson et al. (2024). Stratified Care in Cognitive Behavioural Therapy: A Comparative Evaluation of Predictive Modeling Approaches for Individualized Treatment. Canadian Journal of Psychiatry. DOI: 10.1177/07067437241295635. [In Press].

Faisal Qureshi

Professor, Computer Science, Faculty of Science

Faisal Z. Qureshi is a Professor of Computer Science at University of Ontario Institute of Technology (OntarioTech), Oshawa, Canada, where he directs the visual computing lab. He also holds a Guest Professorship at Mid Sweden University, Sundsvall, Sweden. He holds a Ph.D. and an M.Sc. in Computer Science from the University of Toronto, Canada, an M.Sc. in Electronics from Quaid-e-Azam University, Pakistan, and a B.Sc. in Mathematics and Physics from Punjab University, Pakistan. He joined OntarioTechU in 2008 from Autodesk Canada Co., Toronto. Dr. Qureshi's research interests center around computer vision, camera networks, and video summarization. He is a recipient of Computer Robot Vision (CRV) 2017 Best Vision Paper award and ACM/IEEE International Conference on Distributed Smart Cameras 2007 Outstanding Paper award. Dr. Qureshi is also active in journal special issues and conference organizations, serving as the general co-chair for the Workshop on Camera Networks and Wide-Area Scene Analysis (co-located with CVPR) in 2011-13. In addition he served as the co-chair of CRV 2015/16. He is a senior member of the IEEE and a member of the ACM. He currently serves as the Secretary of the Canadian Image Processing and Pattern Recognition Society (CIPPRS). In the past he has also served as the program director for the CS undergraduate and graduate programs.

Key Publications:

- Attention Based Simple Primitives for Open-World Compositional Zero-Shot Learning. Munir, A.; Qureshi, F.; Khan, M.; and Ali, M. In Proc. 25th Conference on Digital Image Computing Techniques & Applications (DICTA24), pages 8pp, Perth, November 2024.

- Hyperspectral Pixel Unmixing with Latent Dirichlet Variational Autoencoder. Mantripragada, K.; and Qureshi, F. Z. IEEE Transactions on Geoscience and Remote Sensing, 13pp. 2024.

- Hyperspectral Image Compression Using Implicit Neural Representations. Rezasoltani, S.; and Qureshi, F. In Proc. 20th Conference on Robots and Vision (CRV23), pages 8pp, Montreal, Jun 2023.

- A Temporal Boosted YOLO-Based Model for Birds Detection around Wind Farms. Alqaysi, H.; Fedorov, I.; Qureshi, F. Z.; and O'Nils, M. Journal of Imaging, 7(11): 13pp. 2021.

- A Residual-Dyad Encoder Discriminator Network for Remote Sensing Image Matching. Khurshid, N.; Mohbat; Taj, M.; and Qureshi, F. IEEE Transactions on Geoscience and Remote Sensing, 58: 2001–2014. 2020.

Gabby Resch

Assistant Professor, Faculty of Business and IT

Dr. Gabby Resch is an Assistant Professor whose research explores new methods for making sense of data as it moves between physical and digital worlds. At the moment, he is engaged in research projects that explore geospatial visualization in the context of migration-related policy, the use of scrolling data interactives for medical knowledge translation, and immersive augmented and virtual reality simulation and training environments. He is developing new research on rehabilitation interfaces that combine machine learning and data-driven methods, as well as a project that explores AI content generation and data-driven communication in the context of startup pitch decks.

Hossam Gaber

Professor, Faculty of Engineering and Applied Science

Dr. Gaber is a Professor in the Department of Energy and Nuclear Engineering, the Faculty of Engineering and Applied Science, at Ontario Tech University (UOIT), where he has established the Energy Safety and Control Lab (ESCL), Smart Energy Systems Lab, and Advanced Plasma Engineering Lab. He is the recipient of the Senior Research Excellence Aware for 2016, UOIT. He is recognized among the top 2% of worldwide scientists with high citation in the area of smart energy. He Fellow IET (FIET) and Distinguished Lecturer – IEEE NPSS on Nuclear-Renewable Hybrid Energy Systems and Plasma-based Waste-to-Energy. He is leading national and international research in the areas of smart energy grids, with applied AI on resilient energy and interconnected infrastructures. Dr. Gabbar obtained his B.Sc. degree in 1988 with first class of honor from the Faculty of Engineering, Alexandria University (Egypt). In 2001, he obtained his Ph.D. degree from Okayama University (Japan) in Systems Engineering. From 2001 till 2004, he joined Tokyo Institute of Technology (Japan), as a research associate. From 2004 till 2008, he joined Okayama University (Japan) as an Associate Professor, in the Division of Industrial Innovation Sciences. From 2007 till 2008, he was a Visiting Professor at the University of Toronto. Dr. Gaber is leading multidisciplinary research on smart energy with applied AI that includes smart modeling and Multiphysics simulation, LLM and semantic networks for resilient energy, transportation, and community infrastructures. Among recent development is autonomous drone-based inspection, CT-based integrity control, human experience retention system, and intelligent safety management systems.

Key Publications:

- Hossam A.Gabbar, Abderrazak Chahid, Manir U. Isham, Shashwat Grover, Karan pal Singh, Khaled Elgazzar, Ahmad Mousa, and Hossameldin Ouda, HAIS: Highways Automated-Inspection System, Technologies 2023, 11, 51.

https://doi.org/10.3390/10.3390/technologies11020051.

- Hossam A.Gabbar, Abderrazak Chahid, Md. Jamiul-Alam Khan, Oluwabukola Grace, Matthew Immanuel, CTIMS: Automated Defect Detection Framework Using Computed Tomography (CT), Appl. Sci. 2022, 12(4), 2175; https://doi.org/10.3390/app12042175.

- Hossam A. Gabbar, A. Chahid, M. J. A. Khan, O. Grace-Adegboro and M. I. Samson, "Tooth.AI: Intelligent Dental Disease Diagnosis and Treatment Support Using Semantic Network," in IEEE Systems, Man, and Cybernetics Magazine, vol. 9, no. 3, pp. 19-27, July 2023, doi: 10.1109/MSMC.2023.3245814.

- Hossam A.Gabbar, Sk Sami Al Jabbar, Hassan Hassan, Jing Ren, Development of Knowledge Base using Human Experience Semantic Network for Instructive Texts, Appl. Sci. 2021, 11(17), 8072; https://doi.org/10.3390/app11178072.

- Hossam A.Gabbar, Ahmed S. Eldessouky, Energy Semantic Network for Building Energy Management, Intelligent Industrial Systems, Springer, September, 2015, DOI 10.1007/s40903-015-0023-8.

Hui Zhu

Professor, Finance, Faculty of Business and IT

Dr. Hui Zhu is a Professor of Finance at Ontario Tech University in Canada. She earned her Ph.D. in Economics from Queen’s University. She was a visiting scholar at Johannes Kepler University Linz in Austria and an adjunct professor at the University of Ottawa. Her research is primarily in empirical finance with a significant focus on fixed-income securities, initial public offerings (IPOs), corporate innovation, corporate social responsibility, and international finance. She has published over 20 research papers in refereed journals such as the Journal of Banking and Finance, Journal of Corporate Finance, Financial Management, Journal of Financial Research, International Review of Financial Analysis, Journal of International Financial Markets, Institutions and Money, and Pacific-Basin Finance Journal. She has presented her research findings at over 50 prestigious finance conferences and various research institutions in Canada and internationally. Dr. Zhu received the Faculty Research Excellence Award in 2020 and 2023. She was also a scholarship recipient of the Faculty Mobility for Partnership Building Program and the Canada-China Scholars Exchange Program. Dr. Zhu held internal research grants such as Building Equality, Diversity, Inclusion Knowledge in Research, several Partnership and Research Explore Stream grants, and Research Policy Grants. She has twice held external grants from the Social Sciences and Humanities Research Council of Canada (SSHRC).

Key Publications:

- Is Corporate Social Responsibility A Matter of Trust? A Cross-country Investigation (with Eva Wagner), International Review of Financial Analysis, 93, (May 2024): 103127.
- Investor Heterogeneity and Negative Skewness in Stock Returns: Evidence from Institutional Investors (with Ramzi Benkraiem, Stéphane Goutte, Samir Saadi and Steven Zhu), Journal of International Financial Markets, Institutions and Money, 81, (2022): 101690.
- Does National Culture affect Corporate Innovation? International Evidence (with Narjess Boubakri, Imed Chkir, and Samir Saadi), Journal of Corporate Finance 66, (2021): 101847.
- Institutional Influence on Syndicate Structure and Cross-border Leveraged Buyouts (with Chen Liu and Lynnette Purda), 50(1), Financial Management, (2021): 169-202.
- Customer-Supplier Relationships and the Cost of Debt (with Kelly Cai), Journal of Banking and Finance 110, (2020): 105686.

Igor Kotlyar

Associate Professor, Faculty of Business and IT

Dr. Igor Kotlyar is an Associate Professor in the Faculty of Business and IT at Ontario Tech University, where his research applies Artificial Intelligence to the assessment of interpersonal skills, bridging AI with education, organizational behavior, and human resource management. His work has been published in respected journals across AI, education, and organizational behavior, including Computers in Human Behavior, The Leadership Quarterly, Journal of Creative Behavior, Journal of Research on Technology in Education, International Journal of Artificial Intelligence in Education, and International Journal of Selection and Assessment. Through these publications, he has contributed to critical discourse on AI-enhanced assessment and feedback in both educational and organizational contexts. Dr. Kotlyar holds a PhD from the Rotman School of Management at the University of Toronto. His previous experience founding two tech firms specializing in AI-driven simulation technologies further informs his academic insights, underscoring AI's transformative potential in skill development and evaluation.

Key Publications:

- Kotlyar, I., Pearse, N. J., & Krasman, J. (2024). Understanding cross-country differences in assessment simulations: insights from South African and Canadian students. Discover Education, 3(1), 1-23.
- Kotlyar, I., Sharifi, T., & Fiksenbaum, L. (2023). Assessing teamwork skills: can a computer algorithm match human experts?. International Journal of Artificial Intelligence in Education, 33(4), 955-991.
- Kotlyar, I., & Krasman, J. (2022). Virtual simulation: New method for assessing teamwork skills. International Journal of Selection and Assessment, 30(3), 344-360
- Kotlyar, I., Krasman, J., & Fiksenbaum, L. (2021). Virtual high-fidelity simulation assessment of teamwork skills: How do students react?. Journal of Research on Technology in Education, 53(3), 333-352.

Isabel Pedersen

Professor, Faculty of Social Science and Humanities

Dr. Isabel Pedersen is a Professor of Communication Studies at Ontario Tech University, specializing in the intersection of technological change and its cultural, ethical, and political implications. Dr. Pedersen's research focuses on the lifecycle of technology—design, adoption, and adaptation—with a particular emphasis on Artificial Intelligence. Dr. Pedersen's expertise has been recognized through influential roles, including serving on the Meta Reality Labs Policy Advisory Council, the IEEE Standards Association's Global XR Ethics Working Group (P7030), and as Canada Research Chair (2012-2022). She is the founding Director of the Digital Life Institute, an international research network of multidisciplinary scholars. Her recent co-authored books include Augmentation Technologies and Artificial Intelligence in Technical and Professional Communication: Designing Ethical Futures (Routledge, 2023) and Writing Futures: Collaborative, Algorithmic, Autonomous (Springer, 2021). Her work has appeared in leading journals such as AI and Society, Frontiers in Artificial Intelligence, Journal of Information, Communication and Ethics in Society, and Communication Design Quarterly. In 2020, Dr. Pedersen pioneered Ontario Tech's first graduate course in Global AI Ethics, establishing a framework for ethical considerations in the field of computer science.

Key Publications:

- Pedersen, I. The Rise of Generative AI and Enculturating AI Writing in Postsecondary Education. Frontiers in Artificial Intelligence. Volume 6. 2023.

- Pedersen, I. Generative AI, cultural adaptation, and postsecondary education. (July, 2024) The Open/Technology in Education, Society, and Scholarship Association Journal. 4(1), 1-19.

- Slane, A., and Pedersen, I. Bringing Older People's Perspectives on Consumer Socially Assistive Robots into Debates about the Future of Privacy Protection and AI Governance AI & Society: Knowledge, Culture and Communication. March 16, 2024. https://doi.org/10.1007/s00146-024-01894-3

- Duin, A. H. and Pedersen, I. Augmentation technologies and artificial intelligence in technical communication: Designing ethical futures. Routledge, Taylor & Francis, 2023.

- Duin, A. H. and Pedersen, I. Writing Futures: Collaborative, Algorithmic, Autonomous (Studies in Computational Intelligence) Berlin: Springer-Verlag. 2021.

Janette Hughes

Professor, Canada Research Chair,
Director of Centre for Digital Innovation in Education,
Director of STEAM 3D Maker Lab,
2025-2027 Chair of Women in Research Council

Dr. Janette Hughes is a Canada Research Chair, in Technology and Pedagogy and Professor in the Faculty of Education at Ontario Tech University. She is the recipient of multiple research and teaching awards and research grants. She is widely published (86 PR Journal Articles; 42 Conference Proceedings Papers; 4 Books, 35 Book Chapters) and is author of The Digital Principal, a guide for school administrators who are interested in promoting technology-rich learning environments for students and teachers. Dr. Hughes is a prolific author and presenter, sharing her work both nationally and internationally in prestigious scholarly and professional journals, keynote talks, and conferences. She has presented more than 140 peer-reviewed research papers conferences across Canada, the United States, Europe, Asia, and South America. Attesting to the recognition of her leadership in technology and pedagogy, Dr. Hughes is routinely contacted by school districts, Ministry personnel and industry partners to consult on a variety of topics, including online teaching and learning, equity issues in ed tech, creating innovative learning environments, establishing STEAM focused Makerspaces in schools, shifting pedagogies in a digital era, the social and ethical implications of AI, and how to foster the development of global (21st century) skills and competencies in K-12 and higher education.

Key Publications:

- Morrison, L., Hughes, J., Craig, C. (under review: abstract accepted). AI in education: An ethical framework and rubric in action. Technology, Pedagogy & Education.
- Morrison, L., Hughes, J. & Craig, C. (accepted). Evaluating AI Tools for Use in K-12: A Rubric for Teachers and Students. AI in K-12 Education: Shaping Future Classrooms.
- Hughes, J. & Morrison, L. (accepted). A Brave New World: The Perils of AI Image Generators for Women. AI in K-12 Education: Shaping Future Classrooms.
- Butler-Ulrich, T. & Hughes, J. (accepted). Supporting Ethical Artificial Intelligence Literacy Through Technical Competencies and Critical Thinking. CSSE, McGill University, June 2024.
- Hughes, J. & Gadanidis, M. (accepted). An exploration of AI writing tools for secondary school teachers and students. TIE Conference, Cambridge, UK. March 2025.
- Butler-Ulrich, T., Hughes, J., Morrison, L. (2025). Creativity and Generative AI for Preservice Teachers. In Creativity for Contemporaneity, InTech Open.

Jeremy Bradbury

Professor, Computer Science, Faculty of Science

My research focuses on the development of high-quality testing and debugging practices and education/skills training. First, I focus on the development of new automated testing and debugging tools using machine learning (ML), natural language processing (NLP) and large language models (LLMs) that support the tester. These tools prioritize supporting testers in low-resource contexts (where data and computation maybe limited) as well as supporting testers based on their capabilities and limitations. Second, I focus on the development of AI-based personalized learning tools and games that provide testers opportunities to enhance their skills and improve their testing and debugging capabilities. Personalization in training is essential to ensuring that the individual needs of each tester are addressed.

Key Publications:

- Riddhi More and Jeremy S. Bradbury. An analysis of LLM fine-tuning and few-shot learning for flaky test detection and classification. Submitted to international conference, Sept. 2024.

- Michael A. Miljanovic, Jeremy S. Bradbury. "Engineering Adaptive Serious Games Using Machine Learning." in Software Engineering for Games in Serious Contexts – Theories, Methods, Tools, and Experiences, 2023, 17 pages.

- Jude Arokiam, Jeremy S. Bradbury. "Automatically Predicting Bug Severity Early in the Development Process," Proc. of the 42nd International Conference on Software Engineering (ICSE 2020), The New Ideas and Emerging Results (NIER) track, Seoul, South Korea, Oct. 2020.

- Michael A. Miljanovic, Jeremy S. Bradbury. "GidgetML: An Adaptive Serious Game for Enhancing First Year Programming Labs," Proc. of the 42nd International Conference on Software Engineering (ICSE 2020), The Software Engineering Education and Training (SEET) track, Seoul, South Korea, Oct. 2020.

- David Kelk, Kevin Jalbert, Jeremy S. Bradbury. "Automatically Repairing Concurrency Bugs with ARC," Proc. of the 1st International Conference on Multicore Software Engineering, Performance, and Tools (MUSEPAT 2013), pages 73-84, Saint Petersburg, Russia, Aug. 2013.

Jia Li

Professor, Mitch & Leslie Frazer Faculty of Education, Ontario Tech University

Dr. Jia Li is a Professor (full) at the Mitch & Leslie Frazer Faculty of Education, Ontario Tech University. She is Chairperson of Publications for the Canadian Association for Curriculum Studies (CACS) and serves for Editorial Advisory Board of the Canadian Journal of Education (CJE)/La Revue canadienne de l'éducation (RCE). She received her doctoral degree from Ontario Institute for Studies in Education, University of Toronto and conducted her post-doctoral research work at Queen's University. She was a Canada-U.S. Fulbright Scholar at the Harvard Graduate School of Education (2011-2012), and a John A. Sproul Research Fellow at the University of California, Berkeley (2018-2019). Her teaching and professional experience include instructional design and assessment of technology-assisted educational interventions using both quantitative and qualitative methods.

Dr. Li's research agenda focuses on an interdisciplinary approach to address challenge areas in education by leveraging cutting edge technologies, data-driven innovative language and literacy interventions. This include using AI to support the development of academic reading and writing skills for linguistically diverse students. These include diverse urban students from low-income families, university English language learners and Indigenous youth. Her research has been funded by the Social Sciences and Humanities Research Council of Canada and Fulbright Canada. The results of her work have been published in high impact journals including Computers & Education, Teaching and Teacher Education, Language Learning & Technology, and Computer Assisted Language Learning.

Dr. Li is an invited reviewer for over 30 refereed journals, of which many reported high Impact Factors. These include the top 3 journals in education and technology, the top 2 journals in technology assisted language learning, the top 1 journal in teacher education, and a top 3 journal in education

First AI-related manuscript in progress aiming to a high impact peer-reviewed journal.

Justin Rawlins

Academic Associate, Communication and Digital Media Studies

Justin Owen Rawlins is the author of Imagining the Method (University of Texas Press, 2024). His work has also appeared in Journal of Film and Video, Velvet Light Trap, Celebrity Studies, Quarterly Review of Film and Video, as well as Journal of Cinema and Media Studies (forthcoming 2025). His new book, provisionally titled "Speculative Acting," will explore the use of AI to revivify deceased screen performers. This project examines how the rhetoric and self-positioning of the tech and finance firms at the heart of this rapidly materializing Hollywood-adjacent media production ecosystem carve out a distinct identity that resides at the uneasy intersection of the film, tech, and finance industries.

Key Publications:

- Imagining the Method: Reception, Identity, and American Screen Performance. (University of Texas Press, January 2024).

- "The Scandalous Speculative: Stardom and the AI-ification of Posthumous Performance." Celebrity Studies Conference, Amsterdam, Netherlands, July 2024. [Conference Presentation]

Kanika Samuels-Wortley

Associate Professor & Canada Research Chair, Faculty of Social Science and Humanities, Women in Research Council Chair

Before joining Ontario Tech University, Dr. Kanika Samuels-Wortley was an Assistant Professor in the Department of Criminology at Toronto Metropolitan University and the Institute of Criminology and Criminal Justice at Carleton University. Presently, she is a Visiting

Fellow at Australian National University at the School of Regulation and Global Governance (RegNet) in Canberra, Australia. Dr. Samuels-Wortley holds a Ph.D. in Sociology (2021) from the University of Waterloo, an MA and BA in Criminology from Ontario Tech and the University of Toronto, respectively.

Dr. Samuels-Wortley's research explores the intersection of race, racism, and the criminal justice system. Her research aims to advance critical race discourse in Canada through empirical mixed-methods approaches. Through the *Criminological Research Advancing Racial Equity Lab* (cRARE Lab), Dr. Samuels-Wortley and her team engage in research to better understand how bias and discrimination impact racialized peoples experiences and perceptions of the police, court, and correctional system. This includes an exploration into the use of predictive AI technologies within criminal justice processes and the role they play in exacerbating racial inequities in Canada.

Dr. Samuels-Wortley has published in prestigious peer reviewed journals, including Race and Justice, Crime and Delinquency, and the Canadian Journal of Criminology and Criminal Justice. Her research has been supported by a number of awards and grants, facilitating both international and national engagement, including a SSHRC Partnership Grant which involves a multi-disciplinary research team across several academic institutions in Canada. Dr. Samuels-Wortley has served as a member of the research committee for the Learning Advisory Committee on Diversity, Equity, and Inclusion for Correctional Service Canada, and is currently a research member with the Canadian Association of Chiefs of Police.

Key Publications:

- Harb, J., Anantharajah, K., Samuels-Wortley, K., Qureshi, N. (2024) Back at the Kitchen Table: Querying Feminist Support in the Academy. International Feminist Journal of Politics, 26(2), 427-446.

- Samuels-Wortley, K. (2024). Racialization and Crime. In N. Boyd (Ed.) Understanding Crime in Canada: An Introduction to Criminology, Third Edition. Emond Publishing.

- Samuels-Wortley, K. (2024) Community Policing, Police Militarization, and Canada's Colonial Project. In Sebastián Sclofsky and Analicia Mejia Mesinas (Eds.) In Police and State Crime in the Americas: Southern and Postcolonial Perspectives (pp. 99-122), New York, Palgrave Macmillan.

- Greene, C., Urbanik, M.-M., Samuels-Wortley, K. (2022). "It stays with you for life": The everyday nature and impact of police violence in Toronto's inner city. International Journal of Environmental Research and Public Health, Vol. 19, pg. 1-11.

- Samuels-Wortley, K (2022). Black on Blue, will not do: Navigating Canada's evidence-based policing community as a Black academic: A personal counter-story, in Derek

Silva and Mathieu Deflem (Eds.) Sociology of Crime, Law, and Deviance: Diversity in Criminology and Criminal Justice Studies, pg. 63-82. Emerald Publishing.

