ACADEMIC COUNCIL REPORT

SESSION:

Public ☒
Non-Public ☐

ACTION REQUESTED:

Decision ☐
Consultation ☒
Information ☐

TO: **Academic Council**

DATE: **September 24, 2019**

FROM: **Reem Ali, Manager of Technology Enriched Learning – Information Technology Services**

SUBJECT: **PCI Compliance and Information Security Policy Instruments**

ACADEMIC COUNCIL MANDATE:

- Under the Policy Framework, consistent with the "Duty to Consult" under section 10(5) of the UOIT Act, Policy Owners must consult with Academic Council before presenting draft policy instruments to the approval authority for approval.
- We submit this report and drafts of the: 1) Policy on PCI Compliance; 2) Procedures on PCI Compliance; and 3) Policy on Information Security to obtain your feedback on the policy documents before they are presented to the Board for approval.

PURPOSE OF POLICY INSTRUMENT:

1. **Policy on PCI Compliance** - The purpose of this Policy is to establish the foundations required for the University of Ontario institute of Technology to maintain compliance of the Payment Card Industry (PCI) Data Security Standard (DSS), and maintain the integrity of the PCI Cardholder Data Environment.

2. **Procedures for PCI Compliance** - The purpose of these Procedures is to identify the Account Management Requirements for the Compliance with the Payment Card Industry Data Security Standard (PCI DSS Compliance).

3. **Policy on Information Security** – This policy sets out the cornerstone of the university's information security program. It establishes the concept that information is an asset and the property of University of Ontario Institute of Technology. All information technology users are required to protect this asset.

The PCI-DSS is a regulation created by the major credit-card companies that defines the protective controls required by all Merchants who store, process, transmit or have access to any form of cardholder data or sensitive authentication data.

PCI-DSS compliance is a requirement that authorizes Merchants to accept card-based payments.

The information security policy strives to minimize the possibility of information misuse, corruption, and loss through the adoption of reasonable procedures for the University community to follow. It relates to information that is stored electronically as well as paper, microfilm, and video, and the content of confidential meetings and conversations**.**

CONSULTATION:

Date	**Document Name**	**Description of stakeholder/community consultation**	**Comments received and response**
June 25, 2019	Presentation on PCI Compliance	Academic Council	
June 27, 2019	Presentation on PCI Compliance	Policy Advisory Committee.	Members raised questions on training offered to third party members i.e. parents wanting to pay their child's tuition using credit card, admin staff. Explained that the scope of PCI Compliance policy is the receiver of credit card information however training for third parties (i.e. guidelines on how to protect credit card data) can be arranged after policy and procedures are rolled out. Questions were raised about how accountability is ensured with DC providing IT services on behalf of OntarioTech. Clarification was provided that this is explained in service level agreement containing an indemnity

			clause where one party commits to compensate the other of any harm, liability or loss arising out of a contract.
September 3 – 17, 2019	Online Consultation	Review by Online Community	

COMPLIANCE WITH POLICY/LEGISLATION:

- Payment Card Industry (PCI) Data Security Standard (DSS)

NEXT STEPS:

1. Academic Council feedback considered and incorporated, where appropriate.
2. Remaining consultation and approval pathway:
   (a) Administrative Leadership Team (October 16)
   (b) Audit and Finance for deliberation (November 20)
   (c) Board of Governors for approval (November 28)

SUPPORTING REFERENCE MATERIALS:

- PCI Compliance Policy

- PCI Compliance Procedures
- Information Security Policy

Classification Number	
Framework Category	Legal, Compliance & Governance
Approving Authority	Board of Governors
Policy Owner	
Approval Date	
Review Date	
Supersedes	

POLICY TITLE

PCI Sustainability

PURPOSE

1. The purpose of this Policy is to establish the foundations required for the University of Ontario institute of Technology to maintain compliance of the Payment Card Industry (PCI) Data Security Standard (DSS), and maintain the integrity of the PCI Cardholder Data Environment.

