Faculty of Business and Information Technology (FBIT)

Program: Master of IT Security

Major Program Modification

Date: November 30, 2017

Prepared by:
Shahram S. Heydari, FBIT Graduate Program Director

Motion to CPRC or GSC: To approve a new field for the Master of IT Security program, titled: Master of IT Security – Artificial Intelligence in Security (MITS-AIS) Field

Proposal Brief

1. SUMMARY OF PROPOSED CHANGE

This proposal will create a new field for the MITS program – Artificial Intelligence in Security. The proposed field will include eight courses, a seminar and a capstone project. No new courses need to be developed, as the program map for this field will include four courses from the main MITS program, three AI-related courses that have already been approved as elective for the main MITS program, and another elective course from CSCI or MITS. Admission and program rules remain the same as the main MITS program.

2. BACKGROUND

UOIT is an innovative and market-oriented institution, pursuing inquiry, discovery and application through excellence in teaching and learning, value-added research and vibrant student life. As its mission, UOIT provides many career-oriented graduate university programs with a primary focus on innovation and responsiveness to the needs of students and employers.

The Master of IT security (MITS) program was the first graduate program at UOIT. It is a professional graduate degree that prepares students to work in the high-demand IT security industry. The program was designed to enable students to learn how to learn in the rapidly evolving IT security field. The program adopts a project method that provides students with the experience to apply core course materials to a substantial project in the workplace during the latter part of the program.

The MITS program is one of the first of its kind in Canada and one of few specialized IT security graduate degree programs available in the world. Through theory and applied learning, the program enables students to develop an extensive understanding of business and information technology security, polish communication skills and examine business and IT ethics in a team environment.

The new advances in the field of IT security have required new skills for professionals in this field, and Artificial Intelligence is one of such important skills. Artificial Intelligence is quickly becoming one of the most sought after skills for industry and academia. The Ontario government just recently announced plans for training of 1000 applied (professional) Masters students in the field of AI with funding through the Vector institute in Toronto, and UOIT as a leader in delivering market-driven programs, is in the best position to play an important role in this initiative.

The Master of IT Security (MITS), as UOIT's first graduate program, has established a reputation for high quality, market-oriented approach to train IT professionals in the field of security. Now with a new focus on the application of artificial intelligence techniques in all areas that require big data analytics, including information security, a specialized field in this area is a logical step to provide training for the next generation of IT security professionals.

3. DEGREE REQUIREMENTS

a) Program learning outcomes

Upon completing this program, students will be able to:

1) Depth and Breadth of Knowledge:

- Demonstrate working comprehension of risk assessment, IT infrastructure, and related security policies.
- Demonstrate mastery of security-related technologies and their applications in design and deployment of secure information systems
- Demonstrate comprehensive understanding of machine learning models and techniques

2) Knowledge of Methodologies in Research and Scholarship:

- Understand the research process in the discipline of information technology security.
- Understand the research process in the discipline of machine learning and artificial intelligence.
- Demonstrate mastery of the application of artificial intelligence in information security by producing a practical, original research paper

3) Application of Knowledge:

- Create and evaluate machine learning models for security-related data sets
- Demonstrate working comprehension of how AI techniques can be applied in dealing with cybersecurity threats

4) Communication Skills

- Communicate state-of-the-art research results with regard to the application of artificial intelligence in information security in a seminar presentation

5) Awareness of Limits of Knowledge:

- Understand the legal and ethical issues in dealing with issues related to information security and artificial intelligence

6) Autonomy and Professional Capacity

- Demonstrate full understanding of the requirements for independent research consistent with academic integrity and professionalism

b) Admission Requirements

Admission requirements for the new MITS-AIS field is the same as the main MITS program.

c) Program Structure

The calendar copy for the new MITS-AIS field is presented in the following.

Master of IT Security –Artificial Intelligence in Security Field

Program information

The purpose of the MITS-AIS field is to prepare and train IT professionals for the emerging applications of Artificial Intelligence in the field of IT Security. This professional stream is the first of its kind in Canada, and builds upon the successful general stream in UOIT Master of IT security program. This program combines a deep knowledge of IT Security with hands-on knowledge of AI systems and machine learning, and provides students with a

comprehensive understanding of the applications of this technology. Graduates of this program can seek employment in the growing AI industry as well as IT security firms.