Karla Dhungana Sainju

Associate Professor, Criminology and Justice, Faculty of Social Science and Humanities, Women in Research Council Chair

One of my areas of expertise is bullying and my research related to this topic has examined various aspects including macro and micro-level influences of bullying, role of teachers and schools, xenophobic bullying, identity-based bullying, gender-based violence, and bullying discourse on social media. With support from grants through a SSHRC institutional small grant and a Mitacs Research Training grant, I've conducted studies where I merged social science and social media data and machine learning to provide an interdisciplinary approach to examine the old issue of bullying in a new way. While my work in the area of AI research is still in its infancy, my interests broadly is to explore how data sources such as Big Data and social media can address pressing societal questions using AI tools such as machine learning and quantitative and qualitative social science approaches. I am currently putting together proposals to examine the impact of hashtag feminism, especially as it relates to the #MeToo movement, and bullying and suicide-related discourse on social media. I hypothesize that this research will provide important implications for intervention, digital activism, social movements, and considerations of how to utilize social media for positive change. I am eager to engage and learn more about how my interests may align with and support the work of MAIRI.

Key Publications:

- Dhungana Sainju, K., Mishra, N., Kuffour, A., & Young, L. Bullying Discourse on Twitter: An Examination of Bully-Related Tweets Using Supervised Machine Learning. Computers in Human Behavior, 120, 106735. https://doi.org/10.1016/j.chb.2021.106735.

- Dhungana Sainju, K., Kuffour, A., Young, L., & Mishra, N. Bullying-Related Tweets: A Qualitative Examination of Perpetrators, Targets, and Helpers. International Journal of Bullying Prevention, 4(1), 6-22. Part of the special issue: The Use of Artificial Intelligence to Address Online Bullying and Abuse. https://doi.org/10.1007/s42380-021-00098-3

- Dhungana Sainju, K., Zaidi, H, Mishra. N., & Kuffour, A. Xenophobic Bullying & COVID-19: An Exploration Using Big Data & Qualitative Analysis. International Journal of Environmental Research and Public Health, 19(8), 4824. Part of the special issue:

Second Edition of Stigma, Health and Wellbeing. https://doi.org/10.3390/ijerph19084824

- Dhungana Sainju, K., Young, L., Kuffour, A., & Mishra, N. A Machine Learning and Qualitative Examination of Cyberbullying Experiences on Twitter. Journal of Social Media in Society, 11(2), 209-235.

Kathleen Pierce

Academic Associate, Faculty of Business and IT

I have a Bachelor of Arts in Business and Communication Arts from the University of Waterloo and a Master of Education in Adult Education and Community Development from OISE, University of Toronto. Since 2011, I've taught business and communication at various post-secondary institutions, focusing on effective teaching and business communication. In early 2023, I began researching generative AI to stay ahead of its impact on my students. I became fascinated with all things "Generative AI", and this led me to develop a program with the Continuing Education department called Generative AI for Business Leaders", which we delivered twice in 2024, with the next session planned for winter 2025. In addition, I've presented at two conferences on the topic of using AI in education ("Teaching professor conference" in New Orleans, 2023, and Ontario Tech's "AI in Education" conference, 2024).

Key Publication:

- Pierce, Kathleen. "Ai-Powered Personalized Feedback – Save Time & Spark Critical Minds." Artificial Intelligence in Education Conference Shaping Future Classrooms, Ontario Tech University, 29 May 2024, https://ecampusontario.pressbooks.pub/artificialintelligenceineducationconference/chapter/ai-powered-personalized-feedback-save-time-spark-critical-minds/

Ken Pu

Associate Professor, Computer Science, Faculty of Science

Dr. Ken Pu earned his PhD in Computer Science from the University of Toronto in 2006 and has been a faculty member at Ontario Tech University since 2007. His primary areas of expertise include big data, data lakes, novel data models, and query languages. He has worked in several areas: applying machine learning techniques to data lake management, developing search algorithms for internet-scale open data repositories, and exploring new approaches in time-series databases.

Recently, Dr. Pu's research has pivoted toward the intersection of machine learning and artificial intelligence within data management, focusing on how these technologies can enhance data processing and analysis. His current work emphasizes the development of data processing pipelines and the use of large language models to automate workflows as an effort to harness the power of AI to improve reliability and efficiency of modern workplace.

Key Publications:

- Ma, Limin, and Ken Q. Pu. "Accelerating Relational Keyword Queries With Embedded Predictive Neural Networks." 2024 IEEE International Conference on Information Reuse and Integration for Data Science (IRI). IEEE Computer Society, 2024.

- Wasti, Syed Mekael, Ken Q. Pu, and Ali Neshati. "Large Language User Interfaces: Voice Interactive User Interfaces powered by LLMs." Intelligent Systems Conference. Cham: Springer Nature Switzerland, 2024.

- Ma, Limin, and Ken Q. Pu. "Neural Network Accelerated Tuple Search For Relational Data." 2022 IEEE 23rd International Conference on Information Reuse and Integration for Data Science (IRI). IEEE, 2022.

- Nargesian, Fatemeh, Ken Pu, Bahar Ghadiri-Bashardoost, Erkang Zhu, and Renée J. Miller. "Data lake organization." IEEE Transactions on Knowledge and Data Engineering 35, no. 1 (2022): 237-250.

Khalid Elgazzar

Associate Professor, Canada Research Chair, Faculty of Engineering and Applied Science

Dr. Khalid Elgazzar is a Canada Research Chair and assistant professor with the Faculty of Engineering and Applied Science at Ontario Tech University, Canada and holds an adjunct assistant professor at Queen’s University where he also received his PhD degree in Computer Science from the School of Computing in 2013. He is the founder and director of the IoT Research Lab at Ontario Tech University. Prior to joining Ontario Tech, he worked at University of Louisiana at Lafayette and Carnegie Mellon School of Computer Science. Dr. Elgazzar named the recipient of the outstanding achievement in sponsored research award from UL Lafayette in 2017 and the distinguished research award from Queen's University in 2014. He also received several recognition and best paper award at top international venues. Dr. Elgazzar is world leader in the areas of Internet of Things (IoT), computer systems, real-time data analytics, and mobile computing. He is currently an associate editor for a number of IEEE/ACM journals and transactions in Peer-to-Peer Networking, Future Internet, Internet of Things and Mobile Computing. He also chaired a number of IEEE conferences and symposia on mobile computing, communications and IoT. Dr. Elgazzar is Senior IEEE Member and an active volunteer in technical program committees and organizing committees in both IEEE and ACM events.

Key Publications:

- Amr Zaki, Sara Elsayed, Khalid Elgazzar, Hossam Hassanien, “Quality and Budget-Oriented Task Offloading for Vehicular Cooperative Perception Using Reinforcement Learning”, IEEE Journal of Internet of Things, 2024.

- Amr Zaki, Sara Elsayed, Khalid Elgazzar, Hossam Hassanien, “Quality-Aware Task Offloading for Cooperative Perception in Vehicular Edge Computing”, IEEE Transactions on Vehicular Technology, 2024.

- Ahmed Elgazwy, Somayya Elmoghazy, Khalid Elgazzar, Alaa Khamis, “Pedestrian Crossing In- tent Prediction using Vision Transformers”, The 27th IEEE International Conference on Intelligent Transportation Systems (ITSC), Edmonton, Canada, September 24 - 27, 2024.

- Abeer Badawi, Ahmed Badr, Somayya Elmoghazy, Sara Elgazzar, and Khalid Elgazzar, Amer Burhan, “A Real-Time System for Monitoring and Managing Neuropsychiatric Symptoms in Dementia Patients” The 6th International Conference on Communications, Signal Processing, and their Applications, ISTANBUL, Turkey, 8-11 July 2024.

- Dipkumar Patel, Khalid Elgazzar, “Deep Learning Based Road Boundary Detection Using Camera and Automotive Radar”, The 35th IEEE Intelligent Vehicles Symposium (IV) (IEEE IV 2024), Jeju Island, Korea, June 2-5, 2024.

Langis Roy

Professor, Electrical, Computer and Software Engineering,
Faculty of Engineering and Applied Science

Has co-authored over 100 scientific papers and holds three patents on RF system-on-package designs. His current research interests include microwave electronics, integrated active antennas, reconfigurable microwave components, wireless sensors, high-performance electronic circuit packaging, and aerospace/automotive applications, now extending to terahertz biosensing and wireless power harvesting.

Laura Morrison

Assistant Professor, Faculty of Education

Dr. Laura Morrison is an Assistant Professor in the Learning Sciences within the Faculty of Education at Ontario Tech University. Her research focuses on innovative education and emerging technologies, with expertise in critical digital literacies, promising practices for online and hyflex teaching and learning and making as a pedagogical approach for inclusive education. Her current research is investigating AI literacy and ethics in education. Dr. Morrison is a prolific scholar who has published extensively and presented her research at over 30 national and international conferences, and she is co-editor of the Journal of Digital Life and Learning.

Key Publications:

- Morrison, L., Hughes, J., & Craig, C. (2024). Evaluating A.I. tools for use in education: A rubric for teachers and students. Proceedings of AI in Education Conference, 2024. https://ecampusontario.pressbooks.pub/artificialintelligenceineducationconference/

- Hughes, J., & Morrison, L. (2024). A brave new world: The perils of A.I. image generators for women. Proceedings of AI in Education Conference, 2024. https://ecampusontario.pressbooks.pub/artificialintelligenceineducationconference/

- Morrison, L., Hughes, J., & Craig, C. (Accepted). A.I. in education: An ethical framework and rubric in action. The South East Asian Conference on Education 2025, Kuala Lumpur.

- Butler-Ulrich, T., Hughes, J., & Morrison, L. (Accepted). The impact of generative AI on student creativity and well-being. ITAR Conference November 2024, Costa Rica.

- Morrison, L., Hughes, J., & Craig, C. (Submitted). A.I. in education: An ethical framework and rubric in action. International Journal of Artificial Intelligence in Education.

Li Yang

Assistant Professor, Faculty of Business and IT

Li Yang is an Assistant Professor in the Faculty of Business and Information Technology at Ontario Tech University. He received his Ph.D. in Electrical and Computer Engineering from Western University in 2022. He was the vice chair of the IEEE Computer Society, London Section, Canada, from 2022 to 2023. He was also on the technical program committee for

IEEE GlobeCom 2023 and 2024, the workshop chair for SMC-IoT 2023, and the technical session chair for IEEE CCECE 2020. His papers and code publications related to AI have received more than three thousand citations and GitHub stars. Li Yang's research focuses on applying AI and machine learning to cybersecurity, with a particular emphasis on intrusion detection and anomaly detection in 5G/6G networks and IoT systems. This involves the development of optimized and Automated ML (AutoML), concept drift adaptation, online learning, and continual learning techniques to enhance cybersecurity measures. Additionally, his work extends to the realms of trustworthy AI and AI security, specifically addressing adversarial machine learning attacks and defense strategies. Li Yang is also included in Stanford University/Elsevier's List of the World's Top 2% Scientists. He was ranked among the world's Top 0.5% of researchers in 'Networking & Telecommunications' in 2024, and 52nd in Canada.

Key Publications:

- L. Yang and A. Shami, "On hyperparameter optimization of machine learning algorithms: Theory and practice," Neurocomputing, vol. 415, pp. 295–316, 2020, doi: 10.1016/j.neucom.2020.07.061.

- L. Yang, A. Moubayed, I. Hamieh, and A. Shami, "Tree-Based Intelligent Intrusion Detection System in Internet of Vehicles," in 2019 IEEE Global Communications Conference (GLOBECOM), 2019, pp. 1–6. doi: 10.1109/GLOBECOM38437.2019.9013892.

- L. Yang and A. Shami, "A Lightweight Concept Drift Detection and Adaptation Framework for IoT Data Streams," IEEE Internet of Things Magazine, vol. 4, no. 2, pp. 96–101, 2021, doi: 10.1109/IOTM.0001.2100012.

- L. Yang and A. Shami, "A Transfer Learning and Optimized CNN Based Intrusion Detection System for Internet of Vehicles," in 2022 IEEE International Conference on Communications (ICC), 2022, pp. 1–6. doi: 10.1109/ICC45855.2022.9838780.

- L. Yang and A. Shami, "IoT Data Analytics in Dynamic Environments: From An Automated Machine Learning Perspective," Engineering Applications of Artificial Intelligence, vol. 116, pp. 1–33, 2022, doi: 10.1016/j.engappai.2022.105366.

Mariana Shimabukuro

Associate Teaching Professor, Computer Science, Faculty of Science

Mariana Shimabukuro (she/her) is an Associate Teaching Professor in the Faculty of Science and a Ph.D. candidate at Ontario Tech University; her current research is related to creating learner-centred foreign language learning applications leveraging generative AI, NLP, and other data-driven resources. She has been supervised by Dr. Christopher Collins since 2015 when she started her M.Sc. degree (2017). Her research interests include language learning, data visualization, HCI, recommendation systems, robotics and education.

Key Publications:

- Panchal, D., Collins, C., & Shimabukuro, M. (2024, October). LingoComics: Co-Authoring Comic Style AI-Empowered Stories for Language Learning Immersion with Story Designer. In Adjunct Proceedings of the 37th Annual ACM Symposium on User Interface Software and Technology (pp. 1-3).

- Leung, B., Shimabukuro, M., & Collins, C. (2024, October). NeuroSight: Combining Eye-Tracking and Brain-Computer Interfaces for Context-Aware Hand-Free Camera Interaction. In Adjunct Proceedings of the 37th Annual ACM Symposium on User Interface Software and Technology (pp. 1-3).

Matthew Shane

Associate Professor, Psychology, Faculty of Social Science and Humanities

I am an Associate Professor of Psychology and Director of the Clinical Affective Neuroscience Laboratory at Ontario Tech University, where I have held a tenure-track position since January 2013. Prior to that, I held a non-tenure track Research Associate position at The Mind Research Network in Albuquerque, New Mexico, where I undertook cutting-edge psychologically and neuroscience-based research focused on socioemotional processing in healthy and offender populations.

Across both institutions, I have established and maintained several strong programs of research, utilizing both psychological and neuroscientific methods, dedicated to the study of emotional and cognitive processing in healthy and antisocial populations. Main areas of interest include the detrimental consequences of an avoidant coping style, and the emotional deficits seen within individuals with heightened psychopathic traits.

To support this work, I have received over five million dollars in competitive research funding, including funding for several large-scale NIH- (1 RO1; 3 R21s) and tri-council-(2 SSHRC IDG; 1 NSERC Discovery Grant) sponsored projects. I currently hold a SSHRC IDG and an an NSERC Discovery Grant, and was primary applicant on a successful CFI-JELF awarded in the spring of 2023.

In total, these projects has led to 31 peer-reviewed publications in high-tier academic journals, 2 book chapters, several preprints, and over 80 conference abstracts/presentations.

This work has been fortunate enough to have received considerable attention from both academic colleagues (amassing a total of 3022 academic citations) and the popular media (e.g. the New York Times, the Discovery Channel). Moving forward, I plan to increasingly incorporate AI into the research workflow, to facilitate the research process, and to further elucidate the neural features underlying healthy and problematic emotional processing.

Key Publication:

- Shane MS, Denomme WJ. Machine learning approaches for parsing comorbidity/heterogeneity in antisociality and substance use disorders: A primer. Personality Neuroscience. 2021;4:e6. doi:10.1017/pen.2021.2

Meaghan Charest-Finn

Assistant Professor, Automotive and Mechatronics Engineering,
Faculty of Engineering and Applied Science.

Dr. Meaghan Charest-Finn is an assistant professor in the Faculty of Engineering and Applied Science Department of Automotive and Mechatronics Engineering at Ontario Tech University. She teaches Industrial Automation, Machine learning, and Artificial Intelligence, among other courses. Her research focuses on developing advanced automation methods to control complex systems effectively. She has worked on integrating Model Predictive Controls and Machine learning schemes into the modelling and control of real-world systems.

Key Publications:

- M. Charest-Finn and R. Dubay, “General Industrial Process Optimization Method to Leverage Machine Learning Applied to Injection Moulding”, Expert Systems, e13769, Oct. 2024, doi: 10.1111/exsy.13769

- S. Mohsini, D. Landori-Hoffmann, A. K. Komarsofla, M. Charest-Finn and R. Dubay, “ Control of a Self Balancing Bicycle Robot using PID control tuned with linear Regression”, the Canadian Society for Mechanical Engineering International Congress (CSME), Toronto, Canada, May 2024

- A. K.Komarsofla, M. Charest-Finn, S. Nokleby. (2023). Autonomous Inspection of Steel Pipe Weld Lines Implementing Frequency Analysis Combined with YOLOv5. CSME-2023. Canadian Society Mechanical Engineering (CSME), Sherbrook, Canada, 2023

- M. Charest, R. Finn, and R. Dubay, “Integration of artificial intelligence in an injection molding process for on-line process parameter adjustment,” in 2018 Annual IEEE International Systems Conference (SysCon), Apr. 2018, pp. 1–6.

Michael Bliemel

Professor of Information Systems, Faculty of Business and IT

Dr. Bliemel has had diverse interdisciplinary research experience around the impacts of new technologies, data literacy, business analytics, e-health, problem gambling, gamification in education, information systems, e-commerce, NeuroIS and human computer interaction. His current interests are in the strategic management of information technology, the innovation and adoption of emerging technology in business. He explores these topics at different levels, ranging from firm performance to task performance and individual usability perspectives.

Dr. Bliemel has been recognized with several awards for university teaching and for academic leadership. He works closely with leading companies and industry organizations to build connections between academia, business and government around the topics of analytics, digital literacy and digital transformation. Dr. Bliemel has also taught professors and professionals analytics and has coached several winning student teams in local, provincial and global analytics competitions.

Key Publications:

- V. Pandeliev, A. A. Namanloo, K. Lyons, M. Bliemel and H. Ali-Hassan, "A Serious Game for Teaching Data Literacy," 2022 IEEE Games, Entertainment, Media Conference (GEM), St. Michael, Barbados, 2022, pp. 1-6, doi: 10.1109/GEM56474.2022.10017613.

- Pierre-Majorique Léger, Jean-François Plante, Jean-François Michon, Forough Karimi-Alaghehband, Michael Bliemel, and Marc Fredette, “EDGE: A Simulation Game to Change How We Teach and Learn Analytics”, Prototype at 2018 Pre-ICIS SIGDSA Symposium, San Francisco, December 13th, 2018

- Alex McLeod Jr., Michael Bliemel, and Nancy Jones, “Examining the Adoption of Big Data and Analytics Curriculum”, Business Process Management Journal, Vol. 23 Issue: 3, 2017, pp. 506-517

- SHRC Knowledge Synthesis Report with Mike Smit, Hossam Ali-Hassan, Michael Bliemel, Dean Irvine, Daniel Kelley, Stan Matwin, and Brad Wuetherick, “Strategies and Best Practices for Data Literacy Education”, 2015

- Michael Bliemel and Kristof Schneider, “Introduction to next generation Business Intelligence with Automated Analytics Mode in SAP Predictive Analytics”, in Business Intelligence SAP University Alliances Faculty Community, April 2015

Michael Miljanovic

Assistant Teaching Professor, Faculty of Science

Dr. Michael Miljanovic is the Software Education Lead of the Software Engineering & Education Research (SEER) Lab at Ontario Tech University. His thesis focused on the application of machine learning to educational programming games for computer science, and was part of the SEER Lab's Serious Games for Computer Science Project. His research interests include pedagogical techniques, serious games, and adaptive learning tools.

Key Publications:

- Miljanovic, Michael A., and Jeremy S. Bradbury. "Engineering Adaptive Serious Games Using Machine Learning." Software Engineering for Games in Serious Contexts: Theories, Methods, Tools, and Experiences. Cham: Springer Nature Switzerland, 2023. 117-134.

- Miljanovic, Michael A. Adaptive serious games for computer science education. Diss. University of Ontario Institute of Technology, 2020.

- Miljanovic, Michael A., and Jeremy S. Bradbury. "GidgetML: An adaptive serious game for enhancing first year programming labs." Proceedings of the ACM/IEEE 42nd International Conference on Software Engineering: Software Engineering Education and Training. 2020.

- Miljanovic, Michael Alexander. "Enhancing computer science education with adaptive serious games." Proceedings of the 2019 ACM Conference on International Computing Education Research. 2019.

- Miljanovic, Michael A., and Jeremy S. Bradbury. "Making serious programming games adaptive." Joint International Conference on Serious Games. Cham: Springer International Publishing, 2018.

Miguel Vargas Martin

Professor, Faculty of Business and IT

Dr. Miguel Vargas Martin is Professor in Computer Science at Ontario Tech University. PhD (Computer Science) from Carleton University, Master's degree (Electrical Engineering) from CINVESTAV del IPN, and Bachelor of Science (Computer Science) from UAA. Licenced Professional Engineer in the Province of Ontario. His research area include AI-assisted computer and systems security, natural language processing, companion robots.

Key Publications:

- Reyes-Acosta, R., Dominguez-Baez, C., Mendoza-Gonzalez, R., & Vargas Martin, M. (2024). Analysis of machine learning-based approaches for securing the Internet of Things in the Smart Industry: A state of knowledge review. International Journal of Information Security. To appear.

- Nimmagadda, R., Arora, K., & Vargas Martin, M. (2022). Emotion recognition models for companion robots. The Journal of Supercomputing, 1–18.

- Maraj, A., Vargas Martin, M., & Makrehchi, M. (2024). Words that stick: Using keyword cohesion to improve text segmentation. In Conference on computational natural language learning (CoNLL 2024), Miami, USA: Association for Computational Linguistics.

- Mithila, M., Yu, F., Vargas Martin, M., & Wang, S. (2024). Visualizing differential privacy: Assessing infographics' impact on layperson data-sharing decisions and comprehension. In Conference on Privacy, Security, and Trust (PST). IEEE.

- Maraj, A., Vargas Martin, M., & Makrehchi, M. (2024). Coherence graphs: Bridging the gap in text segmentation with unsupervised learning. In Conference on natural language & information systems (NLDB), Turin, Italy: Springer.

Min Dong

Professor, Electrical, Computer and Software Engineering,
Faculty of Engineering and Applied Science

Min Dong received a Ph.D. degree in Electrical and Computer Engineering with a minor in Applied Mathematics from Cornell University, Ithaca, New York, in 2004 and a B.Eng. degree from Tsinghua University, Beijing, China, in 1998. From 2004 to 2008, she was with Corporate Research & Development at Qualcomm Research, Qualcomm Inc., San Diego, CA. Since 2008, she has been with the Faculty of Engineering and Applied Science at Ontario Tech University, where she is currently a Professor in the Department of Electrical, Computer and Software Engineering. She served as the Associate Dean (Academic) of the Faculty of Engineering and Applied Science from January 2017 to June 2017 (interim) and during 2021 and 2022. She also holds a status-only Professor appointment in the Department of Electrical and Computer Engineering at the University of Toronto.

Prof. Dong is an IEEE Fellow. She received the Early Researcher Award from the Ontario Ministry of Research and Innovation in 2012, the Best Paper Award at IEEE ICCC 2012, and the 2004 Best Paper Award from the IEEE Signal Processing Society (Transactions). She is also a co-author of The Best Student Paper at IEEE SPAWC 2021 and the Best Student Paper of Signal Processing for Communications and Networks at IEEE ICASSP 2016. She is a recipient of the NSERC Discovery Accelerator Supplement (DAS award) in 2019.