DEFINITIONS

For the purposes of this Policy the following definitions apply:

"**Authentication Factor**" means a method used to prove the user of a resource is permitted to use said resource, such as: a password, an authentication token, or a biometric (thumb/retina scanner).
"**Cardholder Data**" means any Personally Identifiable information (PII) associated with a person who has a credit.
"**Cardholder Data Environment"** or "**CDE**" means the segmented area of the network which encompasses applications, hardware, and network services in the transmission, processing, or storing of cardholder data
"**Dual Factor Authentication**" means a method of confirming users' claimed identities by using a combination of *two* different factors.
"**Finance"** means the organization under the direction of the Chief Operations Officer
"**Hardened**" means a secured computer system.
"**Merchants**" means departments, faculties and vendors using payment processing technologies deployed on the University of Ontario Institute of Technology networks, whether employees, students, vendors, contractors or business partners
"**Multi Factor Authentication**" or" **MFA**" means an authentication method to grant access only after successfully presenting two or more pieces of evidence (or factors) to an authentication mechanism.
"**Password**" means the sequence of characters used to confirm the identity of a user or permission to access a resource.
"**PCI DSS**" means the Payment Card Industry Data Security Standard which drives many of the items identified in this policy.
"**PCI Zone**" means anything that is in scope for PCI DSS compliance
"**Role-Based Access Control"** or "**RBCA**" means a system of permissions where access to a specific resource is defined by permissions assigned to specific roles; a role is given to a user based on their position/needs in relation to the organization.
"**Unauthorized Network Equipment**" means unauthorized devices connected to the network that poses a significant risk to the organization.

"**Vulnerabilities**" means a type of weakness in a computer system, in a set of procedures, or in anything that leaves information security exposed to a threat.
"**Workstations**" means a computer dedicated to a user or group of users engaged in business or professional work.

SCOPE AND AUTHORITY

2. This Policy applies to all Merchants using payment processing technologies deployed on the University of Ontario Institute of Technology networks, whether employees, students, vendors, contractors or business partners. Exemptions from this policy will be permitted only if approved in advance and in writing by the Chief Financial Officer (CFO).

3. The Chief Financial Officer (CFO), or successor thereof, is the Policy Owner and is responsible for overseeing the implementation, administration and interpretation of this Policy.

POLICY

4. Finance shall ensure that the following activities are performed

4.1. Ensure that payments taken over the phone leverage the PCI DSS acceptable third-party solution.

4.2. Regularly, and prior to the annual PCI DSS compliance assessment, update inventory of critical PCI related technology such as cash registers and pin pads.

4.3. Maintain a list of Merchants whose products are used to process credit card payments on behalf of the university. Ensure the service providers' PCI DSS compliance is monitored regularly, and prior to the annual assessment.

4.4. Secure written agreements with Merchants that includes an acknowledgement that Merchants will maintain all applicable PCI DSS requirements to the extent the Merchant handles, has access to, or otherwise stores, processes, or transmits the customer's Cardholder Data or sensitive Authentication data, or manages the customer's Cardholder Data Environment on behalf of a customer.

4.5. Ensure there is an established process for engaging PCI related Merchants including proper due diligence prior to engagement.

4.6. Ensure new Merchants wanting to accept credit card information on campus are not allowed to process electronic transactions using the campus network infrastructure. New Merchants should use cellular enabled pin pads for in person transactions wherever possible. Exceptions need approval from the Executive Director of Information Technology Services.

4.7. Ensure that if Cardholder Data is available through remote-access technologies, special precautions must be taken.

4.7.1. Personnel with a valid business need to see Cardholder Data must be authorized by Chief Financial Officer

4.7.2. Copying, moving, or storing Cardholder Data onto local hard drives and removable electronic media is prohibited

5. Finance will ensure that Merchants responsible for PCI account access shall perform the following activities as needed:

5.1. Creating, controlling and managing user accounts that can access the (CDE).

5.1.1. Every user must use a unique user ID and a personal secret Password for access to campus information systems and networks.

