UNIVERSITÉ Concordia UNIVERSITY

INFORMATION SECURITY POLICY

Effective Date: December 9, 2020	**Approval Authority:** Board of Governors
Supersedes /Amends: N/A	**Policy Number:** VPS-33

PREAMBLE

This Policy is adopted in accordance with the *Directive sur la sécurité de l'information gouvernementale* (section 7) which requires public bodies to adopt and implement a policy on the security of information.

SCOPE

This Policy applies to all Members (as defined below) of the University community and applies with respect to all Information (as defined below) owned, collected, held, transmitted and/or produced by the University or a third party, consultant, supplier or any external partner in whatever format it exists (ex: paper, digital) and for the entire Life-Cycle (as defined below) of the Information.

This Policy has been developed in the context of and co-exists with other policies and regulations of the University, particularly those governing the use of University property and services; Data Governance (as defined below); computer use; privacy; risk management; records management; disciplinary procedures; copyright and intellectual property.

PURPOSE

The purpose of this Policy is to affirm the University's commitment to ensure the security of all Institutional Data and Institutional Information (as such terms are defined below) held by the University, in compliance with applicable laws and regulations. More specifically, the purpose is to ensure appropriate levels of control are in place in support of the availability, accessibility, integrity and confidentiality of the Information, including research data. This Policy also sets out the governance structure and the units and/or teams responsible for ensuring the security of information.

DEFINITIONS

For the purposes of this Policy, the following definitions shall apply:

“Asset(s)” means any physical and/or digital asset which holds, uses, transmits, receives or is related to the Life-Cycle of Information. Assets include, but are not limited to, applications, databases, servers, computers, laptops, phones, cells.

“Assigned Custodian” means the unit or person responsible for an Asset and for ensuring regular reviews of compliance with the present Policy and all applicable guidelines and frameworks.

“Data Governance” means a set of standards and processes relating to data which are followed by all Members of the community and which ensure the accuracy, integrity and accessibility of Information.

“Data Mart” means a subset of a Data Warehouse (as defined below) used by specific Users (as defined below). It holds the data related to a particular subject area such as finance, human resources or students.

“Data Steward(s)” means the individual having responsibility and oversight of an information system, Data Mart or Data Warehouse, and its associated Information.

“Data Trustees” means the administrators with institutional oversight for Information.

“Data Warehouse” means a central repository which serves the purpose of facilitating access to data for decision-making. It holds Institutional Data on multiple subject areas from multiple sources.

“Document(s)” means Information inscribed on a medium. The Information is delimited and structured, according to the medium used, and can be in the form of words, sounds or images. The Information may be rendered using any type of writing, including a system of symbols that may be transcribed into words, sounds, images or another system of symbols. For the purposes of this Policy, a database whose structuring elements allow the creation of documents by delimiting and structuring the Information contained in the database is considered to be a Document.

"Information" means any Institutional Data, Institutional Information and/or Personal Information.

"Information Security Program" refers to projects, training or steps undertaken to remediate any existing information security gaps, address any new threat to security, modify standards and implement processes in order to attain and maintain the desired security level.

"Institutional Data" means any standardized representation or depiction of facts or figures that can be created, collected, processed, communicated or interpreted.

"Institutional Information" means Institutional Data that have been derived, aggregated, processed, organized, structured and presented as a report, dashboard, graphic visualization, Key Performance Indicators (KPIs) or as a corollary database, Data Mart or Data Warehouse.

"Life-Cycle" means all the stages in the creation, use, retention and the destruction of a Document. Such stages include the creation, holding/saving or preserving the Document, transferring, consulting or viewing and the destruction of the Document in accordance with the applicable University rules and laws.

"Member(s)" means any student and any full-time, part-time or temporary employee of the University, including staff, faculty, postdoctoral fellows, researchers, members of the administration, stagiaires, interns and volunteers.

"Personal Information" means information that permits the identification of an individual.

"Supervisor" refers to a person with direct supervisory responsibility over employees of the University.

"User(s)" means any individual (Members, contractors and guests) with access to Information.

<u>POLICY</u>

1. The management of information security must support the University's mission and ensure the University can carry out its mission securely, without interruption, and in conformity with all applicable laws and standards.