Key Publications:

- J. Wang, B. Liang, M. Dong, G. Boudreau, and H. Abou-Zeid, “Joint online optimization of model training and analog aggregation for wireless edge learning,” IEEE/ACM Transactions on Networking, vol. 32, pp. 1212-1228, April 2024

- F. Moradi Kalarde, M. Dong, B. Liang, Y. Ahmed, H.T. Cheng, "Beamforming and device selection design in federated learning with over-the-air aggregation," IEEE Open Journal of the Communications Society, vol. 5, pp. 1710-1723, March 2024.

- C. Zhang, M. Dong, B. Liang, A. Afana, Y. Ahmed, “Multi-model wireless federated learning with downlink beamforming,” in Proc. of IEEE International Conference on Acoustics Speech and Signal Processing (ICASSP), April 2024

- C. Zhang, M. Dong, B. Liang, A. Afana, and Y. Ahmed, “Joint downlink-uplink beamforming for wireless multi-antenna federated learning,” in the 21st International Symposium on Modeling and Optimization in Mobile, Ad Hoc and Wireless Networks (WiOpt), August 2023.

- S. Kiani, M. Dong, S. ShahbazPanahi, G. Boudreau, and M. Bavand, "Learning-based user clustering in NOMA-aided MIMO networks with spatially correlated channels," IEEE Transactions on Communications, vol. 70, no. 7, pp. 4807-4821, July 2022.

Pariss Garramone

Associate Teaching Professor and Undergraduate Program Director of Liberal Studies, Faculty of Social Science and Humanities

Dr. Pariss Garramone, PhD, is an Associate Professor of Teaching and the Undergraduate Program Director of Liberal Studies at Ontario Tech University. Dr. Garramone is an active board member of the Oshawa Culture Leadership Council and has helped to facilitate approaches for land-based slow pedagogy for teaching and learning about local heritage and digital archival research for students. Currently, her research focuses on assessing the implementation of scaffolded AI literacy for composition classes and equity-focused community building for online learning.

Key Publication:

- King, A. & Garramone, P. (forthcoming, December 2024). Teaching writing in the time of ChatGPT: Rethinking what counts as learning. Artificial Intelligence, Assessments and Academic Integrity. Springer Publishing.

Patrick Hung

Professor, Faculty of Business and IT

Patrick C. K. Hung is a Professor at Ontario Tech University, Faculty of Business and Information Technology. He is a Leverhulme Visiting Professor at Aston University, England, and an Honorable Guest Professor at Shizuoka University, Hamamatsu, Japan. He was also a Distinguished Visiting Fellow at Abertay University, Scotland, and a Visiting Researcher at the University of São Paulo, Brazil. Dr. Hung worked with Boeing Research and Technology in Seattle on aviation services-related research with two U.S. patents on the mobile network dynamic workflow system. Before that, he was a Research Scientist with Australia's Commonwealth Scientific and Industrial Research Organization. He is a founding member of the IEEE Technical Committee on Services Computing and IEEE Transactions on Services Computing. In addition, he is an editorial board member for the IEEE Transactions on Engineering Management and a coordinating editor of the Information Systems Frontiers.

Key Publications:

- Bonfim Pita, M. A., Fantinato, M., and Hung, P. C. K. (2025). SeniorMedManagement: Assistive Solution to Help Older Adults Manage Treatment Using Social Robots and Virtual Assistants, The 58th Hawaii International Conference on System Sciences (HICSS-58), Big Island, Hawaii, United States of America, 10 Pages.

- Tashiro, J. S. and Hung, P. C. K. (2024). Complexities of Using Large Language Model Generative AI in Health Education and Robots, The 17th International Conference on Blended Learning, Macao SAR, China, Springer’s Lecture Notes in Computer Science Series, Page(s): 77-89.

- Liu, Y.-H., Hung, P. C. K., Iqbal, F., and Fung, B. C. M. (2021). Automatic Fall Risk Detection Based on Imbalanced Data, IEEE ACCESS, Vol. 9, Page(s): 163594-163611.

Peter Lewis

Associate Professor & Canada Research Chair, Faculty of Business and IT

Dr. Peter Lewis holds a Canada Research Chair in Trustworthy Artificial Intelligence (AI), at Ontario Tech University, Canada, where he is an Associate Professor and Director of the Trustworthy AI Lab. Peter’s research advances both foundational and applied aspects of AI and draws on extensive experience applying AI commercially and in the non-profit sector. He is interested in where AI meets society, and how to help that relationship work well. His current research is concerned with challenges of trust, bias, and accessibility in AI, as well as how to create more socially intelligent AI systems, such that they work well as part of society, explicitly taking into account human factors such as norms, values, social action, and trust.

He is Associate Editor of IEEE Transactions on Technology & Society, IEEE Technology & Society Magazine (TSM) and ACM Transactions on Autonomous and Adaptive Systems (TAAS), a board member of the International Society for Artificial Life (ISAL) with responsibility for Social Impact, and Co-Chair of the Steering Committee for the IEEE International Conference on Autonomic and Self-organizing Systems (ACSOS). He has published over 100 papers in academic journals and conference proceedings, as well as the foundational book Self-aware Computing Systems: An Engineering Approach, in 2016. He has a PhD in Computer Science from the University of Birmingham, UK.

Key Publications:

- Peter R. Lewis and Stefan Sarkadi. Reflective Artificial Intelligence. Minds and Machines, 34:1–30, 2024.

- Peter R. Lewis and Stephen Marsh. What is it like to trust a rock? A functionalist perspective on trust and trustworthiness in Artificial Intelligence. Cognitive Systems Research, 72:33–49, 2022.

- Chloe M. Barnes, Abida Ghouri, and Peter R. Lewis. Explaining evolutionary agent-based models via principled simplification. Artificial Life, 27(3), 2021.

- Simon T. Powers, Anikó Ekárt, and Peter R. Lewis. Modelling enduring institutions: The complementarity of evolutionary and agent-based approaches. Cognitive Systems Research, 52:67–81, 2018.

- Peter R. Lewis, Arjun Chandra, Funmilade Faniyi, Kyrre Glette, Tao Chen, Rami Bahsoon, Jim Torresen, and Xin Yao. Architectural aspects of self-aware and self-expressive computing systems. IEEE Computer, 48:62–70, 2015.

Pierre Côté

Professor & Director, Institute for Disability and Rehabilitation Research,
Faculty of Health Sciences

Dr. Côté is a professor and epidemiologist in the Faculty of Health Sciences at Ontario Tech University. He holds the Hann-Kelly Family Chair in Disability and Rehabilitation Research and the Ontario Tech University Research Excellence Chair in Musculoskeletal Rehabilitation. He held the Canada Research Chair in Disability Prevention and Rehabilitation from 2013-2023. His clinical training was in the field of chiropractic, he completed his Master of Science degree in Surgery from the University of Saskatchewan and his PhD in Epidemiology from the University of Toronto. Dr. Côté is the Director of the Institute for Disability Prevention and Rehabilitation (IDRR) at Ontario Tech University, Director of the World Health Organization (WHO) Collaborating Center on Rehabilitation and Musculoskeletal Health and Chair of the IDRR unit of the Cochrane Collaboration Thematic Group – Functioning, Disability and Rehabilitation. Côté is also appointed as a Professor of Epidemiology at the Dalla Lana School of Public Health, University of Toronto; Adjunct Professor of Disability Prevention at Southern Denmark University; and as Honorary Professor, School of Physiotherapy, MGM Institute of Health Sciences, Navi Mumbai, India. His current research focuses on understanding “who” could benefit from rehabilitation and “what” rehabilitation interventions are effective for individuals with musculoskeletal conditions. Professor Côté has published more than 400 scientific papers in peer-reviewed journals.

Pooria Madani

Assistant Professor, Faculty of Business and IT

Dr. Pooria Madani is an Assistant Professor at Ontario Tech University, with research in adversarial machine learning and cybersecurity funded by prominent agencies, including NSERC and NCC. His work sits at the intersection of machine learning and cybersecurity, focusing on emerging threats in connected and automated vehicles, IoT, and aerospace systems. Dr. Madani collaborates with industry partners on projects such as securing satellite communication networks and enhancing IoT cybersecurity to strengthen defenses against evolving cyber threats. He holds a Ph.D. in Computer Science from York University (2021), an M.Sc. in Computer Science from the University of New Brunswick (2015), and a B.Sc. (Honours) in Computer Science from the University of Prince Edward Island (2012).

Key Publications:

- Bakos, Steve, Pooria Madani, and Heidar Davoudi. "Noise as a Double-Edged Sword: Reinforcement Learning Exploits Randomized Defenses in Neural Networks." arXiv preprint arXiv:2410.23870 (2024).
- Setak, Mohammad, and Pooria Madani. "Fine-Tuning LLMs for Code Mutation: A New Era of Cyber Threats." arXiv preprint arXiv:2410.22293 (2024).
- Madani, Pooria. "Metamorphic malware evolution: The potential and peril of large language models." 2023 5th IEEE International Conference on Trust, Privacy and Security in Intelligent Systems and Applications (TPS-ISA). IEEE, 2023.
- Madani, Pooria, Natalija Vlajic, and Ivo Maljevic. "Randomized moving target approach for MAC-layer spoofing detection and prevention in IoT systems." Digital Threats: Research and Practice 3.4 (2022): 1-24.
- Madani, Pooria, and Natalija Vlajic. "Robustness of deep autoencoder in intrusion detection under adversarial contamination." Proceedings of the 5th Annual Symposium and Bootcamp on Hot Topics in the Science of Security. 2018.

Qusay Mahmoud

Professor of Software Engineering, Faculty of Engineering and Applied Science

My current research centers on (1) developing middleware for intelligent software systems, aimed at creating a secure, adaptable, and responsive layer that can support the demands of complex systems. As software systems continue to proliferate—ranging from smart cities and healthcare devices to industrial automation—these systems require middleware that can manage vast, heterogeneous data streams in real time, applying intelligent filtering, processing, and decision-making to ensure both functionality and security. My work leverages artificial intelligence within middleware architecture to address unique challenges, such as scalability, data integrity, privacy, and resilience to cyber-attacks; and (2) integrating AI into engineering education, exploring ways in which AI can support student learning and promote critical thinking in technical fields.

Key Publications:

- P Sarzaeim, QH Mahmoud, A Azim, A Framework for LLM-Assisted Smart Policing System, IEEE Access, 2024

- P Sarzaeim, QH Mahmoud, A Azim, Experimental Analysis of Large Language Models in Crime Classification and Prediction, Proceedings of the Canadian Conference on Artificial Intelligence, 2024.V Gharavian, et al.,

- Intrusion Detection for Wireless Sensor Network Using Graph Neural Networks, 2023 IEEE Symposium Series on Computational Intelligence (SSCI), 807-813

- A Avan, F Kheiri, QH Mahmoud, A Azim, M Makrehchi, S Rahnamayan, A Task Scheduler for Mobile Edge Computing Using Priority-based Reinforcement Learning, 2023 IEEE Symposium Series on Computational Intelligence (SSCI), 539-546

- M Lescisin, QH Mahmoud, Design and Development of Policy Enforcement for the Privacy by Design Framework, 2023 20th ACS/IEEE International Conference on Computer Systems and Applications (AICCSA)

  And I maintain this blog: https://DrQWrites.com

Rajen Akalu

Associate Professor, Faculty of Business and IT

Rajen Akalu is an associate professor in the Faculty of Business and IT at Ontario Technology University in Oshawa. He is also the founder of the Akalu Law Professional Corporation www.akalulaw.com. His law firm provides legal services to individual and corporate clients on issues relating to information governance, privacy compliance, security policy, and starting a business. His research interests law firm practice areas relate to privacy law and artificial intelligence.

Key Publications:

- Curzon, J., Kosa, T. A., Akalu, R., & El-Khatib, K. (2021). Privacy and artificial intelligence. IEEE Transactions on Artificial Intelligence, 2(2), 96-108.

- Akalu, R. (2023). The Academic Vampire. Independently Published (Amazon)
  [Has a chapter on AI]

Robin Kay

Professor, Faculty of Education

Dr. Robin Kay is a Full Professor in the Faculty of Education at Ontario Tech University in Oshawa, Canada. Dr. Kay received his MA in Computer Applications in Education at the University of Toronto and his Ph.D. in Cognitive Science (Educational Psychology) at the University of Toronto. He has published over 200 articles, chapters, and conference papers in the area of pedagogy, education, and technology and has taught in the fields of computer science, mathematics, and educational technology for over 30 years at the high school, college, undergraduate and graduate level.

Current projects include research on AI in education, e-learning tools, online and blended learning in secondary and higher education, video podcasts, scale development, emotions and the use of computers, and factors that influence how students learn with technology

Robyn Ruttenberg-Rozen

Assistant Professor, Faculty of Education

Dr. Robyn Ruttenberg-Rozen is an inclusion scholar. Through her work she seeks to understand how historically marginalized STEM learners, leverage their agency and powers to learn, innovate, and make positive social change in the world. As an interdisciplinary scholar, she draws from the fields of disability, science and technology studies, mathematics education, inclusion, and gender studies. Since beginning her current role, Robyn has published 30 publications and has received over 1 million dollars of funding, including a prestigious NFRF grant as Nominated Principal Investigator. For this grant, Robyn is leading a team of interdisciplinary scholars from Canada the US and South Africa. In 2023 Robyn received a fully funded scholar in residence to Durban University of technology where she helped build research capacity in South African TVET colleges. Community is always at the center of Robyn's work, and aside from her international work, locally she has helped develop programming for the Ontario Science Centre, co-organized stakeholder events with Future Black Female, co-led workshops on belonging for Canadian mathematicians and educators, given numerous invited talks including on the future of AI in education at the Enoch Turner School house, and was invited to a give a presentation to the Special Committee on Social Policy about mathematics education at the Legislative Assembly of Ontario. Robyn is passionate about teaching and mentoring. In 2020 she received the Ontario Tech 2020 Early Career Teaching Award and in 2022 she received the Tim McTiernan Mentorship Award. In 2023 she was the faculty nominee for the Teaching Excellence Award. In 2024 Robyn received the Ontario Tech Excellence in Research Award in the category of Emerging Scholar.

Salma Karray

Professor and Research Excellence Chair, Faculty of Business and IT

Dr. Salma Karray is the Research Excellence Chair in Marketing Analytics and Decision Models and Professor at the Faculty of Business and Information Technology. She uses optimization, data analytics, and AI techniques to help businesses improve their performance and strive to be competitive. Applications of her work include digital advertising, pricing, retailing, loyalty program management, CRM, and e-commerce.

Dr. Karray works with students and colleagues at Ontario Tech in the Business Analytics and AI lab, the Modeling and Computational Science program (C.L.A.I.M lab), and the Computer Science program at the Faculty of Science. She has also collaborated with students at the University of Waterloo and Toronto Metropolitan University, where she holds adjunct positions.

Key Publications:

- Maarfavi N and Karray, S. (2024). Predicting user engagement toward movie trailers using applications of AI tools. AIMS conference, June 2024.

- Machado, M. and Karray, S. (2022). Assessing credit risk of commercial customers using hybrid machine learning algorithms. Expert Systems with Applications. 200: 116889.

- Machado, M. and Karray, S. (2022). Applying hybrid machine learning algorithms to assess customer risk-adjusted revenue in the financial industry. Electronic Commerce Research and Applications. 56: 101202.

- Marcos, M. and Karray, S. (2022). Integrating Customer Portfolio Theory and the Multiple Sources of Risk-Approaches to Model Risk-Adjusted Revenue. 18th IFAC Workshop on Control Applications of Optimization CAO 2022, France.

- Machado, M., Karray, S. and de Souza, I T. (2019). LightGBM: an Effective Decision Tree Gradient Boosting Method to Predict Customer Loyalty in the Finance Industry. IEEE ICCSE 2019 conference proceeding. IEEE ICCSE 2019, Toronto, Canada.

Sanaa Alwidian

Assistant Professor of Software Engineering, Faculty of Engineering and Applied Science

Dr. Sanaa Alwidian is an assistant professor of software engineering at the Department of Electrical, Computer, and Software Engineering at Ontario Tech University, and the director of the Requirements and Software Engineering Advanced Research (ReSEARch) Lab. Her research focus is on requirements engineering (RE), human-centric software engineering, and AI-enabled solutions for requirements and software engineering. Her background in applying AI and machine learning-enabled solutions to complex software problems ensures the integration of advanced, scalable techniques that enhance the system's resilience to evolving requirements and constraints. By focusing on both technical and human-centric requirements, Dr. Alwidian contributes meaningfully to the development of reliable, efficient and high-performance systems. Her work has been published in top peer-reviewed journals and conferences.

Prior to joining Ontario Tech, Dr. Alwidian worked as a Postdoctoral Research Fellow with the GEODES Software Engineering Research Lab at the Université de Montréal. She conducted research on the intersection of AI and Software Engineering, where she investigated research opportunities about the application of Model Driven Software Engineering abstractions, methodologies, and technologies to the AI embedded systems. To achieve this, she collaborated with the National Bank of Canada (NBC) on a project titled "Performance Management of AI Initiatives". The purpose of this project was to monitor the performance of the deployment of AI initiatives in the NBC's business processes in order to monitor the quality of decision-making processes and to achieve an optimal allocation of resources. From 2015 to 2020, she worked as research and a teaching assistant at the University of Ottawa, and as a researcher at the CyberJustice lab, where she contributed to the development of a framework to model and analyze sensitive data in jurisdiction systems in Canada, where most of these systems deployed AI systems. Dr. Alwidian has considerable teaching experience in several academic institutions across three countries. Sanaa holds a Ph.D. degree in Computer Science from the University of Ottawa, and she was the recipient of the prestigious Ontario Trillium Scholarship (OTS), awarded to the best international doctoral students from around the world (with a first-class average and excellent academic record). She has also received the International Ontario Graduate Scholarship (OGS), the University of Ottawa Excellence Scholarship, the International Doctoral Scholarship, the BMO Financial Group Scholarship, and the Scientific Research Scholarship/ Jordan.

Key Publications:

- Siddeshwar, V., Alwidian, S. and Makrehchi, M., 2024. A Systematic Review of AI-Enabled Frameworks in Requirements Elicitation. IEEE Access.

- Siddeshwar, V., Alwidian, S. and Makrehchi, M., 2024, September. A Comparative Study of Large Language Models for Goal Model Extraction. In Proceedings of the

ACM/IEEE 27th International Conference on Model Driven Engineering Languages and Systems (pp. 253-263).

- Siddeshwar, V., Alwidian, S. and Makrehchi, M., 2024, September. Goal Model Extraction from User Stories Using Large Language Models. In International Conference on the Quality of Information and Communications Technology (pp. 269-276). Cham: Springer Nature Switzerland.

- Zhao, W., Mahmoud, Q.H. and Alwidian, S., 2023. Evaluation of GAN-based model for adversarial training. Sensors, 23(5), p.2697.

- Zhao, W., Alwidian, S.A. and Mahmoud, Q.H., 2023, February. Evaluation of GAN Architectures for Adversarial Robustness of Convolution Classifier. In SafeAI@ AAAI.

Shahram S. Heydari

Professor, Faculty of Business and Information Technology

Shahram S. Heydari is a Professor with the Faculty of Business and Information Technology, University of Ontario Institute of Technology (Ontario Tech), Canada; and the Co-Director of Ontario Tech Advanced Networking Technology and Security Research Laboratory. Prior to joining Ontario Tech, he was a System Designer and a member of Scientific Staff with Nortel Networks, where he worked on element management in ultrahigh speed IP/MPLS routers, performance modeling of automatically switched optical networks (ASON), and proprietary voice-over-IP transport control protocols. His main research interests include network design and planning, software-defined networking, applications of artificial intelligence (AI) in network management, and network quality of experience (QoE). He received the B.Sc. and M.Sc. degrees in electronic engineering from Sharif University of Technology, Iran, the M.A.Sc. degree from Concordia University, Montreal, and the Ph.D. degree from the University of Ottawa, Canada.

Key Publications:

- Sabeel, Ulya, Shahram Shah Heydari, Khalil El-Khatib, and Khalid Elgazzar. "Unknown, Atypical and Polymorphic Network Intrusion Detection: A Systematic Survey." IEEE Transactions on Network and Service Management (2023).

- U. Sabeel, S. S. Heydari, H. Mohanka, Y. Bendhaou, K. Elgazzar and K. El-Khatib, "Evaluation of Deep Learning in Detecting Unknown Network Attacks," 2019 International Conference on Smart Applications, Communications and Networking (SmartNets), Sharm El Sheikh, Egypt, 2019.

- Chauhan, Ravi, and Shahram Shah Heydari. "Polymorphic Adversarial DDoS attack on IDS using GAN." 2020 International Symposium on Networks, Computers and Communications (ISNCC). IEEE, 2020.

- Hassan, Ali, and Shahram Shah Heydari. "Enterprise Application Outage Prediction Using XGBoost and LSTM." 2023 19th International Conference on Network and Service Management (CNSM). IEEE, 2023.

- Sabeel, U., Heydari, S.S., El-Khatib, K. and Elgazzar, K., 2024. Incremental Adversarial Learning for Polymorphic Attack Detection. IEEE Transactions on Machine Learning in Communications and Networking.

Stephen (Steve) Marsh

Professor, Faculty of Business and IT

Steve is a computational philosopher who thinks, writes and talks about social norms in sociotechnical environments. These include trust, distrust, untrust, forgiveness, wisdom, hope, and grace. He has published and presented about all of these topics. His seminal PhD thesis at the University of Stirling in Scotland introduced the concept of computational trust in 1994. He has been at Ontario Tech in the Faculty of Business and IT since 2012, prior to which he was a Research Scientist at the Communications Research Centre (Government of Canada) and before that a Research Officer at the National Research Council of Canada. He lives in Ontario with his family and other animals.

Key Publications:

- Lewis, P.R. & Marsh S., 2022. What is it like to trust a rock? A functionalist perspective on trust and trustworthiness in Artificial Intelligence. Cognitive Systems Research 72, 33-49.
  https://doi.org/10.1016/j.cogsys.2021.11.001

- Marsh, S., Atele-Williams, T., Basu, A., Dwyer, N., Lewis, P.R., Miller-Bakewell, H., Pitt, J., 2020. Thinking about Trust: People, Process, and Place. Patterns 1(3).
  https://doi.org/10.1016/j.patter.2020.100039

- Marsh, S., Briggs, P., El-Khatib, K., Esfandiari, B., Stewart, J., 2011. Defining and Investigating Device Comfort. Journal of Information Processing, June 2011. Information Processing Society of Japan. 19:231-252.
  http://www.jstage.jst.go.jp/article/ipsjjip/19/0/19_231/_article

- Marsh, S. and Briggs, P., 2009. Examining Trust, Regret and Forgiveness as Computational Concepts. Chapter 2 of Golbeck, J., Computing with Social Trust, Springer.