5.1.2. User accounts must be created with the lowest required access level appropriate for the user, following the Role-Based Access Control principle.

5.1.3. User privileges are to be reviewed on a regular basis and removed if the privileges are no longer required.

5.1.4. Mechanisms such as tokens, digital certificates, or other means of Multi Factor Authentication may be used in addition to Passwords for the identification and Authentication of users, and must also be unique to each user.

5.1.5. Where possible, users must be forced to change their Password when they first log on to the system.

6. Finance shall ensure the following activities are performed as needed:

6.1. User accounts are only to remain active for the period required for users to fulfill their responsibilities.

6.2. Central IT accounts of staff will be disabled once the staff no longer appear on payroll.

6.3. Password Aging Rule

6.3.1. Administrators who operate their own systems associated with the Cardholder Data Environment (CDE) are responsible for implementing a process to force Aging of Passwords at least every 90 days.

6.4. Merchants processing credit cards shall perform the following activities on a regular basis:

6.4.1. Ensure that they understand the PCI standards

6.4.2. Inspect pin pad devices for signs of tampering or substitution such as broken seals or incorrect serial numbers.

6.4.3. Ensure that credit card information at rest is encrypted if electronic, and physically secured if on paper.

6.4.4. Ensure that Multi Factor Authentication is used to access payment workstations remotely.

7. IT Services shall ensure that the following activities are performed on a regular basis

7.1. Ensure that the network and data flow diagram(s) accurately reflect the network architecture.

7.2. Ensure that the Credit Card Data information in transit is secure and encrypted within the campus infrastructure.

7.3. Review firewall and router rulesets pertaining to the PCI Zone at least every six months

7.4. Regularly, and prior to the annual assessment, update inventory of all CDE locations, hardware / software / applications and networks.

7.5. Update configuration standards as necessary and ensure the Workstations used are Hardened and comply with the PCI Standard.

7.6. Review Vulnerabilities in a timely fashion once the software publisher provides security alerts.

7.7. Install applicable vendor-supplied patches: critical within one month, non-critical within three months for all IT Assets in the CDE.

7.8. Scan for the presence of all Unauthorized Network Equipment in the PCI Zone

7.9. Ensure that Multi Factor Authentication is used to administer or access payment Workstations remotely

7.9.1. All remote-access technologies must be configured to automatically disconnect sessions after 30 minutes of inactivity.

7.9.2. All remote-access technologies and associated accounts used by Merchants to access the CDE must be activated only when needed, with immediate deactivation after use. Activating these remote-access paths and accounts requires submitting a request to the IT Service Desk.

7.10. Engage and manage an Approved Scanning Vendor (ASV) to conduct external vulnerability scanning.

7.11. Review, and update as necessary, the organization's information security related policies, procedures, and standards from a PCI perspective.

8. IT Services shall ensure that the following activities are performed on a regular basis

8.1. Confirm the location(s) of the CDE and flow of Cardholder Data and ensure that they are included in the PCI DSS scope, including backups.

8.2. Review compensating controls to ensure that they are properly documented and are still applicable.

8.3. Conduct a formal threat risk assessment at least annually and upon significant changes to the environment (for example, acquisition, merger, relocation, etc.).

8.4. Run an awareness program for Merchants. Confirm they've read and understand the policy/procedures

MONITORING AND REVIEW

9. This Policy will be reviewed as necessary and at least every three years. The Chief Financial Officer, or successor thereof, is responsible to monitor and review this Policy.