Admission requirements for this program is the same as the Master of IT security program. Part-time studies are available.

Degree Requirements

The program includes eight courses, a seminar and a capstone project as following:

MITS 5100G - Law & Ethics of IT Security
MITS 5400G - Secure Software Systems
MITS 5500G - Cryptography and Secure Communications
MITS 5600G - Security Policies and Risk Management
MITS 5620G – Special Topics in IT Management
MITS 6700G – Network Data Analysis
MITS 6800G – Machine Learning
MITS 5900G – MITS Seminar**
MITS 6300G – MITS Capstone Research Project I**
MITS 6600G – MITS Capstone Research Project II**
One elective course by GPD approval*

*The elective course could include relevant courses from MITS, CSCI or ENGR graduate course listing.

**The rules for the seminar and capstone project remain the same as the MITS general stream.

The following courses from the listing above are specific to AI:

MITS 5620G – Special Topics in IT Management
MITS 6700G – Network Data Analysis
MITS 6800G – Machine Learning

d) Program Content

All courses in the proposed program have already been approved by the Graduate Studies Committee and/or being offered for the main MITS stream.

4. RESOURCE REQUIREMENT

a) Faculty members

FBIT faculty members have an established research track record in the area of IT security and data analytics, and many of them conduct research in the areas related to the applications of AI and machine learning in IT security and data analytics. Dr. Miguel Vargas-Martin is currently conducting research on application of machine learning techniques in authentication and traffic inspection, supported by an NSERC discovery grant. Dr. Amirali Salehi-Abari is conducting research on the application of AI in social network analysis and security attack prediction. Dr. Carolyn McGregor, a world expert on data analytics in health applications, also conducts research that makes use of artificial intelligence techniques. The IT security portion of the field will be delivered by the same faculty members who are teaching this courses for the main MITS program.

There is sufficient expertise in this field within FBIT that would not require adding new faculty members for delivering the new MITS-AIS field.

The list of core faculty members associated with the new MITS-AIS field is as following:

Name	Faculty	Rank	Research Area(s)
Dr. Patrick Hung	FBIT	Professor	Service computing, Security and privacy
Dr. Miguel Vargas Martin	FBIT	Professor	Machine learning techniques for user authentication and traffic inspection
Dr. Carolyn McGregor	FBIT	Professor	Intelligent agents, health informatics, data analytics
Dr. Khalil El-Khatib	FBIT	Associate Professor	Security and privacy, Biometrics, data analytics
Dr. Shahram Shah Heydari	FBIT	Associate Professor	IT networking, Quality of service, Network security
Dr. Julie Thorpe	FBIT	Associate Professor	Authentication, Brain-Computer interface, software security
Dr. Ying Zhu	FBIT	Associate Professor	Overlay networks, Smart mobile devices
Dr. Amirali Salehi-Abari	FBIT	Assistant Professor	Artificial intelligence, algorithms and computer security
Dr. Stephen Marsh	FBIT	Assistant Professor	Computational trust, soft security, social knowledge
Dr. Richard Pazzi	FBIT	Assistant Professor	Data Dissemination, vehicular cloud computing
Dr. Rajen Akalu	FBIT	Assistant Professor	IT Law, Information Privacy

b) Additional academic and non-academic human resources

No new administrative requirements for the new program component is expected.

c) Physical resource requirements

No additional physical resource requirements for the new program is expected. The current expansion to the Hackers Research Lab is sufficient for the delivery of the courses in this new field.

5. BUSINESS PLAN

a) Statement of funding requirements

We expect to accept between 5-10 students in this field for 2018-2019, with the number increasing to a maximum of 15 for 2019-2020. The cost for the program will include the offering of three AI-related courses, which would also be used as electives by the students in the main MITS program.

b) Statements of resource availability

No additional resources are required for the delivery of MITS-AIS field.

6. TIMELINE OF IMPLEMENTATION & TRANSITION PLAN (Include semester of implementation)

- Fall 2018 for the implementation of the proposed field.
- No Transition plan is necessary.

APPROVAL DATES

Curriculum Committee Approval	December 4, 2017
Faculty Council Approval	December 5, 2017
CPRC or GSC Approval	January 30, 2018
Academic Council Approval	
Report to Board of Governors	