- Marsh, S., 2021. Trust Systems. Ecampus Ontario Open Educational Resource Textbook. https://ecampusontario.pressbooks.pub/trustsystems/

Stephen Jackson

Associate Professor, Faculty of Business and IT

I am an Associate Professor in Management Information Systems at Ontario Tech University, Faculty of Business and Information Technology. I have taught at various universities in the UK, including the University of London (Royal Holloway), and the University of Southampton. Before joining academia, I worked as an IT consultant for PricewaterhouseCoopers and was involved in various IT projects across different industry sectors in Europe and Asia. My research focuses on the social, behavioral, and cultural aspects of implementing and managing AI-based systems in organizations. I have published in international journals, including Information and Organization, Journal of the Association for Information Science and Technology, Computers in Human Behavior, Information Systems Frontiers, Studies in Higher Education, Behaviour and Information Technology, International Journal of Information Management, British Journal of Educational Technology, among others.

Key Publications:

- Jackson, S., & Panteli, N. (2024). AI-based digital assistants in the workplace: An idiomatic analysis. Communications of the Association for Information Systems, 55, pp-pp. Retrieved from https://aisel.aisnet.org/cais/vol55/iss1/22.

- Jackson, S. (2024). Understanding trust in workplace AI: A multi-stakeholder lens. Proceedings of the 30th Americas Conference on Information Systems, Salt Lake City, Utah, USA.

- Jackson, S. (2024). The Janus-faced nature of educational AI. The 8th International Conference on Advances in Artificial Intelligence, London, England.

- Jackson S., & Panteli, N. (2023). Trust or mistrust in algorithmic grading? An embedded agency perspective. International Journal of Information Management, 69, 1-12.

Steven Livingstone

Associate Professor, Computer Science, Faculty of Science

I am an Associate Professor in the Computer Science Group, Faculty of Science, at Ontario Tech University, where I lead the Affective Data Science Lab (ADSL). My research focuses on emotion; how we express it through facial expressions, vocal patterns, and physical changes, and what happens in our bodies and brains when we experience emotion. My work combines experimental methods and quantitative modeling to generate new insights into emotion theory. I am also interested in the rehabilitation of facial and vocal deficits in neurodegenerative disorders such as Parkinson's disease.

Key Publications:

- Conley, W. L.Conley, W. W., & Livingstone, S. R. (under review). EMGFlow: A Python package for pre-processing and feature extraction of electromyographic signals. Journal of Open Source Software.

- Livingstone, S. R., & Russo, F. A. (2018). The Ryerson Audio-Visual Database of Emotional Speech and Song (RAVDESS): A dynamic, multimodal set of facial and vocal expressions in North American English. PLoS ONE, 13(5), e0196391.

Tanner Mirrlees

Associate Professor, Communication and Digital Media Studies,
Faculty of Social Science and Humanities

Tanner Mirrlees is an Associate Professor and current Director of the Communication and Digital Media Studies program in the Faculty of Social Science and Humanities at Ontario Tech University. Mirrlees earned a PhD from York University and Toronto Metropolitan University’s Joint Graduate Program in Communication & Culture, and won the prestigious Governor General’s Gold Medal Award for achieving the highest academic standing in the program. Mirrlees is a past president of the Canadian Communication Association (CCA) (2020-2022), a past organizer of the CCA’s annual conference for the Congress of the Federation for the Humanities and Social Sciences (2018-2020), and currently serves on the Board of Directors for the Canadian Journal of Communication and the US-based critical media studies journal, Democratic Communiqué. Mirrlees is the author or co-author of numerous books including Work in the Digital Media and Entertainment Industries: A Critical Introduction (Routledge, 2024), Global Entertainment Media: Between Cultural Imperialism and Cultural Globalization (Routledge, 2013), Hearts and Mines: The US Empire's Cultural Industry (UBC Press, 2016), and EdTech Inc.: Selling, Automating and Globalizing Higher Education in the Digital Age (Routledge, 2019). Mirrlees is also the co-editor of Media

Imperialism: Continuity and Change (Rowman & Littlefield, 2019), Media, Technology, and the Culture of Militarism (Democratic Communiqué, 2014), and The Television Reader (Oxford University Press, 2012).

Mirrlees' current inter-disciplinary research encompasses: the international political economy of technology corporations; Empire and the creative and technology industries; energy sustainability, environmental media and "green technology"; creativity; work and labor in the media and creative industries; war, military futurism, and media technologies; educational sociology and the EdTech industries; social media platform activism, from the Left to the far Right; globalization of entertainment; Internet, platform and AI law, policy and regulation; political communication, PR, propaganda and technology; popular culture, media representations, and ideology; video games and society; science, technology and society (STS) studies; techno-politics and ethics; critical theory of technology, including AI and other techno-social systems.

Mirrlees has given over 100 public presentations, with recent keynotes including "Automating Creativity? Questioning AI's Impact on the Arts (for Educators)" for the Hot Docs Teachers Conference, and "The US and China's Digital Tech War: A New Asymmetric Rivalry. Mirrlees has co-organized over 40 public events (conferences, symposia, and webinars), interviewed with print, radio, TV, digital and podcast media (most recently an episode of Courage my Friends, an AI and higher education), written op-eds, appeared in documentaries such as Theaters of War (Media Education Foundation), Myths on Screen: Hollywood's Role in War and Propaganda (CBC IDEAS), and Man Up! The Masculinity Crisis (CBC IDEAS), co-created podcasts including Tech-Bros and Techno-Utopias: A Darts and Letters Mini-Series, authored video essays for YouTube. Mirrlees is currently co-creating a new podcast series called Green Dreams: A Podcast Series on Our Renewable Futures (with Dr. Imre Szeman and Cited Media Productions), and working toward the completion of a book on the social imaginaries surrounding green technologies, and another, on global Hollywood in the digital age.

Key Publications:

- Work in the Digital Media and Entertainment Industries: A Critical Introduction (Routledge, 2024).

- EdTech Inc.: Selling, Automating and Globalizing Higher Education, in the Digital Age (with Shahid Alvi) (Routledge, 2019).

- The US and China's digital tech war: a new rivalry within and beyond US Empire. In A New Global Geometry (pp. 6-96), edited by Greg Albo. Merlin Press (2024).

- Automating Creativity? Questioning AI's Impact on the Arts (for educators). Hot Docs conference keynote (delivered to 600 high school teachers) (2024): https://www.youtube.com/watch?v=nT9mw5Xd1Fk

- EdTech, AI, and platform capitalism in the classroom. Courage my Friends podcast. Tommy Douglas Institute and Rabble.ca (2024): https://rabble.ca/podcast/edtech-ai-classroom/

Tanya Karam-Zanders

Associate Teaching Professor, General Psychology,
Faculty of Social Science and Humanities

I am a cognitive and social psychologist with research and expertise in areas of social cognition and human memory. My Bachelor's degree is in Psychology, my Master's degree is in Cognitive and Social Processes, and my PhD is in Cognitive and Developmental Psychology. As a teaching faculty, I have taught many different psychology courses, many of which are directly related to issues relevant to AI research. Notably, I teach Introduction to Cognitive Psychology, Thinking and Decision-Making, Social Cognition, Memory, Motivation, and Emotion. I have recently served on a PhD dissertation proposal committee of a student in FBIT whose research explores normative reasoning and social intelligence in AI systems. In working with this student, and his mentor, Dr. Peter Lewis, I have had the opportunity to have meaningful discussions regarding the intersection between human psychology and artificial intelligence. We also collaborated with Marieke van Otterdijk, a scholar from Norway, among others on a project titled "From Human to Agent Intuition: An Architecture for Intuitive Cognition" which is currently under review. Despite having conducted little research in artificial intelligence, I believe I can be of value to the institute and its research endeavors by providing a unique perspective that is necessary in all aspects of AI.

Tao Liu

Assistant professor, Mechanical Engineering, Faculty of Engineering and Applied Science

My research areas mainly focus on computational biomechanics and sport biomechanics. My research has centered on the use of computational modelling, machine learning and engineering principles to evaluate clinical conditions and inform the design of health technology. My research has included developing novel approaches to understand low back pain etiology, scoliosis brace design, and design of talus implants, which have been patented and are currently in use at the University of Alberta Hospital. I am currently collaborating with different industry partners, such as CCM hockey and Adidas, to help evaluate and improve their product to enhance running performance.

Key Publications:

- Liu T., El-Rich M., 2024, “Subject-specific Trunk Segmental Masses Prediction for Musculoskeletal Models using Artificial Neural Networks”, Medical & Biological Engineering & Computing (IF=3.2)

- Liu T., Aziz Vaqar H., El-Rich, M., 2023, “Sensitivity of Subject-Specific Upper Body Musculoskeletal Model Predictions to Mass Scaling Methods”, Computers in Biology and Medicine, 165 (IF=7.7)

- Liu T., Khalaf K., Hebela N., Westover L., Galbusera F., El-Rich M., 2021, “A Novel Methodology for the Prediction of Trunk Mass Distribution Using Anthropometric Measurements”, J. Biomech, 122, 110437 (IF=2.4)

- Liu T., Jomha N., Adeeb S., El-Rich M., Westover M.L., 2020 “Investigation of the average shape and principal variations of the human talus bone: an automatic groupwise registration”, Front Bioeng Biotechnol, 8, 656. (IF=6.064)

Zenia Kish

Assistant Professor, Communication and Digital Media Studies,
Faculty of Social Science and Humanities

Dr. Zenia Kish is an interdisciplinary scholar committed to publicly-engaged teaching and research that bridges the humanities and social sciences. Her work explores unconventional forms of media across global contexts, including the mediation of philanthropy and agriculture, and makes connections between digital media studies, strategic communication, critical finance studies, American studies, food and agriculture, and development. She is Associate Editor at the Journal of Cultural Economy, and serves on the boards of the Journal of Environmental Media and Communication and Race. Before joining Ontario Tech University, Zenia was Assistant Professor of Media Studies at the University of Tulsa, where she also served as the Associate Director of the Oklahoma Center for the Humanities. Zenia’s work on food, agriculture, and the environment explores representations of food and farming on social media as well as the socio-technical infrastructures reshaping the global agri-food system. Her co-edited book Food Instagram: Identity, Influence and Negotiation (University of Illinois Press 2022, with Emily Contois) offers innovative frameworks and case studies at the intersection of social media studies and food studies, and was awarded the 2023 Best Edited Volume Prize from the Association for the Study of Food and Society. She is a member of the NSF-funded Agri-Food Technology Research Project (UC-AFTeR) based at the University of California, Santa Cruz, which examines how Silicon Valley is reshaping the food and ag tech sectors, including research on tech pitching practices and open data in food and agriculture. She also co-edited a special issue of New Media and Society on “farm media” with Benjamin Peters that opens up new lines of agricultural inquiry for media studies.

Key Publications:

- “Agrarian Platform Capitalism: Digital Rentiership Comes to Farming,” with Emily Reisman and Madeleine Fairbairn, Antipode

- “Setting Data Free: The Politics of Open Data for Food and Agriculture,” with Madeleine Fairbairn, New Media & Society, 25, no. 8 (Aug 2023): 1935-1959

- “Pitching Agri-Food Tech: Performativity and Non-Disruptive Disruption in Silicon Valley,” with Madeleine Fairbairn and Julie Guthman, Journal of Cultural Economy 15, no. 5 (2022): 652-670

- “Investing for Profit, Investing for Impact: Moral Performances in Agricultural Investment Projects,” with Madeleine Fairbairn, Environment and Planning A 50, no. 3 (May 2018): 569-588

MAIRI Budget

	Items	Year 1	Year 2	Year 3	Year 4	Year 5	Total	Justification
1. Operatonal Budget								
1.1 Labour Costs - Staff								
	Research Project Manager	$ 57,717	$ 71,268	$ 73,248	$ 77,206	$ 79,186	$ 358,625	
								Level 8 (union possible), assumes Research Project Manager starts two
	Benefits (9%)	$ 5,195	$ 6,414	$ 6,592	$ 6,949	$ 7,127	$ 32,276	LTE (9%); FTE (23%)
SUB-TOTAL Labour		**$ 62,912**	**$ 77,682**	**$ 79,840**	**$ 84,155**	**$ 86,313**	**$ 390,901**	
1.2 Labour Costs - Director								
	Teaching Release - Director	$ 9,024	$ 9,285	$ 9,563	$ 9,563	$ 9,563	$ 46,998	1 course release for the Director
	Benefits (9%)	$ 812	$ 836	$ 861	$ 861	$ 861	$ 4,230	
SUB-TOTAL LABOUR		**$ 9,836**	**$ 10,120**	**$ 10,424**	**$ 10,424**	**$ 10,424**	**$ 51,228**	
1.3 Research Entity Operating Costs								
	Technical/Consulting Services						$ -	
	IT Support						$ -	
	Equipment	$ 2,000					$ 2,000	
	Office Supplies and Services						$ -	
	Staff and Director Travel						$ -	
	Technical Grant Writer/Consultant		$ 20,000		$ 20,000		$ 40,000	
	Other (explain)						$ -	
SUB-TOTAL-Research Entity Operating Costs		**$ 2,000**	**$ 20,000**	**$ -**	**$ 20,000**	**$ -**	**$ 42,000**	
2. Research Networking								
	Seminars and workshops						$ -	
	Conference	$ 5,000.00	$ 5,000.00	$ 5,000.00	$ 5,000.00	$ 5,000.00	$ 25,000	Internal Conference Y1&2; Y3-5 expand to external attendees for a fee.
	High profile speaker event	$ 1,500.00					$ 1,500	For advancement purpose
	Research awards for seed fund / hackathons	$ 10,000.00	$ 10,000.00	$ 10,000.00	$ 10,000.00	$ 10,000.00	$ 50,000	Two per year, as an incentive for new projects
SUB-TOTAL-Research Networking		**$ 16,500**	**$ 15,000**	**$ 15,000**	**$ 15,000**	**$ 15,000**	**$ 76,500**	
3. Communications								
	Launch of Institute	$ 2,000	$ -	$ -	$ -	$ -	$ 2,000	Expenses to launch Institute
	Communications Material (zap stand, electro	$ 2,000	$ 500	$ 500	$ 500	$ 500	$ 4,000	Promotinoal material
	Other (merch)	$ 5,000	$ 2,000	$ -	$ -	$ -	$ 7,000	Merchandize
		$ 9,000	**$ 2,500**	**$ 500**	**$ 500**	**$ 500**	**$ 13,000**	
4. Knowledge Transfer and Dissemination								
	Other (explain)							
SUB-TOTAL								
TOTAL OPERATIONAL BUDGET		**$ 100,248**	**$ 125,302**	**$ 105,764**	**$ 130,078**	**$ 112,237**	**$ 573,629**	
REVENUE								
	Faculty contribution (Director's Faculty)	$ 9,836	$ 10,120	$ 10,424	$ 10,424	$ 10,424	$ 51,228	**Assumed course release covered in kind**
	Advancement funds	$ 50,000	$ 50,000	$ 30,000	$ 30,000	$ 30,000	$ 190,000	**Y3-5 unconfirmed, requires donors to be identified**
	VPRI Funds / Collaborating Faculties	$ 50,000	$ 25,000	$ -	$ -	$ -	$ 75,000	
	Indirect Cost from Contracts (25%)	$ -	$ 37,500	$ 75,000	$ 112,500	$ 112,500	$ 337,500	**Assumes 25% of overheads from eligible grants are available for institute operating, as per policy: https://usgc.ontariotechu.ca/policy/policy-library/policies/legal,-compliance-and-governance/indirect-costs-of-research-policy.php.**
TOTAL REVENUE		**$ 109,836**	**$ 122,620**	**$ 115,424**	**$ 152,924**	**$ 152,924**	**$ 653,728**	
TOTAL OPERATIONAL BUDGET LESS REVENUE		**$ 9,588**	**$ (2,682)**	**$ 9,660**	**$ 22,845**	**$ 40,687**	**$ 80,099**	

Notes:
Requires a steady state income from grant overhead and/or targeted advancement funds.
Based on a steady state grant income by Y3 of 20 faculty holding grants each worth $75k / year, with 30% overhead, or an equivalent configuration.
If this is not significantly below budget, Research Project Manager position may not be feasible.
If this is met or exceeded, funds will be directed to research capacity building costs,
E.g.: selective grant fund matching, bank-style postdoctoral researchers for exploratory industry collaborations, cross-faculty HQP to engage in interdisciplinary projects, and researcher travel, as determined by the ILT.

OntarioTech
UNIVERSITY

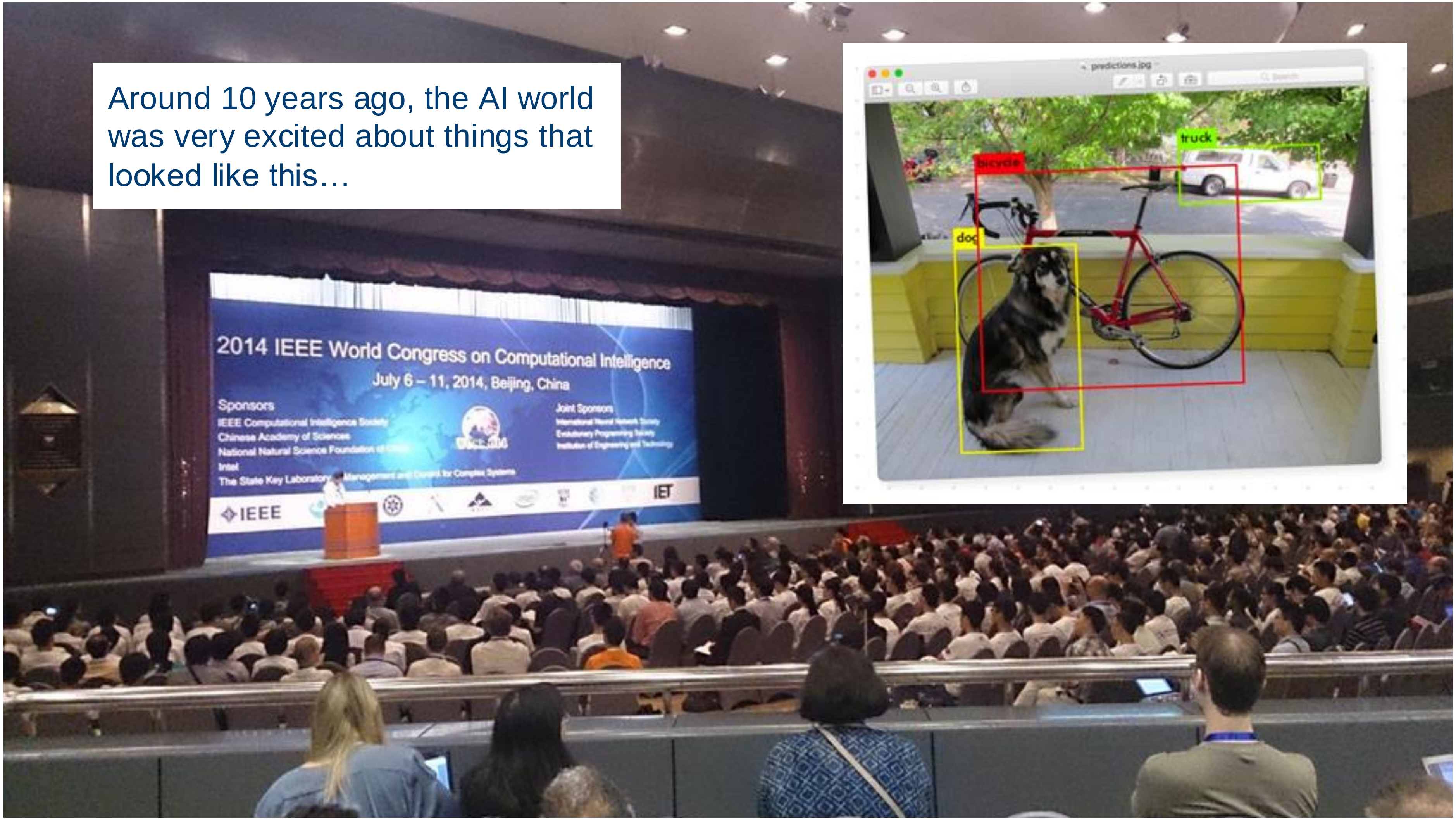
The Mindful AI Research Institute (MAIRI)

Concept & Story: *AI in a Socio-Technical World*

Given where AI is today – and how fast it is changing…

Let's imagine what intelligent machines could be:
- in 10 years time,
- in 50 years time
…and how we want to build and use them.

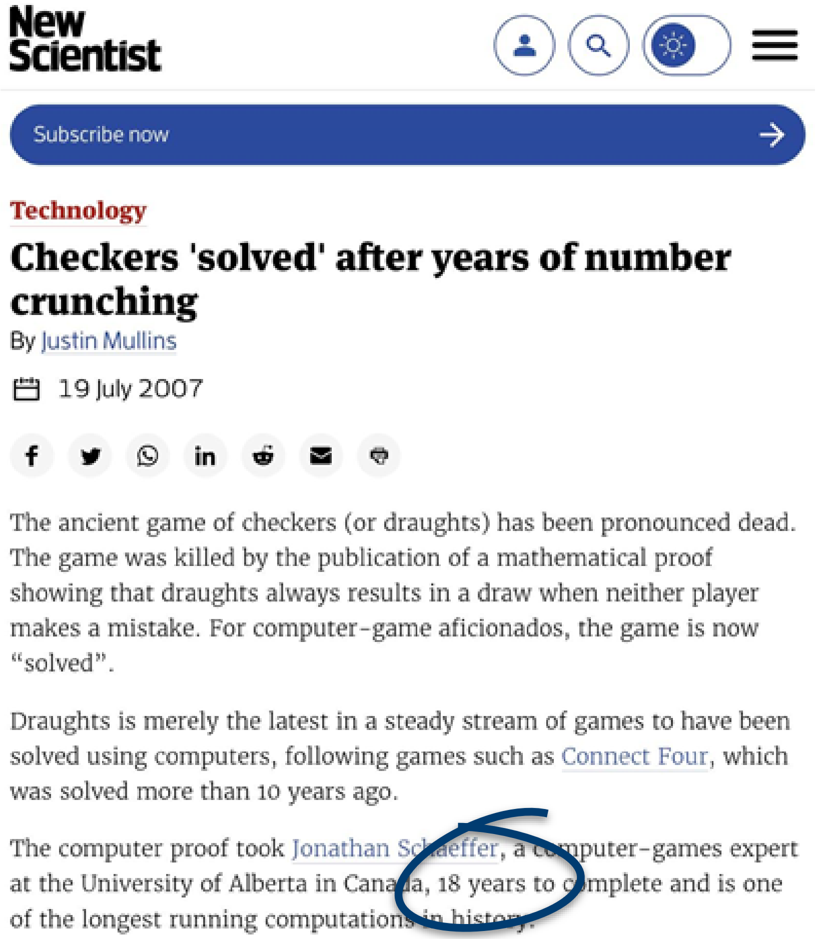
- What's missing from today's intelligent machines?
- What would we like future intelligent machines to become?
- How could they – and our use of them – be more mindful of people and the planet?