RELEVANT LEGISLATION

10. This section intentionally left blank.

RELATED POLICIES, PROCEDURES & DOCUMENTS

11. Information Security Policy

12. Acceptable Use of Information Technology Policy

13. PCI Sustainability Procedure

Classification Number	
Parent Policy	
Framework Category	Legal, Compliance & Governance
Approving Authority	Board Committee
Policy Owner	
Approval Date	
Review Date	
Supersedes	

PROCEDURE TITLE

PURPOSE

1. The purpose of these Procedures is to identify the Account Management Requirements for the Compliance with the Payment Card Industry Data Security Standard (PCI DSS Compliance).

DEFINITIONS

For the purposes of these Procedures the following definitions apply:

"**Authentication Factor**" means a method used to prove the user of a resource is permitted to use said resource, such as: a password, an authentication token, or a biometric (thumb/retina scanner).
"**Cardholder Data**" means any Personally Identifiable information (PII) associated with a person who has a credit.
"**Cardholder Data Environment"** or "**CDE**" means the segmented area of the network which encompasses applications, hardware, and network services in the transmission, processing, or storing of cardholder data
"**Dual Factor Authentication**" means a method of confirming users' claimed identities by using a combination of *two* different factors.
"**Finance"** means the organization under the direction of the Chief Operations Officer
"**Hardened**" means a secured computer system.
"**Merchants**" means departments, faculties and vendors using payment processing technologies deployed on the University of Ontario Institute of Technology networks, whether employees, students, vendors, contractors or business partners
"**Multi Factor Authentication**" or" **MFA**" means an authentication method to grant access only after successfully presenting two or more pieces of evidence (or factors) to an authentication mechanism.
"**Password**" means the sequence of characters used to confirm the identity of a user or permission to access a resource.
"**PCI DSS**" means the Payment Card Industry Data Security Standard which drives many of the items identified in this policy.
"**PCI Zone**" means anything that is in scope for PCI DSS compliance
"**Role-Based Access Control"** or "**RBCA**" means a system of permissions where access to a specific resource is defined by permissions assigned to specific roles; a role is given to a user based on their position/needs in relation to the organization.
"**Unauthorized Network Equipment**" means unauthorized devices connected to the network that poses a significant risk to the organization.

"**Vulnerabilities**" means a type of weakness in a computer system, in a set of procedures, or in anything that leaves information security exposed to a threat.
"**Workstations**" means a computer dedicated to a user or group of users engaged in business or professional work.

SCOPE AND AUTHORITY

2. This Policy applies to all Merchants using payment processing technologies deployed on the University of Ontario Institute of Technology networks, whether employees, students, vendors, contractors or business partners. Exemptions from this policy will be permitted only if approved in advance and in writing by the Chief Financial Officer (CFO).

3. The Chief Financial Officer (CFO), or successor thereof, is the Policy Owner and is responsible for overseeing the implementation, administration and interpretation of this Policy.

3.1. The CFO is responsible for ensuring that the appropriate policies and procedures are in place to handle credit card data securely and that the critical PCI technology inventory is updated.

3.2. Finance is responsible for keeping a PCI related list of Merchants and ensure that new vendors are not permitted to use the campus network to process payment transactions.

4. Executive Director of Information Technology Services responsible for:

4.1. Ensuring policies regarding PCI Sustainability are carried out; confirming that diagrams, technology inventories, vulnerability list, and policy maintenance is done regularly as dictated by PCI DSS.

4.2. Reviewing, monitoring, and updating compensation controls, security policy, conducting formal risk assessments, running awareness and training programs, and ensuring service provider compliance.

4.3. Aapproval, deployment, and use of critical devices, Multi Factor Authentication implementation, and arranging for the documentation of critical device inventory, configuration of critical devices, and remote access technologies and reviewing firewall and router rule sets.

4.4. Ensuring the running and maintaining anti-virus software and scans, deactivating user accounts (including third-party accounts) as dictated by PCI DSS, internal and external security/vulnerability scans, testing for unauthorized access and access points, and updating CDE location and flow diagrams.