Around 10 years ago, the AI world was very excited about things that looked like this…

predictions.jpg
truck
bicycle
dog
2014 IEEE World Congress on Computational Intelligence
July 6 – 11, 2014, Beijing, China
Sponsors
IEEE Computational Intelligence Society
Chinese Academy of Sciences
National Natural Science Foundation of China
Intel
The State Key Laboratory of Management and Control for Complex Systems
Joint Sponsors
International Neural Network Society
Evolutionary Programming Society
Institution of Engineering and Technology
IEEE
IET

Just over 15 years ago, this is what results in AI for games looked like…



Technology

Checkers 'solved' after years of number crunching

By Justin Mullins

19 July 2007

The ancient game of checkers (or draughts) has been pronounced dead. The game was killed by the publication of a mathematical proof showing that draughts always results in a draw when neither player makes a mistake. For computer-game aficionados, the game is now "solved".

Draughts is merely the latest in a steady stream of games to have been solved using computers, following games such as Connect Four, which was solved more than 10 years ago.

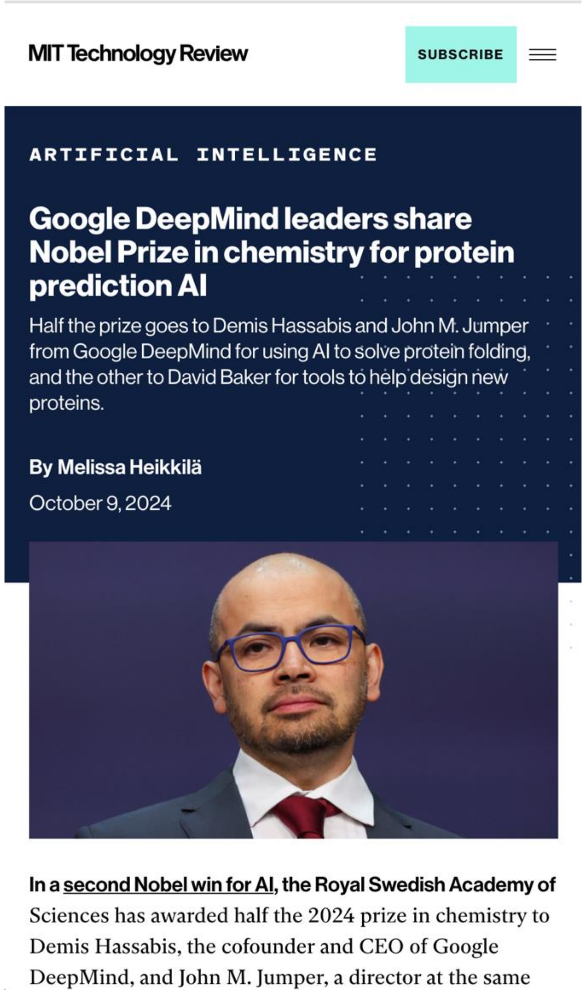
The computer proof took Jonathan Schaeffer, a computer-games expert at the University of Alberta in Canada, 18 years to complete and is one of the longest running computations in history.

Similarly to previous general purpose technologies, such as the invention of the Internet,

Today’s AI technology is having a transformational effect,

And is poised to change many areas of work and life.

But in complex ways.



MIT Technology Review

SUBSCRIBE

ARTIFICIAL INTELLIGENCE

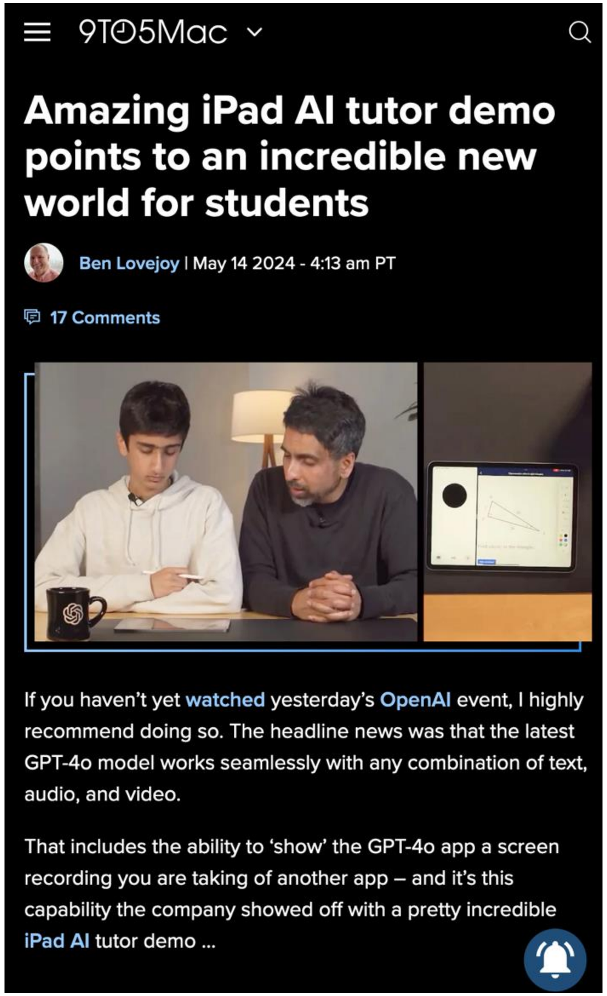
Google DeepMind leaders share Nobel Prize in chemistry for protein prediction AI

Half the prize goes to Demis Hassabis and John M. Jumper from Google DeepMind for using AI to solve protein folding, and the other to David Baker for tools to help design new proteins.

By Melissa Heikkilä

October 9, 2024

In a second Nobel win for AI, the Royal Swedish Academy of Sciences has awarded half the 2024 prize in chemistry to Demis Hassabis, the cofounder and CEO of Google DeepMind, and John M. Jumper, a director at the same



9TO5Mac

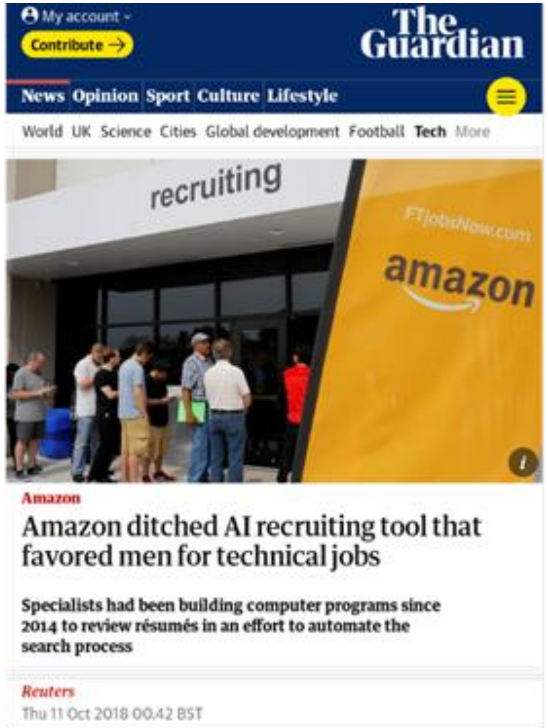
Amazing iPad AI tutor demo points to an incredible new world for students

Ben Lovejoy | May 14 2024 - 4:13 am PT

17 Comments

If you haven’t yet watched yesterday’s OpenAI event, I highly recommend doing so. The headline news was that the latest GPT-4o model works seamlessly with any combination of text, audio, and video.

That includes the ability to ‘show’ the GPT-4o app a screen recording you are taking of another app – and it’s this capability the company showed off with a pretty incredible iPad AI tutor demo …


My account
Contribute →
The Guardian
News Opinion Sport Culture Lifestyle
World UK Science Cities Global development Football Tech More
recruiting
FTJobsNow.com
amazon

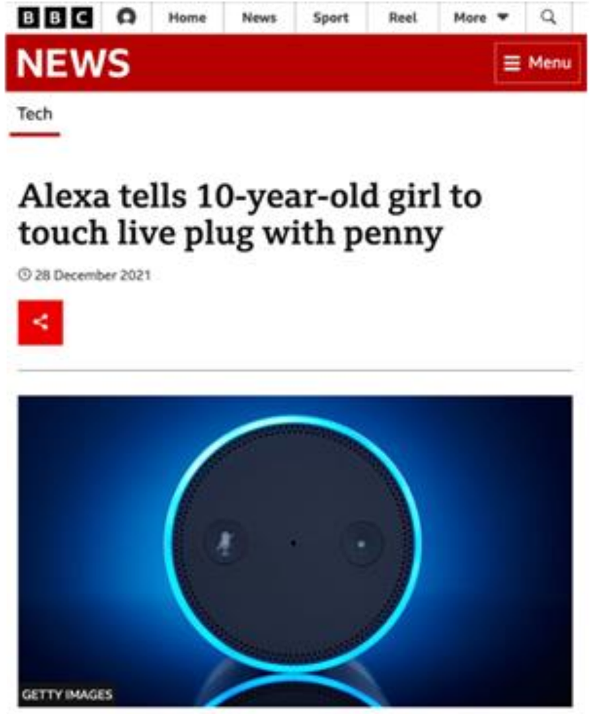
Amazon

Amazon ditched AI recruiting tool that favored men for technical jobs

Specialists had been building computer programs since 2014 to review résumés in an effort to automate the search process

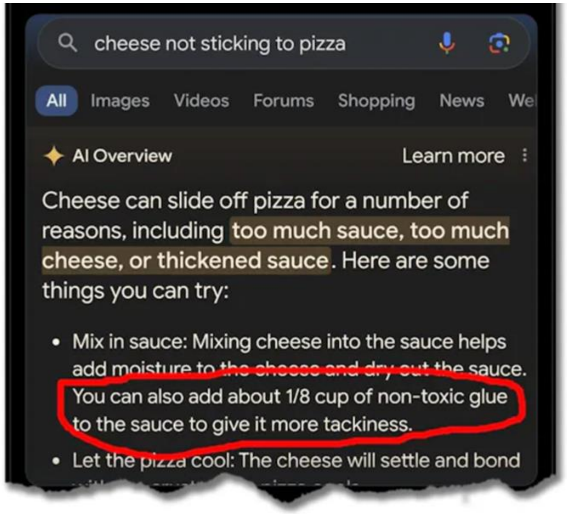
Reuters

Thu 11 Oct 2018 00.42 BST



Alexa tells 10-year-old girl to touch live plug with penny

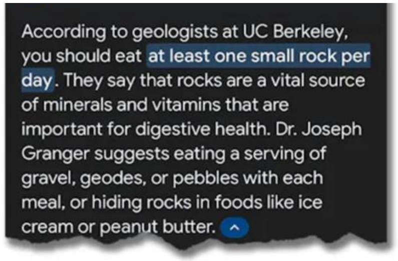
28 December 2021



cheese not sticking to pizza

Cheese can slide off pizza for a number of reasons, including too much sauce, too much cheese, or thickened sauce. Here are some things you can try:

- Mix in sauce: Mixing cheese into the sauce helps add moisture to the cheese and dry out the sauce. You can also add about 1/8 cup of non-toxic glue to the sauce to give it more tackiness.
- Let the pizza cool: The cheese will settle and bond


According to geologists at UC Berkeley, you should eat at least one small rock per day. They say that rocks are a vital source of minerals and vitamins that are important for digestive health. Dr. Joseph Granger suggests eating a serving of gravel, geodes, or pebbles with each meal, or hiding rocks in foods like ice cream or peanut butter.

It is a rocky road, with dangers in building ‘incomplete artificial minds’… and in applying them without sufficient care.

mindful

1. careful, thoughtful, observant

   “to think and consider before taking action"

2. conscious or aware of something

   especially context, self, and consequences

3. *(archaic)* having a good mind

Mindful Artificial Intelligence

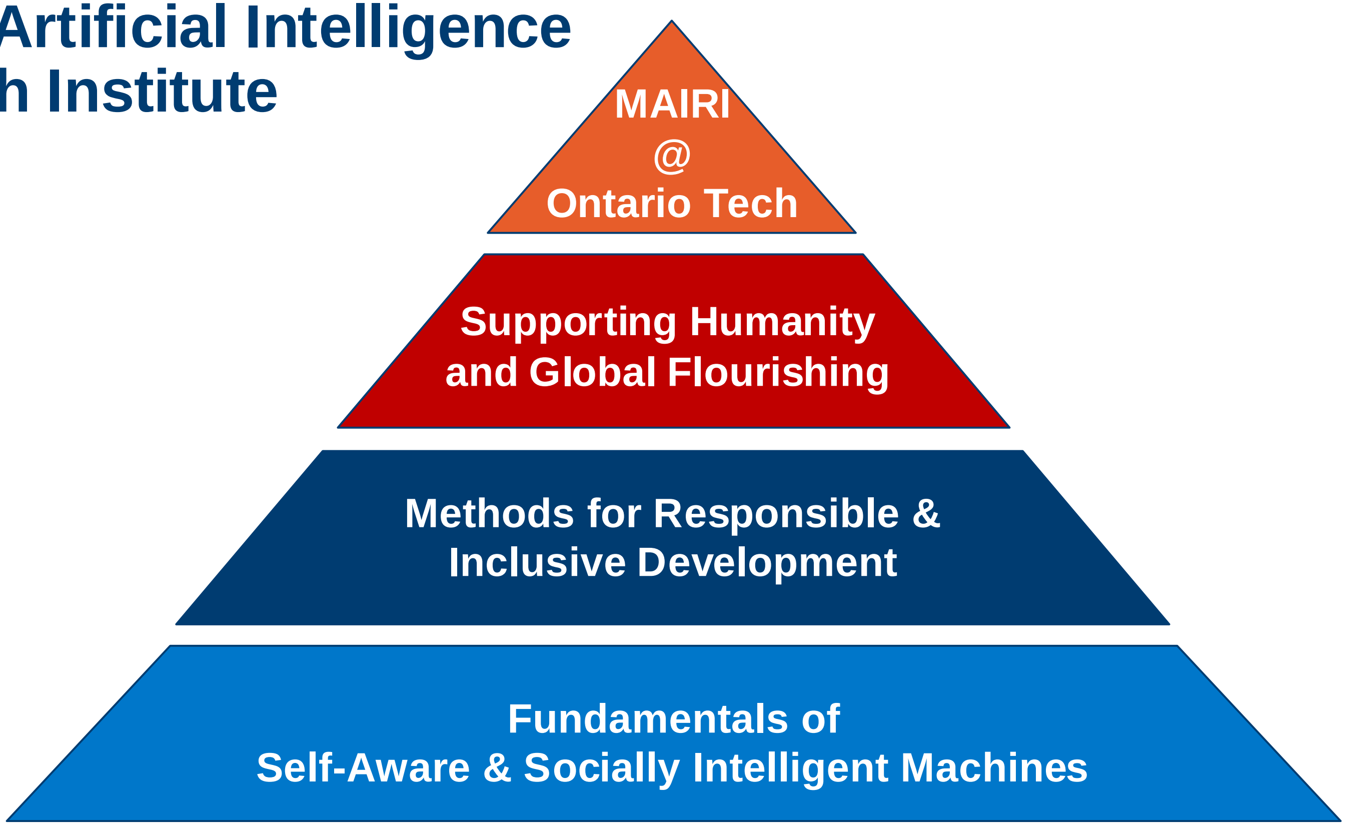
A vision for intelligent machines…

that have **rich and balanced cognitive abilities**,
that are developed in **participatory and responsible** ways,
and used **intentionally, carefully, and opportunistically,**
in ways that **support humanity** and tackle **planetary challenges**.

A vision born from the idea that we already expect intelligent machines to do more than solve puzzles, control equipment, or predict from data.

And that the building and use of these new machines should be done in the right way.

Mindful Artificial Intelligence Research Institute



MAIRI
@
Ontario Tech

Supporting Humanity
and Global Flourishing

Methods for Responsible &
Inclusive Development

Fundamentals of
Self-Aware & Socially Intelligent Machines

Mindful Artificial Intelligence: Research Themes

Fundamentals of Self-Aware & Socially Intelligent Machines

- Architectures & algorithms for reflective self-awareness
- Mechanisms for social & emotional Intelligence
- The capability to cooperate and act collectively

Methods for Responsible & Inclusive Development

- Elevating safety, trustworthiness & explainability
- Rigorous & responsible design practices
- Democratizing co-design
- Sustainable & low-energy systems

Supporting Humanity & Global Flourishing

- Socially & culturally sensitive
- Supporting individual & community empowerment
- Critical AI literacy & education
- Transformative opportunities for humanity & planetary benefit

Mindful Artificial Intelligence Research Institute (MAIRI)

An opportunity…

- To build on Ontario Tech’s strengths, commitments, and purpose:
  - AI *‘with a conscience’.*
  - Societal mission.
  - Strategic industry, academic, and civic society partnerships.
  - People and organizations empowered with and through technology.
- To lead a creative, ambitious, and distinctive research vision.
- By taking a holistic perspective on intelligent machines and their ecosystems.
- By taking a People, Society, and Planet-first approach to AI.

Research Theme

Machines that **reflect on themselves** and
the **social context and impact** of their actions.

That…

- Can model and learn about themselves - and how they react to their environment as it changes.
- Reason about and simulate the consequences of their own decisions, and model those of others (Theory of Mind).
- Understand their social role(s) and impact, reason normatively, and act accordingly.
- Model and reason about their own trustworthiness.
- Challenge: Today's AI does not have the required cognitive mechanisms for this.

Underpins: responsibility, trustworthiness, social & cultural sensitivity, human-machine partnership.

Fundamentals of Self-Aware & Social Intelligent Machines

- **Architectures & algorithms for reflective self-awareness**
- **Mechanisms for social & emotional Intelligence**
- **The capability to cooperate and act collectively**

Research Theme

Development processes that are **responsible**, **trustworthy**, **repeatable, collaborative, responsive,** and **sustainable**.

That…

- Are in partnership with affected groups through co-design.
- Are responsive to changing needs and emerging uncertainties and complexities.
- Are transparent, open and honest about risks and failures, privacy-preserving, and empowering.
- Use interpretable techniques and models to support this.
- Are energy conscious and prioritize sustainability.
- Are agile, but the antithesis of *‘move fast and break things’*.

Underpins: responsibility, trustworthiness, rigor, empowerment, equity, privacy, democracy.

Methods for Responsible & Inclusive Development

- **Elevating safety, trustworthiness & explainability**
- **Rigorous & responsible design practices**
- **Democratizing co-design**
- **Sustainable & low-energy systems**

Research Theme

An approach to deployment that is **intentional, careful**, **critical**, and through interdisciplinary **partnership.**

That…

- Looks for new opportunities for intelligent machines to help tackle the most important problems of our time.
- Acknowledges that domain expertise is essential.
- Uses guardrails to provide safety;
  and is transparent about possible failures and risks.
- Harnesses new cognitive abilities to extend guardrails to provide reflective socially and culturally sensitivity behaviour regulation.
- Changes the nature of work to provide meaningful, empowering human activity – not the reverse.

Supporting Humanity & Global Flourishing

- **Socially & culturally sensitive**
- **Supporting individual & community empowerment**
- **Critical AI literacy & education**
- **Transformative opportunities for humanity & planetary benefit**

Underpins: sustainability, conscientiousness, safety, human flourishing.

How Will We Know We Are Successful?

- Do we offer a **world-class experience** for graduate students, researchers, and research-active faculty?
- Are we **known** for something unique?
- Are we **publishing** world-leading research?
- Do we have the **critical mass** to be competitive for larger grants?
- Do we attract **attention from industry** looking for ‘the next big thing’?
- Are we **informing decision makers**, policy, and government?
- Do we enjoy a broad national and international academic **network**?

Institute Structure & Activity

- Cross-Faculty: FBIT, Science, FSSH, FEd, FHS, Engineering…
- Institute Director
- Institute Leadership Team (Director, Theme Co-Leads)
- Research Project Manager
- Institute-level Activity & Funding:
  - Seminar series; Invited speakers; Thematic workshops; Annual conference
  - Strong branding and sense of identity; Web & social media presence
  - Pump-priming grants; Research travel funds; Bridging funds; Consultancy Opportunities; Partnership Generation; Business Development
- A ‘Connector’: Hub-and-Spoke Model with Affiliated Labs and Researchers:

Institute Physical Space & Visibility

- To achieve a **high profile and sense of community**, congruent physical space and on-campus visibility are important. This is being explored separately from the main MAIRI proposal, through the usual processes.

- A few options (there will be more):

  - **Review SIRC configuration** with a view to creating congruent areas of the building for different research institutes, groups, and concentrations.

    Accompanied by corridor-level branding. E.g. →

  - First floor **'shop front' as part of a new building development**, to grow general on-campus awareness, foster a 'collision environment' for researchers, and have a space to welcome visitors and partners.

Roadmap

Initial Development Period: January – May 2023 [Completed]

- Scoping conversations with key senior stakeholders & administration (Deans & ADRs, adjacent CRCs, Research Office, Advancement)
- Environmental Scan (internal & external)

Consultation & Refinement Period: June 2023 – Dec 2023 [Completed].

Formal Proposal / Approvals Process & Brand Development: Summer & Fall 2024

- *“Faculty members… must submit to the dean(s) of the Faculty or Faculties to which they are appointed a proposal outlining the planned research entity.”*
- *“The sponsoring dean(s) will then submit the proposal to the Research Board which, in turn, will be responsible for advising Academic Council and the Board of Governors on the establishment of the research entity.”*

Institute Launch: Early 2025.

MAIRI Budget

	Items	Year 1	Year 2	Year 3	Year 4	Year 5	Total	Justification
1. Operatonal Budget								
1.1 Labour Costs - Staff								
	Research Project Manager	$ 57,717	$ 71,268	$ 73,248	$ 77,206	$ 79,186	$ 358,625	
								Level 8 (union possible), assumes Research Project Manager starts two
	Benefits (9%)	$ 5,195	$ 6,414	$ 6,592	$ 6,949	$ 7,127	$ 32,276	LTE (9%); FTE (23%)
SUB-TOTAL Labour		**$ 62,912**	**$ 77,682**	**$ 79,840**	**$ 84,155**	**$ 86,313**	**$ 390,901**	
1.2 Labour Costs - Director								
	Teaching Release - Director	$ 9,024	$ 9,285	$ 9,563	$ 9,563	$ 9,563	$ 46,998	1 course release for the Director
	Benefits (9%)	$ 812	$ 836	$ 861	$ 861	$ 861	$ 4,230	
SUB-TOTAL LABOUR		**$ 9,836**	**$ 10,120**	**$ 10,424**	**$ 10,424**	**$ 10,424**	**$ 51,228**	
1.3 Research Entity Operating Costs								
	Technical/Consulting Services						$ -	
	IT Support						$ -	
	Equipment	$ 2,000					$ 2,000	
	Office Supplies and Services						$ -	
	Staff and Director Travel						$ -	
	Technical Grant Writer/Consultant		$ 20,000		$ 20,000		$ 40,000	
	Other (explain)						$ -	
SUB-TOTAL-Research Entity Operating Costs		**$ 2,000**	**$ 20,000**	**$ -**	**$ 20,000**	**$ -**	**$ 42,000**	
2. Research Networking								
	Seminars and workshops						$ -	
	Conference	$ 5,000.00	$ 5,000.00	$ 5,000.00	$ 5,000.00	$ 5,000.00	$ 25,000	Internal Conference Y1&2; Y3-5 expand to external attendees for a fee.
	High profile speaker event	$ 1,500.00					$ 1,500	For advancement purpose
	Research awards for seed fund / hackathons	$ 10,000.00	$ 10,000.00	$ 10,000.00	$ 10,000.00	$ 10,000.00	$ 50,000	Two per year, as an incentive for new projects
SUB-TOTAL-Research Networking		**$ 16,500**	**$ 15,000**	**$ 15,000**	**$ 15,000**	**$ 15,000**	**$ 76,500**	
3. Communications								
	Launch of Institute	$ 2,000	$ -	$ -	$ -	$ -	$ 2,000	Expenses to launch Institute
	Communications Material (zap stand, electro	$ 2,000	$ 500	$ 500	$ 500	$ 500	$ 4,000	Promotinoal material
	Other (merch)	$ 5,000	$ 2,000	$ -	$ -	$ -	$ 7,000	Merchandize
		$ 9,000	**$ 2,500**	**$ 500**	**$ 500**	**$ 500**	**$ 13,000**	
4. Knowledge Transfer and Dissemination								
	Other (explain)							
SUB-TOTAL								
TOTAL OPERATIONAL BUDGET		**$ 100,248**	**$ 125,302**	**$ 105,764**	**$ 130,078**	**$ 112,237**	**$ 573,629**	
REVENUE								
	Faculty contribution (Director's Faculty)	$ 9,836	$ 10,120	$ 10,424	$ 10,424	$ 10,424	$ 51,228	**Assumed course release covered in kind**
	Advancement funds	$ 50,000	$ 50,000	$ 30,000	$ 30,000	$ 30,000	$ 190,000	**Y3-5 unconfirmed, requires donors to be identified**
	VPRI Funds / Collaborating Faculties	$ 50,000	$ 25,000	$ -	$ -	$ -	$ 75,000	
	Indirect Cost from Contracts (25%)	$ -	$ 37,500	$ 75,000	$ 112,500	$ 112,500	$ 337,500	**Assumes 25% of overheads from eligible grants are available for institute operating, as per policy: https://usgc.ontariotechu.ca/policy/policy-library/policies/legal,-compliance-and-governance/indirect-costs-of-research-policy.php.**
TOTAL REVENUE		**$ 109,836**	**$ 122,620**	**$ 115,424**	**$ 152,924**	**$ 152,924**	**$ 653,728**	
TOTAL OPERATIONAL BUDGET LESS REVENUE		**$ 9,588**	**$ (2,682)**	**$ 9,660**	**$ 22,845**	**$ 40,687**	**$ 80,099**	

Notes:
Requires a steady state income from grant overhead and/or targeted advancement funds.
Based on a steady state grant income by Y3 of 20 faculty holding grants each worth $75k / year, with 30% overhead, or an equivalent configuration.
If this is not significantly below budget, Research Project Manager position may not be feasible.
If this is met or exceeded, funds will be directed to research capacity building costs,
E.g.: selective grant fund matching, bank-style postdoctoral researchers for exploratory industry collaborations, cross-faculty HQP to engage in interdisciplinary projects, and researcher travel, as determined by the ILT.

OntarioTech UNIVERSITY

ACADEMIC COUNCIL
Minutes of the Meeting of October 22, 2024

2:31 – 4:18 p.m. videoconference

Present:

Steven Murphy (Chair)
Asifa Aamir
Scott Aquanno
JoAnne Arcand
Robert Bailey
Wendy Barber
Mihai Beligan
Mary Bluechardt
Amanda Cooper
Nicola Crow
Catherine Davidson
Ana Duff
Mikael Eklund
Nawal Elshamiy
Jessica Hogue
Mehdi Hossein Nejad
Brenda Jacobs
Les Jacobs
Hossam Kishawy
Lori Livingston
Janet McCabe
Carolyn McGregor
Fedor Naumkin
Scott Nokleby
Carol Rodgers
Robyn Ruttenberg-Rozen
Gillian Slade
Peter Stoett
Joe Stokes
Jemma Tam
Dwight Thompson
Shannon Vettor
Ken Wilson

Staff & Guests:

Kirstie Ayotte (Secretary)
Chelsea Bauer
Jamie Bruno
Stephanie Callahan
Jacqueline Dupuis
Barbara Hamilton
Michelle Heslip
Krista Hester
Shanti Fernando
Andrea Kassaris
Jennifer MacInnis
Brad MacIsaac
Kimberley McCartney
Niall O'Halloran
Darryl Papke
Jen Rinaldi
Sarah Thrush
Nick Wattie
Adam Wingate

Regrets:

Ahmad Barari
Toba Bryant
Krystina Clarke
Mitch Fraser
Sayyeed Ali Hosseini
Breanne Mcalpin
Denina Simmons
Oghenetega (Tega) Ubor

1. **Call to Order**

   The Chair called the meeting to order at 2:31 p.m. J. Tam began with a thoughtful Land Acknowledgement, sharing their personal reflection and then reading the University's Land Acknowledgement.

2. **Agenda**

   A member requested Item 11.b. 2024-2025 Academic Council and Committee Work Plans be held for discussion.

   Upon a motion duly made by M. Hossein-Nejad and seconded by A. Cooper, the October 22, 2024 Agenda and the Consent Agenda were approved as amended.

3. **Chair's Remarks**

   The Chair opened by thanking participants for their involvement in the recent Ontario Universities Fair (OUF) and reminded everyone about the upcoming Fall Open House this Saturday, encouraging attendance. He highlighted the success of the recent Fall Convocation Ceremonies, noting it as a great opportunity to showcase the university. He also celebrated a successful weekend for varsity sports and mentioned that the university will host the men's National Soccer Championships from November 7-10, encouraging participation in the event.

   In response to a question regarding an update for the Strategic Mandate Agreement Four (SMA4), the Chair noted that updates can be provided during Item 5.b) of the Integrated Academic-Research Plan update.

4. **Inquiries and Communications**

   The Chair invited B. MacIsaac to discuss the question received regarding the banner migration that was asked at the September Academic Council meeting.

   B. MacIsaac referenced the November 2023 budget report presented to Academic Council, that highlighted a plan to separate the university's system from Durham College's shared platform due to increasing delays and risks with upgrades. The project will involve migrating the system to the cloud over the next four years. A request for proposal (RFP) was issued over the summer, and a consultant has been hired. After reviewing different options and the numerous peripheral services, the decision was made to remain with the current provider, Ellucian.

   He addressed privacy concerns, particularly regarding cloud hosting, and confirmed that the university's legal office reviews new software for privacy compliance. While the review is still underway we may use Amazon Web Services (AWS) as the data centre provider, with primary hosting in Canada East and back-up in Canada West, ensuring data remains hosted in Canada.

In response to a question about whether the university was still exploring options or had already decided to separate the enterprise system, B. MacIsaac clarified that separating from Durham College's platform was necessary due to associated risks. He confirmed that the recent summer evaluation focused on reviewing the main system, and the decision to move forward has been finalized. He also noted that the main data governance owners are the Registrar's Office for student data, Human Resources for faculty and staff, and Finance.
Some discussion ensued relating to a cloud-based platform including looking forward to the range of opportunities that will arrive from this.

The Chair addressed a question regarding QuadC software and if it was being considered. He noted that he was unfamiliar with the platform.

5. Provost's Remarks

L. Livingston recognized the contributions of the Registrar's Office, recruitment teams, and booth staff at OUF. She noted that, despite lower overall attendance at the event,, there were more interactions with potential students at our booth than in previous years. Additionally, she thanked the volunteers for their efforts in making the Fall Convocation a success.

a) Senior Academic Administrator Search Update

L. Livingston provided updates regarding the Senior Academic Administrator searches, noting that Dean Carol Rodgers has expressed interest to serve a second term as Dean of the Faculty of Health Sciences. She mentioned that she will be requesting that the President's Office issue a call for expressions of interest in serving on the Renewal Advisory Committee. The work of this committee is expected to begin in January 2025.

She noted that the Deputy Provost Search Advisory Committee and the Dean of Engineering Renewal Advisory Committee have completed their work, with recommendations expected to be considered at the Board of Governors meeting in late November. Due to the timing of the November Board meeting, Dr. Mary Bluechardt's interim appointment as Deputy Provost has been extended to December 31, 2024, and Dr. Joe Stokes' acting role as Dean of the School of Graduate and Post-Doctoral Studies (SGPS) has been converted to interim status, as approved by the Board of Governors on September 26, 2024. She indicated that the plans to issue a call for expressions of interest for members to serve on the Search Advisory Committee for the next Dean of SGPS will be initiated shortly.

b) Integrated Academic-Research Plan Update (Sarah Thrush)

L. Livingston invited S. Thrush to present the Integrated Academic-Research Plan (IARP) update, reminding members that the IARP is a five-year plan evaluated annually.

S. Thrush presented key updates on the Integrated Planning process and timelines, noting that the new Strategic Research Plan (SRP) will be led by the Vice-President

of Research and Innovation (VPRI) as the current one is in its final year, and that a new Strategic Mandate
Agreement (SMA4) is currently under negotiation, advising that initial consultations with the Ministry are scheduled for early December.

She highlighted several differences between SMA4 and SMA3, including no planned enrollment growth for the first two years, a reduction in metrics from ten to eight, and an emphasis on STEM programming. She suggested bringing draft recommendations for the new metrics to the Academic Council for discussion in November, emphasizing the Ministry's interest in metrics related to investment and innovation that align with institutional goals.

She reported that Integrated Plan templates have been distributed to faculties and units to confirm the contents of the integrated plans, which will be evaluated at a later date. She advised that there are a total of 30 Integrated Plans submitted across the university : seven from academic faculties, including graduate studies, and 23 from various units.

She indicated that faculties and units will continue refining their plans, with the report-back cycle commencing this winter to summarize both qualitative and quantitative evaluations. Academic Council and the Board will receive a qualitative summary and dashboard of institutional metrics that highlights key achievements related to the IARP and research metrics as well as results from the SMA3 year five performance, including potential funding impacts .

In response to a question about how the SMA4 consultation process aligns with Academic Council, S. Thrush confirmed that the metrics will be presented to Academic Council in November. She explained that there is limited flexibility in negotiating the metrics, but the university will use its Integrated Academic-Research Plan (IARP) and SRP to shape discussions with the Ministry, focusing on aligning institutional priorities with SMA4. She noted that negotiations are primarily limited to two new metrics, with most data already defined by the Ministry.

The Chair added that unlike previous SMA negotiations, SMA4 has a more rigid framework that focuses on prescribed metrics and excludes key financial concerns, so no longer addressing financial matters typically negotiated in previous agreements.

6. Undergraduate Studies Committee (USC)

a) New Program Proposal – Faculty of Social Science and Humanities; Bachelor of Arts – Sociology, Technology and Innovation* (M)

M. Bluechardt presented the new program proposal from the Faculty of Social Science and Humanities (FSSH) for a Bachelor of Arts in Sociology, Technology, and Innovation, which was recommended by the USC on October 15, 2024. She noted that the program is on an expedited approval path, with a soft launch planned for Fall

2025 and full promotion by 2026. She highlighted that the program will focus on the societal implications of technology, offering unique theoretical and methodological approaches, while fostering interdisciplinary collaboration, cultural awareness, creativity, and leadership.

In response to a question asked regarding resources, P. Stoett explained that the Criminology program is currently underutilized, and existing faculty have the necessary expertise required to teach sociology courses. He notes that the hiring situation could be revisited if enrollment increases.

Motion:
Upon a Motion duly made by M. Bluechardt and seconded by P. Stoett, pursuant to the recommendation of the Undergraduate Studies Committee, Academic Council hereby approves the Bachelor of Arts in Sociology, Technology and Innovation program and recommends approval of the program to the Board of Governors.

7. **Graduate Studies Committee (GSC)**

J. Stokes provided the GSC report from September 24, 2024, noting that the committee reported a successful increase in enrollment this year and a record attendance at the Graduate Orientation. He also highlighted an upcoming Mental Health Workshop on November 7, 2024, encouraging attendance.

a) Duolingo English Proficiency Test – Interim Basis* (M)

J. Stokes presented the Duolingo English Proficiency Test, noting that it was adopted for undergraduate admissions during the pandemic and has since been used by many universities for both undergraduate and graduate studies. During GSC consultation, it was decided to implement Duolingo on a pilot basis to evaluate its effectiveness in relation to student success, specifically for professional degrees. He noted that additionally, some adjustments to current ESL requirements were made to ensure alignment across all programs.

In response to a question, J. Stokes clarified that the primary motivation for adopting the Duolingo English Proficiency Test is to enhance access for students. He noted that traditional tests require in-person attendance at testing centres, which can be challenging for students in rural areas, whereas Duolingo can be taken securely from home. While the test is also less expensive, the emphasis is primarily on improving accessibility rather than solely on cost reduction.

He also addressed concerns regarding data monitoring, explaining that the university tracks English scores with high school and first-year GPAs. Significant drops trigger further investigation, especially for outliers. Annual reports are submitted to the GSC for discussion. A similar approach will apply to the Duolingo test, with data analyzed after the first application cycle.

Motion:
Upon a Motion duly made by M. Bluechardt and seconded by J. Hogue, pursuant to the recommendation of the Graduate Studies Committee, Academic Council hereby approves the amended Duolingo English Test from applicants of non-thesis-based programs as sufficient evidence of English language proficiency for a trial period of 2024-2025 admissions cycle.

The following are the recommended scores for Graduate Programs:

- *Education (Med, EdD) – Minimum score of 130*
- *All other non-thesis graduate programs – Minimum score of 120*

b) Major Program Modification – Master of Health Science (FHSci)* (M)

J. Stokes presented the major program change for the Master of Health Science noting that the proposed changes come from extensive faculty consultation and an external review and includes plans for developing a course-based Master of Health Science.

Motion:
Upon a Motion duly made by M. Bluechardt and seconded by J. Arcand, pursuant to the recommendation of the Graduate Studies Committee, Academic Council hereby approves the Major Program Modification to the Master of Health Science program.

8. Governance & Nominations Committee (GNC)

L. Livingston presented two motions for Academic Council's consideration, noting their review and recommendation by the GNC during the October 15, 2024 meeting. She explained that these motions continue discussions from last month and pertain to the nomination of Faculty Council Vice-Chairs and the Faculty Council Membership lists, which are typically finalized at the first Faculty Council meeting of the year. She highlighted that, depending on timing, these appointments may not be finalized before the September Academic Council meeting.

***a)* Faculty Council Vice-Chair Nominations* (M)**

Motion:
Upon a Motion duly made by P. Stoett and seconded by R. Bailey, pursuant to the recommendation of the Governance & Nominations Committee, the Academic Council hereby approves the appointment of the following individuals as Vice-Chair of their respective Faculty Council for the term of October 1, 2024 until September 30, 2025:

- *Dr. Randy Fortier; Faculty of Science*
- *Dr. Kanika Samuels Wortley; Faculty of Social Science and Humanities*
- *Dr. Nooshin Rotondi; Faculty of Health Sciences*

b) Faculty Council Membership Lists* (M)

L. Livingston responded to a question regarding representation on the lists, explaining that the Deans are actively seeking additional nominations, especially for teaching assistants, to meet the required representation levels. She acknowledged that the timing at the start of the academic year, when new TAs are being onboarded, complicates the nomination process. Consequently, the current underrepresentation is due to timing issues rather than a lack of effort to fill the rosters.

Motion:
Upon a Motion duly made by A. Cooper and seconded by H. Kishawy, pursuant to the recommendation of the Governance and Nominations Committee, that
Academic Council hereby approves the following 2024-2025 Faculty Council membership lists as presented:

- *Faculty of Science*
- *Faculty of Social Science and Humanities*
- *Faculty of Engineering and Applied Science*
- *Faculty of Health Sciences*

9. Research Committee

L. Jacobs noted that the Research Committee recently expressed unanimous support for a draft proposal concerning the Mindful Artificial Intelligence Research Institute, which will include representatives from each faculty and be led by Dr. Peter Lewis. He mentioned that Dr. Carolyn McGregor, Dean of the Faculty of Business and IT (FBIT), will host the institute, and its governance structure will enable directors to rotate among the faculties.

He noted that the Research Committee is finalizing its structure for contributing to the new SRP, with an update expected in January 2025. Additionally, he reported that the final research funding numbers from the Council of Ontario Finance Officers (COFO) reached $28.4 million, marking an 18% increase from the previous year. He also mentioned that the advertisement for the Tier 2 Canada Research Chair (CRC) in Advanced Nuclear Engineering has been released.

Lastly, he announced that the Research Excellence Awards evening is happening next week, with posters displayed around campus and invitations being circulated. He encouraged everyone to attend to celebrate the achievements in research and the latest group of research chair winners, urging those who haven’t RSVP’d to do so.

10. Policy Consultation

a) Risk Management Policy* (C)

J. Dupuis presented the updated Risk Management Policy for consultation at Academic Council, outlining revisions made since its last update in 2019. She explained that the revisions aim to clarify practices, integrate content from the retiring compliance policy, and strengthen the university's risk management framework. Key changes include the addition of compliance risk assessment definitions, the removal of the risk management committee, expanded responsibilities for all university members, and a new training section to enhance risk awareness. She noted that the feedback from the online consultation period raised concerns about the policy being overly top-down, leading to amendments that encourage broader participation in addressing risk-related concerns.

After a comprehensive discussion, J. Dupuis and N. O'Halloran advised that they will review the feedback from this consultation and any additional questions or concerns could be directed to their offices. They confirmed that the policy will proceed to the Board's Audit and Finance (A&F) Committee for deliberation.

J. MacInnis addressed a question raised at the September Academic Council meeting regarding the review of the Postering Procedures and clarified that the procedures are not currently scheduled for review, noting that the last review was two years ago. She confirmed that there are no changes being proposed to the existing procedures and they remain as currently posted and available to view on the University website.

Concerns were raised regarding the recent removal of infrastructure for posting announcements, affecting ability to share event information. C. McGregor clarified that it is a one-off concern at this time due to the Wayfinding project and simultaneous construction in the new science and business buildings.

The Chair acknowledged concerns and reminded attendees not to confuse Communication and Marketing's Wayfinding Project with the Postering Procedures.

11. Consent Agenda

a) Minutes of the Meeting of September 24, 2024* (M)
b) 2024-2025 Academic Council and Committee Work Plans* (M)
c) 2024-2025 Undergraduate and Graduate Calendar Amendments

Upon review, the request to remove item 11.b) for discussion was withdrawn and deferred for dialogue at the next Steering Committee meeting.

The Consent Agenda was passed with the original motion.

12. Other Business

a) R. Ruttenberg-Rozen volunteered to provide the Land Acknowledgement for the November 2024 Academic Council meeting.

In response to a concern regarding unfilled Academic Council positions, N. Crow confirmed that standing committees are complete and that filling Academic Council positions requires a formal election process, noting that the next election timeline to be set by the GNC is in January 2025. She reiterated that this issue had been discussed at the last Steering Committee meeting and noted that nominations had closed for the current cycle, as also confirmed during the June Academic Council meeting.

In response to the suggestion to address the issue mid-year, the Chair emphasized that the matter had been fully discussed by the relevant governance bodies and that no further action would be taken this year.

13. Termination

Upon a Motion made by S. Nokleby, the October Academic Council meeting was terminated at 4:18 p.m.

Kirstie Ayotte, Assistant University Secretary

ACADEMIC COUNCIL REPORT

SESSION:		**ACTION REQUESTED:**	
Public	☒	**Decision**	☒
Non-Public	□	**Discussion/Direction**	□
		Information	□

TO: **Academic Council**

DATE: **November 26, 2024**

FROM: **Joe Stokes, Registrar**

SUBJECT: **Conferral of Degrees – Fall 2024**

MANDATE:

Article 1.1(a)(g) of By-law No. 2 provides that Academic Council has the authority to establish the procedures necessary to grant bachelor's degrees, master's degrees, doctoral degrees, honorary degrees and all other degrees, certificates, and diplomas in any and all branches of learning.

MOTION for CONSIDERATION:

That pursuant to the recommendations of each Faculty and the Registrar, Academic Council hereby confirms the eligibility for graduation of those students who have fulfilled all degree requirements at the end of the Fall 2024 term and recommends the conferral of degrees by the Chancellor.

POLICY CONSULTATION REPORT

TO: **Academic Council**

DATE: **November 26, 2024**

FROM: **Andrew Sunstrum, Director, Human Rights Office**

SUBJECT: **Written Consultation Opportunity: Guidelines – Anti-Hate/Anti-Racism**

BACKGROUND:

Anti-Hate/Anti-Racism Guidelines

Following the Strengthening Accountability and Student Supports Act, 2024 and the recently issued Minister's Anti-Racism/ Anti-Hate Directive, the University is required to have a robust policy in place relating to anti-hate and anti-racism.

The Minister's Directive emphasizes a human rights approach to addressing hate and racism in promotion of a safe, inclusive and respectful campus free from harassment and discrimination. The guidelines are designed to define and clarify behaviors that are inconsistent with the University's commitment to maintaining a campus free of Racism and Hate and are unacceptable under the Respectful Campus Policy.

The Guidelines include high-level descriptions of Racism and Hate Activities and how they intersect with and/or contribute to Discrimination and Discriminatory Harassment.

OPPORTUNITY TO COMMENT:

- The General Counsel is seeking community comments on the proposed policy instrument. Comments submitted will be considered by the Policy Owner.
- You may submit your feedback and recommendations for this draft policy instrument to policy@ontariotechu.ca until December 3.

NEXT STEPS:

The consultation and approval path for the Guidelines will be as follows:

- Policy Advisory Committee (complete)
- Academic Council (written consultation)
- Online Consultation
- Senior Leadership Team (deliberation)
- President (approval)

SUPPORTING MATERIALS:

- Guidelines Anti-Hate/Anti-Racism (draft)

Classification Number	*To be assigned by Policy Office*
Parent Policy	Respectful Campus Policy
Framework Category	*To be assigned by Policy Office*
Approving Authority	*To be assigned by Policy Office*
Policy Owner	General Counsel
Approval Date	
Review Date	
Supersedes	

GUIDELINES – Anti-Hate/Anti-Racism

PURPOSE

1. The purpose of these Guidelines is to define and clarify behaviors that are inconsistent with the University's commitment to maintaining a campus free of Racism and Hate, and are unacceptable under the Respectful Campus Policy. These Guidelines also clarify the University's commitment and obligation to support an inclusive campus environment free from Discrimination and Discriminatory Harassment.