PROCEDURES

5. Authentication

All users of systems in the PCI Zone are required to follow strict password management procedures. In some cases, these requirements will be implemented by the owners of the relevant systems. In others, it will be the responsibility of the user to ensure these procedures are followed. The

procedures below are the bare minimum requirement. If a system has procedures which are more restrictive than those outlined below, continue with the more restrictive procedures.

5.1. Initial Passwords or Password Resets.

a) Passwords for new user accounts or after a password reset must be set to a unique random value.
b) The unique random value password must be changed on first use. If possible, this will be required by the system. If the user is not prompted by the system to modify the password, it is their responsibility to change the password.
c) Users must follow best practices for secure passwords. Examples can be found at http://servicedesk.ot.ca

5.2. Password Aging Rule

a) System owners and administrators are responsible for ensuring users regularly change their passwords. Enforce a password change at least every 90 days.
b) Limit password reuse to the last 6 passwords.

5.3. Multi Factor Authentication

a) In addition to passwords, there will be situations where Multi Factor Authentication is required. The following scenarios require Multi Factor Authentication:
    a. An administrator is accessing the CDE from anywhere other than the server console.
    b. A user is accessing the CDE through a virtual private network tunnel (VPN)
b) Users are required to contact IT services to obtain Multi Factor Authentication access if either of the situations above apply to them.

5.4. Re-Authentication

a) Any time a user steps away from a workstation that has access to the CDE should lock their computer to prevent inadvertent access by another user. At a minimum, screensavers that lock the computer should start after at most 15 minutes of inactivity, requiring re-authentication to access the system.

b) Systems should also have session time-outs, which require a user to re-authenticate.

5.5. PCI Account Access and Management

Managers responsible for PCI account access and management are responsible for:

a) Regularly reviewing accounts.

b) Generate a report that contains the following types of accounts, and remediate as necessary

- Locked accounts
- Disabled accounts
- Accounts with passwords exceeding the maximum age
- Accounts with passwords that never expire
- Accounts that cannot be associated with a business owner

c) Revoking Access

a. User credentials and other authentication methods need to be revoked as soon as possible upon an employee's departure.

b. Upon quarterly review of accounts, inactive accounts must be deactivated (at least every 90 days).

c. Accounts must be locked out after 6 unsuccessful authentication attempts.

5.6. Monitoring Inappropriate Account Usage

a) System owners and administrators are responsible for ensuring that old accounts are not being used.

b) Monitor account usage to identify dormant accounts, and determine appropriate action for those accounts.

c) Monitor any attempts to use deactivated accounts.

MONITORING AND REVIEW

6. These Procedures will be reviewed as necessary and at least every three years (unless another timeframe is required for compliance purposes). The [insert position/committee], or successor thereof, is responsible to monitor and review these Procedures.

RELEVANT LEGISLATION

7. "This section intentionally left blank"

RELATED POLICIES, PROCEDURES & DOCUMENTS

8. PCI Sustainability Policy

9. Information Security Policy

10. Acceptable Use of Information Technology Policy

Classification Number	
Framework Category	Legal, Compliance & Governance
Approving Authority	Board of Governors
Policy Owner	
Approval Date	
Review Date	
Supersedes	

POLICY TITLE

Information Security

PURPOSE

1. This Policy is the cornerstone of the university's information security program. It establishes the concept that information is an asset and the property of University of Ontario Institute of Technology. All information technology users are required to protect this asset.

2. DEFINITIONS

"Information Assets" means any information that is printed or written on paper, stored electronically, transmitted by post or using electronic means, shown on visual media, or spoken in conversation.

"**University Constituents**" means individuals that have an existing relationship with the University, including but not limited to adjunct professors, affiliates, alumni, external contractors, faculty, graduate students, guests, librarians, partners, postdoctoral fellows, retirees, staff, undergraduate students, visiting professors, visitors, and volunteers.

"**Information Owners"** means individuals that have administrative control over the information and has been officially designated as accountable for a specific information asset dataset.