DEFINITIONS

2. For the purposes of these Guidelines the following definitions apply:

"Announced Intention to Discriminate" means publishing or displaying or causing the publication or display before the public of any notice, sign, symbol, emblem or other similar representation that indicates the intention of the person to Discriminate or that is intended to incite others to Discriminate.

"Antisemitism" means a certain perception of Jews, which may be expressed as hatred toward Jews. Rhetorical and physical manifestations of Antisemitism are directed toward Jewish or non-Jewish individuals or their property, toward Jewish community institutions and religious facilities.

"Discrimination" means a distinction without lawful justification, whether intentional or not, which has the effect of denying benefits to, or otherwise disadvantaging, an individual based on a Protected Ground. Discrimination may involve direct actions that are discriminatory on their face, or it may involve rules, practices or procedures that appear neutral, but have the effect of disadvantaging one or more groups of people. Discrimination includes Discriminatory Harassment and creating a Poisoned Environment.

"Discriminatory Harassment" means engaging in a course of vexatious comment or conduct based on any Protected Ground, that is known or ought reasonably to be known to be unwelcome. Discriminatory Harassment may include, for example, taunting or mocking someone's race; making, distributing, or posting hateful content; ridiculing an individual's disability; or, targeting others with sexual, gender-based or homophobic slurs.

"**Employee**" means an individual that is employed by the University either directly or indirectly or holds an appointment with the University, including paid, unpaid and honorific appointments

“Hate Activity” means, for the purposes of these guidelines, any act that falls under the definition of a Hate Crime, Hate Propaganda and/or Announced Intention to Discriminate.

“Hate Crime” means a criminal offense committed against a person or property that is motivated in any part by bias, prejudice or hate based on race, national or ethnic origin, language, colour, religion, sex, age, mental or physical disability, sexual orientation, or any other similar factor.

“Hate Propaganda” means any communication used by a person or group that promotes hatred based on colour, nationality or ethnic origin, race, religion and/or sexual orientation, including public communication that wilfully promotes hatred against any identifiable group, or the incitement of hatred against any identifiable group where such incitement is likely to lead to a breach of the peace and includes advocating genocide.

“Homophobia” means the fear, hatred, discomfort with, or mistrust of people who are lesbian, gay, or bisexual.

“Implicit Bias” means a negative attitude, of which an individual is not consciously aware, towards a specific social group. Implicit bias is thought to be shaped by experience and based on learned associations between particular qualities and any Protected Ground. Individuals’ perceptions and behaviors can be influenced by the implicit biases they hold, even if they are unaware they hold such biases.

“Islamophobia” means a certain perception of Muslims, which may be expressed as hatred toward Muslims. Rhetorical and physical manifestations of Islamophobia are directed toward Muslim or non-Muslim individuals or their property, toward Muslim community institutions and religious facilities.

“Microaggression” means a comment or action that negatively targets an individual or group based on a Protected Ground (e.g. a single racist, sexist or homophobic comment that causes fleeting harm). Microaggressions may be intentional or accidental but are nonetheless harmful and stigmatizing to individuals based on their group identification.

“Misogyny” means the dislike of, contempt for, or ingrained prejudice against women.

"Person(s) of Authority" means any person who has charge of a workplace, authority over another Employee or authority in the administration of education, including supervisors, managers, senior management and Faculty leadership (e.g. Deans, Associates Deans, etc.).

“Poisoned Environment” means a pattern of comments or conduct including comments or conduct that are condoned or allowed to continue when brought to the attention of a manager, leader or other person of authority, that ridicule or demean a person or group based upon a Protected Ground. The comments or conduct need not be directed at a specific person, and may be from any person, regardless of position or status.

"Protected Ground" mean a ground set out in the Ontario Human Rights Code under which individuals are protected against Discrimination and Harassment. All University Members are protected under the following Protected Grounds: race, ancestry, place of origin, colour, ethnic origin, citizenship, creed, sex, sexual orientation, gender identity, gender expression, age, marital status, family status and disability. Employees are additionally protected under the Protected Ground record of offences.

"Race" is a socially constructed way of judging, categorizing and creating difference among people on the basis of geographic, historical, political, economic, social and cultural factors.

"Racialized" means the process by which societies construct races as real, different, and unequal and make these differences relevant to economic, political, and social life.

"Racism" means an abuse of power and privilege based on an ideology of superiority/inferiority between a dominant race over a non-dominant or marginalized population. It marks one set of people as 'other' and 'different' and another set of people as 'normal' or 'better'.

"Student" means an individual who is registered either as a part- or full-time student at the University.

"Stereotype" means when a group of people are categorized by attributing characteristics, whether positive or negative, to all members of that group.

"Transphobia" means the fear, hatred, discomfort with, or mistrust of people who are two-spirited, transgender, nonbinary, and gender nonconforming.

"University" means Ontario Tech University.

"**University Member**" means any Employee, Student, or individual who Is otherwise subject to University policies by virtue of the requirements of a specific policy or the terms of an agreement or contract, including visitors and guest speakers.

SCOPE AND AUTHORITY

3. These Guidelines apply to all University Members.

4. The General Counsel, or successor thereof, is responsible for overseeing the implementation, administration and interpretation of these Guidelines.

GUIDELINES

5. Commitment

5.1. The University is committed to providing a campus environment where all University Members are treated with dignity, and to fostering a climate of understanding and mutual respect. The University commits to taking swift and deliberate steps to address all forms of Racism, hatred and Discrimination, including but not limited to anti-Indigenous Racism, anti-Black Racism, Antisemitism, Islamophobia, Homophobia and Transphobia, through the consistent application of its human rights policies.

5.2. The University has an obligation to pay attention to historical and ongoing injustice and Racism, to address it, and to play an active part in creating a more just and equitable society. To this end, the University commits to:

a) Proactively assess and address signs of systemic Discrimination.

b) Respond to acts of Discrimination, including a Poisoned Environment, in a timely, effective and proportionate manner, pursuant to the Procedures to Prevent and Address Discrimination and Harassment by or Against Employees and the Procedures to Prevent and Address Discrimination and Harassment by or Against Students.

c) Implement proactive measures to support an inclusive campus environment free from Discrimination, including measures such as practices to support dialogue, early intervention and de-escalation.

d) Continuously review and improve the University's efforts to prevent and respond to incidents of Discrimination, Racism and Hate Activity by analyzing dispute resolution data for trends and patterns and in response to specific acts identified through the dispute prevention and resolution program.

5.3. The University shall publicly report annually to the Board of Governors on: (i) the number and type of complaints of Discrimination related to Racism and Hate Activity, reported by University Members; (ii) the general categorization of the complaints; (iii) the associated Protected Ground and applicable sub-category for the complaints; and (iv) outcomes of the complaints including whether a complaint was substantiated, whether remedial measures were implemented, adherence to associated timelines, and any involvement of law enforcement.

6. Race and Racism

6.1. The University recognizes the dignity and worth of every person and acknowledges that Racism can have a significant and lasting impact on our classrooms, workplaces and the broader community. The University recognizes the importance of continuing to act against Racism and Discrimination in the University Community and to identify and address systemic barriers to full and equal participation.

6.2. Race is a concept. It is a socially constructed way of judging, categorizing and creating difference among people. It is related to geographic, historical, political, economic, social and cultural factors. Although there are no biological "Races" the social construction of Race is so strong that it creates real consequences for individuals. Specific traits and attributes can be Racialized by connecting them with Racialized people and deeming these traits as abnormal or of less worth (such as skin colour). Historically, Racialized traits include physical features, accents, manner of speaking, names, clothing, grooming, diet, beliefs, practices, etc.

6.3. Not every manifestation of Racism can be dealt with through the formal human rights complaint mechanism and process of the University. Nevertheless, Racism plays a major role in the social processes that give rise to and entrench racial Discrimination. As such, acknowledging and understanding Racism as a historical and current reality in Canadian society is critical to achieving human rights goals.

6.4. When generalizations are applied to groups, they can lead to assumptions that have no basis in reality and ignore the diversity within the group. Historical context can play a role in the creation of Stereotypes, for example, the Stereotype of Jewish persons being greedy originated in Europe around the 11th century when the Church forbade Christians from lending money. At the time, Jewish people were restricted from other occupations but were permitted to lend money as it was considered 'dirty' for Christians to do. This led to associating Jewish people with greed since the European Middle Ages and crops up in the writings of Shakespeare and Dickens. This negative stereotyping has led to Discrimination and Harassment to this day. Even positive stereotypes, (such as believing that all Asians are excellent at math, or all Black people excel at sports) act as a limiting characteristic for members of the group. These Stereotypes carry with them assumptions of lack of creativity and do not reflect the diversity of talents or experiences that exist within Asian and Black communities. Stereotypes based on Race can lead to subtle or overt Microaggressions and contribute to Discriminatory Harassment, Discrimination and even acts of hate.

6.5. Discrimination based on Race is particularly egregious as employment opportunities are integral to socio-economic well-being which in turn impacts health, generational access to education, and services more broadly. Racial Discrimination has significant impacts on victims as it attacks the core of basic human respect and dignity. Racial Discrimination tells its victims that they are ‘less than’, that they are ‘abnormal’ or ‘different’ and the perpetrator is ‘normal’ and ‘better’. In this way, Racism can result in excluding individuals from their society, their community, or their workplace, which can cause extreme psychological, emotional, and physical harm. These harms can have lasting effects that carry on through generations and can create a continual cycle of marginalization.

6.6. Deep-rooted Stereotypes and racist attitudes often persist due to these long-standing historical contexts. Although Racism can be experienced by any Race and ethnicity, the following examples are used to highlight the interplay between historic events and attitudes, and Racism experienced today by Indigenous and Black communities:

A) **Anti-Indigenous Racism:** Historically, policies and practices towards Indigenous persons (First Nations, Inuit and Metis peoples) have been based on ill-conceived assumptions that they are inferior and incapable of governing themselves. Other patterns of interaction were characterized by a desire to assimilate, displace or segregate Indigenous persons, and to suppress Indigenous cultures – all of which formed official government policy actively pursued over generations. While recent decades have seen progress in addressing Indigenous rights in Canada, much remains to be done on the path to reconciliation, healing and to level the playing field for Indigenous peoples. The legacy of colonialism and racist government policy continues to negatively impact Indigenous individuals and communities to this day and contribute to the perpetuation of racist attitudes towards Indigenous people.

B) **Anti-black racism:** The enslavement of Africans, racial segregation and Discrimination are also part of Canada's history. Black slavery was actively practiced in Canada between 1628 and the early 1800s. Although Ontario passed the first Act to limit slavery in the British Empire, after the abolition of slavery, prejudice and Discrimination continued to constrict the opportunities of most Canadians of African ancestry. African Canadians were excluded from schools, churches, restaurants, hospitals and public transportation. They were often restricted to menial, low-paying and exhausting labour.

7. Hate

7.1. Hate Activity is committed to intimidate, harm or terrify victims and the identifiable groups to which they belong. Victims of hate are targeted on the basis of who they are and/or the groups to which they belong (e.g., being Jewish, Muslim, Transgendered, Black, Indigenous, Asian, Women). Hate Activity can have a significant psychological and emotional effect on individuals, creating fear and distrust.

7.2. Incidents of Hate Activity may involve direct acts or incitement of others to intimidate, Harass, physically attack or threaten physical violence against a person, a group or a property and can take the form of:

a) acts of violence, intimidation and/or Harassment
b) verbal slurs accompanied by a threat
c) vandalism of ethnic, religious, or 2SLGBTQ+ sites, institutions or businesses
d) sexual assaults
e) bomb threats or swatting
f) Public messages that imply that members of an identifiable group are to be despised, scorned, denied respect and made subject to ill-treatment on the basis of group affiliation.

7.3. Hate can be motivated by membership in any identifiable group including, but not limited to, motivations of one or more of the following: Antisemitism, Homophobia, Islamophobia, Misogyny, Racism and Transphobia.

7.4. Hate Activities are a serious breach of the Respectful Campus Policy, may constitute a criminal offense, and will not be tolerated by the University. The University will not hesitate to engage and cooperate with local law enforcement to appropriately address and respond to allegations of Hate Activities on campus.

8. Freedom of Expression and Academic Freedom

8.1. Excellence in the University community is fostered by promoting the freest possible exchange of information, ideas, beliefs and opinions in diverse forms. It can include dissemination and discussion of controversial topics and unpopular points of view. However, freedom of expression and freedom of inquiry must be exercised responsibly, in ways that demonstrate active concern and respect for others, including their ability to participate meaningfully in the exchange of information, ideas, beliefs and opinions.

8.2. Differing opinions, beliefs, ideas and controversial topics can be presented and expressed in a manner that benefits academic and intellectual pursuits while maintaining a safe space for all. These same sentiments may also be expressed in a manner that runs afoul of the University's attempts to create and maintain a campus environment that is equitable, inclusive and accessible. It is the responsibility of all University Members to know the difference and to act accordingly.

8.3. Expression that extends to Discriminatory Harassment or Hate Activity is never acceptable on the University campus. The University will not tolerate, ignore or condone Discrimination of any kind, and will not hesitate to take action to address behaviour contrary to the values of the institution.

9. Responsibilities

9.1. All University Members are expected to:

a) Familiarize themselves with the contents of the University's Human Rights Policy instruments, including these Guidelines;

b) Refrain from Discrimination and Discriminatory Harassment, including Hate Activity;

c) Treat others with respect and in a manner that does not perpetuate discriminatory beliefs or outcomes, including but not limited to, refraining from subtle or overt acts of Antisemitism, Homophobia, Islamophobia, Misogyny, Racism, and Transphobia; and,

d) Reflect upon one's potential Implicit Bias and how it may contribute to ingrained attitudes and treatment of others based on their membership in a protected group, including acts that amount to Microaggressions.

9.2. University Members are further encouraged to:

a) Call out and confront behaviours and acts that perpetuate discriminatory beliefs or outcomes, such as Antisemitism, Homophobia, Islamophobia, Misogyny, Racism, and Transphobia when it is safe to do so; and,

b) Report incidents of Discrimination and Discriminatory Harassment to the University's Human Rights office.

MONITORING AND REVIEW

10. These Guidelines will be reviewed as necessary and at least every five years (unless another timeframe is required for compliance purposes). The General Counsel, or successor thereof, is responsible to monitor and review these Guidelines.

RELEVANT LEGISLATION

11. Criminal Code of Canada

Ministry of Training, Colleges and Universities Act

Ontario Human Rights Code

RELATED POLICIES, PROCEDURES & DOCUMENTS

12. Respectful Campus Policy

Procedures to Prevent and Address Discrimination and Harassment by or Against Employees

Procedures to Prevent and Address Discrimination and Harassment by or Against Students

POLICY CONSULTATION REPORT

TO: **Academic Council**

DATE: **November 26, 2024**

FROM: **Niall O'Halloran, Manager, Policy & Privacy**

SUBJECT: **Written Consultation Opportunity:**
Student Mental Health Services Policy and Supportive Leave Procedure

BACKGROUND:

Student Mental Health Services Policy

Following the Strengthening Accountability and Student Supports Act, 2024 and the recently issued Minister's Student Mental Health Directive, both the legislation and the directive require the University to have a robust policy in place relating to mental health and wellness supports and services available to students.

The Minister's Directive emphasizes a holistic approach to mental health, combining promotion, intervention and crisis response. The policy is designed to promote mental health awareness, provide accessible mental health services and foster a supportive campus environment to help students succeed academically and personally.

The Student Mental Health Services Policy includes a high-level description of the services and supports available to students. The Policy was developed in consultation with the services and staff that provide these services.

Supportive Leave Procedure and Student of Concern Committee Terms of Reference

The Supportive Leave Procedure provides a non-punitive process by which students whose behaviours may cause significant disruption of their educational experience or that of fellow students can seek a voluntary leave of absence. Alternatively, where a student is unable or unwilling to take a leave, the Deputy Provost can initiate a Supportive Leave. In either case, the Procedure allows for the university to confirm that any conditions which resulted in disruptive behavior have been addressed before the student may return to studies. The procedure and terms of reference have been developed in collaboration with the General Counsel's Office, the Office of Campus Safety, the Deputy Provost's Office, Risk Management and Student Counselling.

OPPORTUNITY TO COMMENT:

- The Office of the Deputy Provost is seeking community comments on the proposed policy instruments. Comments submitted will be considered by the Policy Owner.
- You may submit your feedback and recommendations for these draft policy instruments amendment to policy@ontariotechu.ca until December 3.

NEXT STEPS:

The consultation and approval path for the Policy will be as follows:

- Policy Advisory Committee (complete)
- Online Consultation (complete)
- Academic Council (written consultation)
- Senior Leadership Team (deliberation)
- President (approval)

SUPPORTING MATERIALS:

- Student Mental Health Services Policy (draft)
- Supportive Leave Procedure (draft)
- Student of Concern Committee Terms of Reference (draft)

Classification Number	ADM 13XX
Framework Category	Administrative
Approving Authority	President
Policy Owner	Provost and VP Academic
Approval Date	DRAFT FOR REVIEW
Review Date	
Supersedes	

STUDENT MENTAL HEALTH POLICY

PURPOSE

1. The purpose of this Policy is to describe the programs, policies, services and supports available at the University in respect of student mental health.

2. The University recognizes the significant impact of mental health on academic success, social interactions and overall quality of life and that each and every member of the University has the right to learn and work in an environment that does not have a harmful impact on their mental health. The University is committed to continue providing its students with access to various services and resources for mental health and well-being. This Policy has been developed with a number of best practices in mind such as prompt access to services, close collaboration with peers, proactive student-focused approaches, high quality counselling, and early alert system implementation.

DEFINITIONS

3. For the purposes of this Policy, the following definitions apply:

“Leave of Absence” means a temporary withdrawal from courses at the request of a Student and that is approved under the Supportive Leave Procedure to enable a Student to address health or other issues prior to return to studies.

“**Mental Health Needs**” comprises of the unique needs for care and support that a student requires to ensure their emotional, social and psychological well-being and to help the student deal with their state of mind and behaviour that adversely affects the student psychologically or emotionally.

“**Student**” means anyone who is registered in an undergraduate program or in a master’s or doctoral program at the University on either a full-time or part-time basis and **Students** will be interpreted accordingly to refer to more than one Student.

“Student Behaviour Policies” means the University’s policy instruments that regulate student conduct, including the Student Conduct Policy, Student Sexual Violence Policy, Respectful Campus Policy, Professional Suitability Policy, and Academic Integrity Policy and related procedures.

“Supportive Leave” means a leave directed by the University when a registered Student poses a risk of harm to themselves or others or poses a significant risk of disruption to their own or others educational experience. This may include a state or conduct that prevents them from being able to succeed academically, even with academic accommodations in place.

SCOPE AND AUTHORITY

4. This Policy applies to all Students registered with the University in accordance with its academic regulations.

5. The Provost and Vice-President, Academic, or successor thereof, is the Policy Owner and is responsible for overseeing the implementation, administration and interpretation of this Policy.

POLICY

6. The University is committed to creating and maintaining a safe and supportive environment that promotes the mental well-being of its Students and helps Students thrive emotionally, academically and personally.

7. To this end, the University:

7.1. offers accessible services, programs and workshops to support the Mental Health Needs of Students, and to ensure timely intervention; and

7.2. makes resources related to mental health available to all faculty and staff that are intended to reduce stigma by promoting awareness of Mental Health Needs, and facilitating a greater understanding of basic strategies and resources for supporting individuals experiencing a mental health challenge.

8. The University understands that individual Students have unique needs and aims to provide a range of services that will meet these unique needs with appropriate support and care.

STUDENT MENTAL HEALTH SERVICES AND SUPPORTS

9. Mental Health Services

9.1. Student Mental Health Services ("SMHS") provides a range of mental health services following the Centre for Innovation in Campus Mental Health's endorsement of a Stepped Care model such as professional short-term counselling and therapy services, as well as appropriate referrals to supports in the community. The approach uses the optimized level of intervention to produce the most effective results.

9.2. The University offers the following services:

a) Single Session Supports provided by SMHS –

- Intake session – one of the Mental Health and Wellness Facilitators will assess the Student's needs and make recommendations.
- Distress drop-ins – these are appointments focusing on current distress and may be available only during business hours.

b) Therapy and specialised supports – Therapy and specialised supports for Students who need one-on-one support from a mental health counsellor or a referral to a specialized program.

c) Students who have been impacted by sexual violence can access trauma-informed treatment and support for their wellness and healing by making an appointment. Mental health workers provide Students who have experienced sexual violence with a safe, therapeutic environment to discuss their experiences. The Student Sexual Violence Policy and Procedure provides various reporting and disclosure options that can be initiated by students.

d) Mental Health Groups – Students can participate in a range of groups that will support their mental health.

e) Mental Health Peer Mentors – Peer Mentors provide emotional and social support.

f) Workshops – Workshops help Students participate in activities that support their mental health. One such workshop, Campus Connected, helps Students listen with empathy and engage with an attitude of care.

g) Self-Help Resources – Students can explore various ways to improve mental health using the on-campus and community resources, digital resources and information regarding helplines accessible on the Student Life webpages. Most of the community and digital resources may be accessed by individuals registered in a continuous learning program.

9.3. Student members of the Ontario Tech Student Union ("OTSU") have access to additional services, such as an e-mental health program and a wellness centre.

10. Health Care Services

10.1. The Campus Health and Wellness Centre offers access to confidential and comprehensive services. Their team consists of physicians, nurses, a pharmacist, lab technician, residence outreach coordinators, and administrative staff working together to assist students in managing a healthy lifestyle and support mental well-being.

10.2. Student members of the OTSU also have access to a student health insurance plan.

11. Student Support Committee

11.1. The University has established a Student Support Committee (the "Committee") to assess and review matters related to Student behavior that may be influenced by student mental health. The Committee is advisory to the Deputy Provost and the Office of Campus Safety, or other decision-makers under applicable Student Behaviour Policies.

11.2. The Committee may assign a designate to provide support to individual Students in accessing resources and ensuring that appropriate Accommodations can be provided. The designate will also assist with any transition to a Leave of Absence or Supportive Leave, and support the Student in a return to learning.

12. Other Student Support Services

12.1. Students have access to an academic advisor whose advice and support may help address stress related to academic performance.

12.2. Students living in residence have access to Outreach Coordinators who provide coaching and support.

12.3. Student members of the OTSU have access to additional support services, including resources for financial wellness and student organizations such as faculty-based societies and clubs.

12.4. The University provides various other facilities and resources for promoting the overall well-being of its Students. These include resources and facilities for adopting a healthy lifestyle, for recreation, and for Students' fitness.

13. Academic Accommodations

13.1. The University is committed to creating a campus community that is inclusive of all individuals. The University provides academic accommodations for qualified Students with disabilities in accordance with the Procedures for Academic Accommodation for Students with Disabilities.

14. Interruption of Studies or Withdrawal

14.1. A Student may decide to withdraw, temporarily or permanently, due to Mental Health Needs in accordance with the University's applicable policies and procedures.

14.2. The University will continue to offer such a Student access to mental health services and support until such withdrawal.

15. Conduct

15.1. Mental Health Needs do not exempt Students from complying with the University's Student Behaviour Policies.

15.2. Mental Health Needs may be considered as a mitigating factor in disciplinary or misconduct proceedings. When a Student is affected by Mental Health Needs, the decision makers and the recommending bodies under the University's Student Behaviour Policies may acknowledge it as a mitigating factor, and must refer to appropriate support and approach the situation with due sensitivity.

16. Confidentiality of Disclosures

16.1. All disclosures made by Students regarding Mental Health Needs will be considered confidential and handled in accordance with applicable legislation and the University's Access to Information and Protection of Privacy Policy or Privacy Policy: Personal Health Information Collection, Use and Disclosure, as applicable.

16.2. The University encourages Students to access these mental health services and to disclose Mental Health Needs to allow for early intervention. The University recommends such disclosure when they substantially impact the day-to-day activities of a Student. This enables the University to offer appropriate support at an early stage.

MONITORING AND REVIEW

17. A report will be submitted to the Board of Governors every year on the implementation and effectiveness of this Policy in the preceding year. Reports will be available on the University's website.

18. This Policy will be reviewed as necessary and at least every three years. The Provost and Vice-President, Academic, or successor thereof, is responsible to monitor and review this Policy.

RELEVANT LEGISLATION

19. Strengthening Accountability and Student Supports Act, 2024

Freedom of Information and Protection of Privacy Act

Personal Health Information Privacy Act

RELATED POLICIES, PROCEDURES & DOCUMENTS

20. Accommodation Policy

Accessibility Policy

Procedures for Academic Accommodation for Students with Disabilities

Respectful Campus Policy

Student Conduct Policy

Student Sexual Violence Policy & Procedures

Academic Integrity Policy & Procedures

Access to Information and the Protection of Privacy Policy

Privacy Policy: Personal Health Information Collection, Use and Disclosure

Policy on the Recognition of Student Organizations

Student Association Accountability Policy

Classification Number	*To be assigned by Policy Office*
Parent Policy	Student Mental Health Policy
Framework Category	Administrative
Approving Authority	Administrative Leadership Team
Policy Owner	Deputy Provost
Approval Date	DRAFT FOR REVIEW
Review Date	
Supersedes	

SUPPORTIVE LEAVE PROCEDURE

PURPOSE

1. In alignment with the University's commitment to providing appropriate support and care to meet the unique needs of its Students, this document provides a pathway for Students who are struggling and require assistance in addressing behaviours that may pose a risk of harm to themselves or other University Members, or result in significant disruption of their educational experience or that of fellow students.

2. This Procedure intends to:

a) identify and support Students with behaviours that pose a risk to themselves or others or cause significant disruption of their educational experience or that of fellow students in order to promote academic success and well being for University Members;

b) assess the level of risk Students may pose to themselves and to other University Members,

c) provide a non-punitive process by which Students can seek a Leave of Absence or undertake a Supportive Leave and;

d) educate the University community on the Student Support Committee function and the role the community plays.

DEFINITIONS

3. For the purposes of this Procedure, the following definitions apply:

"Administrative Fairness" means that University Decision-Making Processes result in Decisions that are arrived at fairly, in accordance with the standards set out in the Fair Processes Policy.

"Decision" means:

- a decision to place a Student on a Supportive Leave;
- the imposition of Interim Measures;
- a decision rejecting the Student's application to return from a Supportive Leave;

"Interim Measures" means the set of interim actions recommended by the Student Support Committee in cases where it believes reasonably that the Student may harm themselves and / or others, damage the university property, or their continued presence on University campus may disrupt the operation of the University.

“Leave of Absence” means a temporary withdrawal from courses at the request of a Student and that is approved under this Procedure to enable a Student to address health or other issues prior to return to studies.

“Online University Environment” means all online media including websites, email, social media accounts, online learning tools and applications provided, managed or self-identified as belonging to the University. This includes but is not limited to the University’s website, branded social media events (i.e. Facebook Live and X), as well as online learning and collaboration tools such as Google Apps for Education.

“**Return to Campus Plan**” means a plan prepared to facilitate the return of a Student who had been on Leave of Absence or Supportive Leave, to the University and the relevant academic program.

“Student” means anyone who is registered in an undergraduate program or in a master’s or doctoral program at the University on either a full-time or part-time basis and “**Students**” will be interpreted accordingly to refer to more than one Student.

“Student Behaviour Policies” means the university’s policy instruments that regulate student conduct, including the Student Conduct Policy, Student Sexual Violence Policy, Respectful Campus Policy, Professional Suitability Policy, and Academic Integrity Policy and related procedures**.**

“Student Support Committee” or **“Committee”** means a committee established under the Student Mental Health Policy to assess and review matters related to Student behavior that may be influenced by an individual’s mental health needs. The Committee is advisory to the Deputy Provost or other decision-makers under applicable Student Behaviour Policies.

“Supportive Leave” means a leave directed by the University when a registered Student poses a risk of harm to themselves or others or poses a significant risk of disruption to their own or others educational experience. This may include a psychological state or conduct that prevents them from being able to succeed academically, even with academic accommodations in place.

“University Members” means any individual who:

- is employed by the University or holds an appointment with the University, including paid, unpaid and/or honorific appointments (“Employee”);
- is a Student;
- Is otherwise subject to University policies by virtue of the requirements of a specific policy (e.g. Booking and Use of University Space) and/or the terms of an agreement or contract.

SCOPE AND AUTHORITY

4. The Provost, or successor thereof, is the Policy Owner and is responsible for overseeing the implementation, administration, interpretation and application of this Procedure.

5. This Procedure will be interpreted and applied in conjunction with the University’s Student Behaviour Policies and the Student Mental Health Policy. Where appropriate, certain administrative decisions taken under this Procedure may supersede other University policies or procedures, particularly with respect to health and safety.

6. This Procedure applies to all individuals who are registered as a Student, in accordance with the academic regulations of the University, or were at the time behaviours occurred.

PROCEDURE

7. The University acknowledges that some Students, either for their own well-being and academic success or that of other University Members, may need care and support which, in some cases, may exceed what the University can provide with respect to accommodative, mental health or other resources or supports and is best provided if the Student is not actively engaged in studies. In these exceptional circumstances, the potential disciplinary approach of Student Behaviour Policies may not be suitable.

8. Actions taken under this Procedure are supportive in nature and will not be considered disciplinary actions. Any action must respect Student rights, including rights to integrity, and rights regarding the protection of personal information. However, the University will seek to balance the rights of the Student and the rights of other University Members when assessing the conduct and making decisions with respect to the Student.

9. This Procedure will be invoked only in extraordinary circumstances such as, but not limited to, situations where a Student is unable and/or unwilling to take steps to request a Leave of Absence, as applicable. Such inability could for example occur due to a Student's mental health condition which may impede their ability to have insight into their behaviour.

10. Before a Supportive Leave is considered, efforts will be made to ensure the Student has been offered appropriate accommodations and to encourage the Student to avail themselves of a Leave of Absence at their election.

11. A Student may be required to take a Supportive Leave in situations where the Student's physical and/or mental state and/or related conduct is such that it poses a risk of harm to themselves, other University Members or significant disruption to the educational experience. This may include a state or conduct that prevents them from being able to succeed academically, even with academic accommodations in place.

12. Concerns received about conduct off-campus or in the Online University Environment will be considered by the University on a case-by-case basis, taking into account factors including whether there is an external body that is better positioned to address the concern in question.

13. Student Support Committee

13.1. The Student Support Committee ("Committee") will meet to review matters that have been referred to it.

13.2. The Committee will meet on an urgent basis to consider reports of Students referred to it that may be considered high-risk, and will provide recommendations to the Office of Campus Safety regarding Interim Measures.

13.3. The Committee will provide recommendations to the Deputy Provost or designate, as to supportive measures required, up to and including a Supportive Leave.

13.4. The Committee may assign a designate to provide support to individual Students in accessing resources and ensuring that appropriate accommodations can be provided. The designate will also assist with any transition to a Leave of Absence or Supportive Leave, and support the Student in a return to learning.

14. University Commitments

14.1. The University will make every reasonable effort to support a Student to enable the successful completion of studies.

14.2. The Deputy Provost, or designate, will endeavor to work with Students that are directed to take a Supportive Leave or elect to take a Leave of Absence to help minimize academic and/or financial impact as much as possible.

15. Protection of Privacy

15.1. The University is committed to compliance with legislation dealing with the protection of privacy, including the Freedom of Information and Protection of Privacy Act and the Personal Health Information Protection Act. Collection, use, and disclosure of personal information including personal health information pursuant to this Procedure must be in accordance with relevant law.

15.2. Personal information or Personal Health Information collected or used under this Procedure will be used only for the purposes of administering this Procedure, or for mitigating the Student's risk to self or other University Members, and will be disclosed only on a need-to-know basis. Subject to applicable law, personal information or personal health information collected, used and disclosed under this Procedure will otherwise be kept confidential, and will be stored and disposed of in accordance with the applicable legislation and Ontario Tech University's Records Management Policy.

15.3. It is understood that safety considerations are paramount, and privacy and confidentiality rights must be weighed against potential risks to the health and safety of individuals and the University community. In certain circumstances, specific and limited disclosure of personal information or personal health information must be made to mitigate risks, including where the University is obliged by law to disclose the information. Examples include where:

a) an individual is at risk of imminent and/or serious physical or psychological harm to themselves or others;

b) members of the University community may be at risk of harm; and/or

c) reporting or investigation is required by law.

16. Student Support Committee Process

16.1. Individuals who have concerns that a Student is exhibiting behaviours that may pose a risk of harm to themselves or other University Members, or result in significant disruption of their or others' educational experience should report these concerns to the relevant Dean.

16.2. Where the Dean believes that the Student's behavior is such that they may benefit from a Supportive Leave, they may refer the matter to the Deputy Provost or designate, for consideration under this Procedure.

16.3. The notification to the Deputy Provost or designate, should generally include the following information:

a) Description of events/incidents, including location, behaviour, and any other information relevant to the assessment of whether the threshold has been met and to the assessment of the possibility of a leave;

b) Additional relevant information such as other people involved and/or any witnesses;

c) Supportive resources offered or engaged, accommodations if any, and interventions taken to date; and,

d) Any other information that may assist the Deputy Provost, or designate in making an informed assessment and a fair engagement with the Student who is the subject of the notification.

16.4. After receipt of a report of a Student, the Deputy Provost or designate, will review it to make a preliminary determination of the risk level. Where there is a severe level of risk, the Student Support Committee will convene as soon as possible to discuss the case, normally, within two working days.

17. Risk Mitigation

17.1. The Committee may recommend actions to address and mitigate risk to the Student, affected University Members and/or to the campus community. Multiple actions may be recommended, including, but not limited to:

a) no further action,

b) assigning a Committee delegate to assist the Student in accessing university or community supports,

c) continued monitoring of the Student's behaviour,

d) participation in on- or off-campus counselling,

e) a professional assessment, including a psychiatric or psychological assessment or violence threat assessment,

f) a referral to the Student Mental Health Services and/or Student Accessibility Services,

g) a referral to academic and non-academic supports offered by the university, including academic advising, the Student Learning Centre, and advocacy and support services for Equity and Inclusion.

h) a referral to another internal or external agency,

i) modification of the academic course load,

j) a recommendation of a Leave of Absence until such time the Student can address health issues without incurring formal consequences,

k) relocation within residence,

l) eviction from residence,

m) suspension from residence,

n) a non-contact directive,

o) suspension of privileges,

p) restricted movement on campus (including but not limited to issuance of a no-trespass order),

q) agreement and compliance with a behavior contract including a residence behaviour contract,

r) a Supportive Leave.

18. When reasonable grounds exist, and less intrusive measures are unfeasible or have been exhausted, a professional assessment, including a psychiatric or psychological assessment or violence threat assessment, may be requested by the University. Failure to produce results of the evaluation that demonstrates the Student's fitness to remain on campus may result in a Supportive Leave or the Student may elect a Leave of Absence.

19. Failure to comply with the risk mitigation strategies communicated to the Student may result in additional risk mitigation strategies being implemented, including but not limited to a Supportive Leave or the Student may elect a Leave of Absence.

20. Interim Measures

20.1. In cases where there is reasonable apprehension that the safety of self and/or others is endangered, damage to university property is likely to occur, or where the continued presence of the Student(s) would be disruptive to the legitimate operations of the University, the Committee may recommend interim actions for consideration by the Office of Campus Safety. The director of Campus Safety, or delegate is authorized to immediately implement Interim Measures as necessary.

20.2. A Student may apply to the Deputy Provost or delegate to vary the terms of the Interim Measures within ten working days of receiving the notification, and provide any additional relevant information for consideration. The Deputy Provost will render a final decision on any Interim Measures within three business days.

20.3. Any Interim Measures will be reviewed on a regular basis.

21. Responses

21.1. Leave of Absence

A Leave of Absence occurs when a Student agrees to temporarily withdraw from the University due to mental or physical health reasons. A request for a Leave of Absence requires the appropriate medical documentation and is considered by the

Student Support Committee, with recommendations made to the Deputy Provost, or designate.

Students should complete the appropriate forms from the Registrar's Office to avoid academic penalties in advance of the Leave of Absence, or as soon as reasonably practicable. The Committee will assign a designate to assist the Student in this process. A Leave of Absence may also involve conditions (as recommended by the Committee, who may consult with a health care professional) that must be fulfilled should the Student wish to return to the University, that will be set out in a Return to Campus Plan recommended by the Committee and approved by the Deputy Provost, or designate.

21.2. Supportive Leave

Prior to the Committee arriving at a recommendation for a Supportive Leave, a University representative will endeavor to meet with the Student to obtain relevant information from the Student's perspective.

If the Committee recommends a Supportive Leave to the Deputy Provost, or designate, the Student will receive notice that their file has been referred for decision under this Procedure and the reasons why this recommendation was made. The Student will be afforded an opportunity to present their views on the matter to the Deputy Provost, or designate, prior to a final decision, and be offered an opportunity to avail themselves of a Leave of Absence.

If the Deputy Provost or designate accepts the recommendation for a Supportive Leave, the Student will not be permitted on campus or to participate in any University activities until the University determines that the Student is fit and safe to return to campus in accordance with the terms and conditions of the Supportive Leave and the Return to Campus procedure.

21.3. Decision Notification

If the Deputy Provost, or designate, decides a Supportive Leave is appropriate, the Student will be notified in writing of the Decision to their ontariotechu.net and personal email address on file and via a meeting (when possible). The Student will be provided with the terms and conditions associated with the Supportive Leave, rationale for the Decision, a review of the process leading to this Decision, appeal procedures under section 23 herein and information on the Return to Campus Procedure.

22. Return to Campus Procedure

22.1. Students placed on a Supportive Leave will be required to apply in writing to the Deputy Provost in order to return to campus. The completed application is due at least 45 days prior to the start of the semester the Student wishes to attend.

The application will require the following in order to be considered:

a) evidence that all terms and conditions associated with the Supportive Leave have been met; and

b) an assessment has been completed by appropriate treating medical professional(s) in order to demonstrate that the Student does not pose a risk of harm to themselves or others and is capable of participating appropriately in the academic life of the University.

22.2. The Office of the Deputy Provost will evaluate completed applications and their accompanying documentation and consult with the Committee. A recommendation regarding whether the Student should be permitted to return to campus and any Return to Campus Plan will be forwarded to the Deputy Provost, normally within 20 working days after receipt of a completed application.

22.3. During the review process, the Deputy Provost may require the Student to provide additional documentation from treating medical professional(s). The Deputy Provost will inform the Student, in writing, whether the application has been approved.

22.4. If, based on the available information, the Deputy Provost is of the view that the Student is unable to return to studies safely and/or to engage in the essential activities required to pursue an education at the University, the Deputy Provost may continue the Supportive Leave under this Procedure. The Decision of the Deputy Provost is subject to review and appeal as described in section 23.

22.5. The University has established time limits for the completion of academic programs. If a student is unable to receive approval to return to campus within the time limit established by applicable policy, or is unable to fulfil terms and conditions of the Supportive Leave or Return to Campus Plan within established timelines, including failure to contact the University at specified times, the University may notify the Student of the University's intention to terminate the Student's registration and/or association with the University and provide an opportunity for the Student to respond. The University must consider any response from the Student including whether an extension should be agreed to prior to proceeding to terminate the Student's registration and/or association.

23. Return to Campus Plan

23.1. Where a Student has received approval to return to campus following a Supportive Leave, the Committee will establish a Return to Campus Plan that outlines any terms of the Student's return to campus including recommended support services.

23.2. A designate of the Committee will work with the Student and oversee their transition back to campus, including reporting on progress to the Committee. The Return to Campus Plan may also include the disposition of any outstanding non-academic discipline matters and/or sanctions, and allow for accommodation of any disability-related needs to the point of undue hardship.

24. Decision Review

24.1. Students subject to a Decision under this Procedure may request, in writing, a review of the Decision where:

a) New evidence exists that was not available to the Student at the time of the original decision (through no fault of their own) that, if considered would likely have altered the outcome of the Decision; or

b) There was a fundamental flaw in the decision-making process that led to the Decision, resulting in a lack of Administrative Fairness.

24.2. A request for review must be submitted in writing to the Office of the Provost within ten working days of the Student having received notification of the Decision from the Deputy Provost, or delegate. The request must include the grounds for the review.

24.3. The Student may request an extension on the time limit for the Student to request a review and the Provost may extend the time limit, if appropriate, having regard to the University's duty to accommodate to the point of undue hardship.

24.4. The Provost will receive and review a copy of the request for review, and all materials gathered in the decision-making process and may consult with the Committee or anyone else the Provost believes may have pertinent information.

The Provost will issue a written decision within ten (10) working days of the Student's submission.

MONITORING AND REVIEW

25. This Procedure will be reviewed as necessary, and at least annually for the first two years after its introduction. Thereafter this Procedure will be reviewed every three years. The Deputy Provost, or successor thereof, is responsible to monitor and review this Procedure.

RELEVANT LEGISLATION

26. Human Rights Code, R.S.O. 1990, c. H.19

Accessibility for Ontarians with Disabilities Act, 2005, S.O. 2005

Occupational Health and Safety Act, R.S.O. 1990, c O.1, as amended

Freedom of Information and Protection of Privacy Act, R.S.O. 1990, c F. 31

Strengthening Accountability and Student Supports Act, 2024, S.O. 2024, c. 11

RELATED POLICIES, PROCEDURES & DOCUMENTS

27. Student Conduct Policy

Student Mental Health Policy

Respectful Campus Policy

Procedures to Prevent and Address Discrimination and Harassment by or Against Students

Student Sexual Violence Policy and Procedures

Fair Processes Policy

Accommodation Policy

Accessibility Policy

Procedures for Academic Accommodation for Students with Disabilities

Classification xxxxx

Framework Category Legal, Compliance and Governance

Approving Authority Senior Leadership Team

Policy Owner General Counsel

Approval Date XXXX

Review Date XXX

Last Updated XXXX

STUDENT SUPPORT COMMITEE TERMS OF REFERENCE

I. **Preamble:** Ontario Tech University is a community that values and promotes respect, integrity, diversity and accountability among all members of the university. These values can only be achieved in an environment that supports and protects the safety and security of its members. Occasionally, students who commit serious misconducts or present acute signs of danger to themselves and/or to others may require coordinated interventions from several university departments to mitigate risk. To facilitate this, the University has established a multi-disciplinary Student Support Committee Committee ("SSC" or "Committee") to a) promote academic success and well-being, and prevent possible incidence of violence or self-harm; b) assess the level of risk identified/vulnerable students pose to themselves and the University Community, and; c) educate the University Community on the Committee's role and the part the community plays. The Student Support Committee reports to Provost through the Chair.

II. **Mission:** The Committee's main goal is to connect students-at-risk with the appropriate services for their unique situation and within the limits of its expertise, ensure that the University Community continues to be a safe environment where people can reach their academic and personal potential. The committee will always endeavor to ensure a balance between the needs of the student and the needs of the community. A Committee approach is used to further the University’s goal to provide students-at-risk with a more coordinated and consistent response. The Committee is responsible for making recommendations to Provost’s Office for handling students-at-risk situations, and is committed to ensuring that appropriate advice and support is provided to those resolving and addressing students-at-risk concerns.

III. Responsibilities:

A. The Committee as a whole:

1. Meets weekly, September to May, or as otherwise determined by the SSC Committee Chair, to discuss new cases, existing cases, and other general topics related to SSC operations and best practices. June to August the SSC Committee Chair will schedule meetings as needed to discuss case activity as needed and/or general topics related to SSC operations and best practices.

2. Assesses, the risk of harm/violence to the student-at-risk or other University Community members by bringing to the task their professional training, experience, and perspective from years of working within the field or students, and within the limits of its expertise. (See appendix A for assessment & recommendation guidelines).

3. Review relevant documentation, making recommendations for support/other action on a case-by-case basis.

4. Determine on a case-by-case basis who within the University community or external to it, needs to be given information in order to better protect the health and safety of the individual student, the University Community, and/or others.

5. Builds the University community’s capacity to respond to students-at-risk by educating the campus about appropriate response mechanisms for SSC issues.

B. *Committee Chair (Deputy Provost)*

1. Calls and conducts meetings.

2. Prepares the agenda in advance of each meeting.

3. Ensures the committee operates according to the Terms of Reference.

4. Typically ensures the committee as a whole considers issues, and reaches decisions.

5. Attends all meetings or have an alternate Chair at the meeting.

6. Keeps the Provost up-to-date on the committee's activities.

C. Committee Secretary

1. Take notes of the meeting, recording the key points and making sure that all decisions and recommendations are recorded; notes agenda items for next meeting as required.
2. Prepare a draft of the minutes and consult the Chair for approval.
3. Sends meeting minutes to all members within 3 working days of the meeting.
4. Send a reminder notice of each decision requiring action to the relevant person.
5. Participate at SSC meetings.

D. Committee Members

1. Make every effort to attend meetings when they are called.

2. Contribute to the case discussion in accordance with their expertise.

3. Complete any assigned action items.

3. Act on the Committee's behalf when requested to do so.

IV. The Committee membership shall consist of the following persons or their Designate:

Deputy Provost (Chair)

Director, Counselling & Accessibility

General Counsel

Director, Office of Campus Safety

Director, Risk Management

The Chair may invite persons (or their Designate) to a meeting when there is a case that relates to their position within the University.