"Information Custodians" is a person who has technical control over an information asset dataset, usually IT Services

"Cardholder Data Environment (CDE)" means the segmented area of the network which encompasses applications, hardware, and network services in the transmission, processing, or storing of cardholder data

SCOPE AND AUTHORITY

3. This Policy applies to:

3.1. All University Constituents who are able to create and share information using University computing resources, and to any person or organization that handles University information and data regardless of their affiliation with or function within the University.

3.2. All information within the custody and control of the University, including the Cardholder Data Environment (CDE). Any activity aimed at the manipulation, transportation or use of information is subject to this policy throughout its life cycle.

4. The Executive Director of Information Technology Services, or successor thereof, is the Policy Owner and is responsible for overseeing the implementation, administration and interpretation of this Policy.

POLICY

5. The University is committed to the security of information, both within the University and in communications with third parties.

6. In securing information, it is essential that the following characteristics of information are preserved and maintained:

6.1. Confidentiality: ensuring that information is accessible only to those authorized to have access;

6.2. Integrity: safeguarding the accuracy and completeness of information and processing methods;

6.3. Availability: ensuring that authorized users will have access to information and associated assets when required.

7. Information security training will be available to all employees at the start of employment, and at least yearly thereafter.

8. Information Owners are responsible for properly classifying information in terms of their confidentiality, integrity and availability.

9. Information Owners and Information Custodians shall work together to ensure adequate access measures are in place to protect information and IT resources from loss or unauthorized access.

10. Information Owners and Information Custodians shall work together to ensure the integrity of information is maintained by protecting against unauthorized modification.

11. Information Owners and Information Custodians shall work together to protect confidential information from unauthorized disclosure.

12. All University Constituents may only have access to the confidential information that is required to perform their roles. They shall protect the confidentiality of the information to which they have access.

13. An IT operational information security incident response procedure must be in place, reviewed and tested.

14. Roles and Responsibilities

14.1. Departmental System Managers are directly responsible for implementing the policy and ensuring staff compliance in their respective departments.

14.2. IT Services shall:

14.2.1. Maintain detection and prevention controls to protect against malicious software and unauthorised access to networks and systems.

14.2.2. Be responsible for creating, updating, and auditing information security plans, policies and procedures on an annual basis.

14.2.3. In cooperation with departmental system managers, administrators and users, be responsible for providing information security training.

14.3. All University Constituents handling University related information or using University information systems shall:

14.3.1. Be required to observe this Policy and these Regulations and are responsible for the consequences of their actions regarding computing security practices

14.3.2. Be in part responsible for protecting University information from unauthorized access, modification, destruction or disclosure.

14.3.3. Report immediately to the IT services any observed or suspected security incidents where a breach of this policy has occurred.

14.4. System administrators are responsible for administering user account authentication and account management.

14.5. The Executive Director IT services is responsible for monitoring and enforcing this policy.

15. Accessibility for Ontarians with Disabilities Act considerations

15.1. Accessibility for Ontarians with Disabilities Act (AODA) standards have been considered in the development of this policy.

16. Consequence of Non-compliance:

16.1. Non-compliance could affect the University's ability to conduct business, respond to requests for information, be transparent and accountable, and ensure confidentiality and privacy of personal information. This would be a risk to the University both financially and to its reputation in the community.

16.2. Failure to comply with this policy could result in loss of access to the University's information technology services and equipment, disciplinary action up to and including suspension or termination of an employee, and/or legal action that could result in criminal or civil proceedings.

MONITORING AND REVIEW

17. This Policy will be reviewed as necessary and at least every three years. The Executive Director Information Technology Services, or successor thereof, is responsible to monitor and review this Policy.

RELEVANT LEGISLATION

18. "This section intentionally left blank".

RELATED POLICIES, PROCEDURES & DOCUMENTS

19. Acceptable use Policy

PCI Sustainability Policy

PCI Sustainability procedure