Managing information security includes:

a) Developing the organizational skill set to manage information security risk across the University

b) Creating a culture of information security throughout the community and setting out the responsibilities relating to information security of all Members of the community.

c) Securing and protecting all Assets pertaining to information security.

d) Managing access to Information and the responsible use of the systems as set out in the related University policies.

e) Creating and adopting directives, rules, procedures, guidelines and best practices in information security as determined by the Chief Information Officer (CIO) and the Chief Information Security Officer (CISO) and supported by the senior administration, notably in conformity with applicable laws, University policies and other applicable standards.

f) Keeping and making Information in accordance with applicable University policies and procedures, including, but not limited to, the *Records Classification and Retention Plan*, and the *Policy Concerning the Protection of Personal Information* (SG-9), the *Policy on Confidential Information* (HR-36), the *Policy on Computing Facilities* (VPS-30), the *Policy on Data Governance* (PRVPA-4) as well as applicable laws and regulations.

g) Conducting inventories and classification of Information subject to the present Policy.

h) Managing risks, assigning security levels and ensuring that processes are in accordance with the level of risk and the sensitivity of the Information in question.

i) Providing support, information and training relating to information security to the relevant units and Members of the community.

j) Monitoring, auditing and testing the security of the information systems and, when appropriate, reassessing needs, rules and responsibilities.

k) Developing and implementing procedures to detect information security threats and responding swiftly and responsibly to any breach or incident involving information security.

l) Ensuring the appropriate enforcement of this and related University policies and directives.

Roles and Responsibilities

2. Reporting to the Vice-President, Services and Sustainability, the Associate Vice-President, Information Systems and Chief Information Officer (CIO) is responsible for developing University policies, procedures, guidelines and technologies in relation to information security, and participates in the implementation of same University-wide.

3. Reporting to the CIO, the CISO develops and maintains appropriate strategic and operational plans, participates in the implementation of University policies, procedures, guidelines and technologies in relation to information security and liaises with relevant external and internal parties regarding information security matters.

4. The responsible unit, as determined by the CIO and the CISO, may develop procedures, guidelines, handbooks or other University policy-related documents to help with the implementation of this Policy, including, but not limited to:

   a) Cloud usage procedures and guidelines;

   b) Identity and access management, including password management, procedures and guidelines;

   c) Backup management procedures and guidelines;

   d) Bring Your Own Device procedures and guidelines.

5. The Supervisor is responsible for ensuring that employees and others under their supervision are aware of the present Policy and the responsibilities set out herein.

6. Committees and response teams (as described in Appendix A) have been created each with specific responsibilities and mandates relating notably to:

   a) Ensure the security of Information;

   b) Ensure the security of Assets;

   c) Respond to breaches of Personal Information;

   d) Respond to fraud;

   e) Respond to information security incidents.

   Such committees and response teams may, as technology and/or the needs of the University change over time, be modified, added to or abrogated.

7. In alignment with the *Policy on Data Governance* (PRVPA-4) and the related *Data Governance Framework*, Instructional and Information Technology Services (IITS) and Data Stewards will ensure that systems are designed, configured, implemented, operated, maintained, upgraded and decommissioned in a manner consistent with established information security needs.

8. System and application administrators are responsible for configuring the security features of the Assets under their administration in accordance with University policies, procedures, guidelines and other requirements. All Assets with security settings that can be configured and/or changed must have an assigned administrator.

9. Data Trustees are accountable for ensuring that Information is accurate, available to authorized Users and classified in accordance with University policies and guidelines, including the *Policy on Data Governance* (PRVPA-4) and the *Data Governance Framework*.

10. The IITS Security Team and Data Stewards are responsible for ensuring systems are assessed for information security requirements on a regular basis or as mandated by governmental obligations.

11. All Assets (owned by the University or Users) must have an Assigned Custodian who is responsible for ensuring compliance with this Policy.

12. Users are notably responsible for:

    a) Complying with this Policy, all information security requirements defined herein, all other related University policies and supporting procedures, rules, directives and guidelines.

    b) Completing training relating to information security as requested and/or prescribed.

    c) Protecting passwords and accesses provided to them via IITS or system administrators. Access is to be used by the assignee and not provided to any other User.

    d) Taking appropriate measures to prevent loss, damage, abuse or unauthorized access to Assets under their control.

    e) Respecting the established classification of Information.

    f) Promptly reporting all acts that may constitute real or suspected breaches of security including, but not limited to, unauthorized access, theft, system or network intrusions, willful damage, and fraud.

<u>Non-compliance</u>

13. Non-compliance with this Policy may result in a variety of responses including the immediate suspension of a User’s access to any or all systems, termination of access to the University’s information systems and disciplinary action.

Policy Responsibility and Review

14. The overall responsibility for the implementation and recommended amendments to this Policy shall rest with the Vice-President, Services and Sustainability.

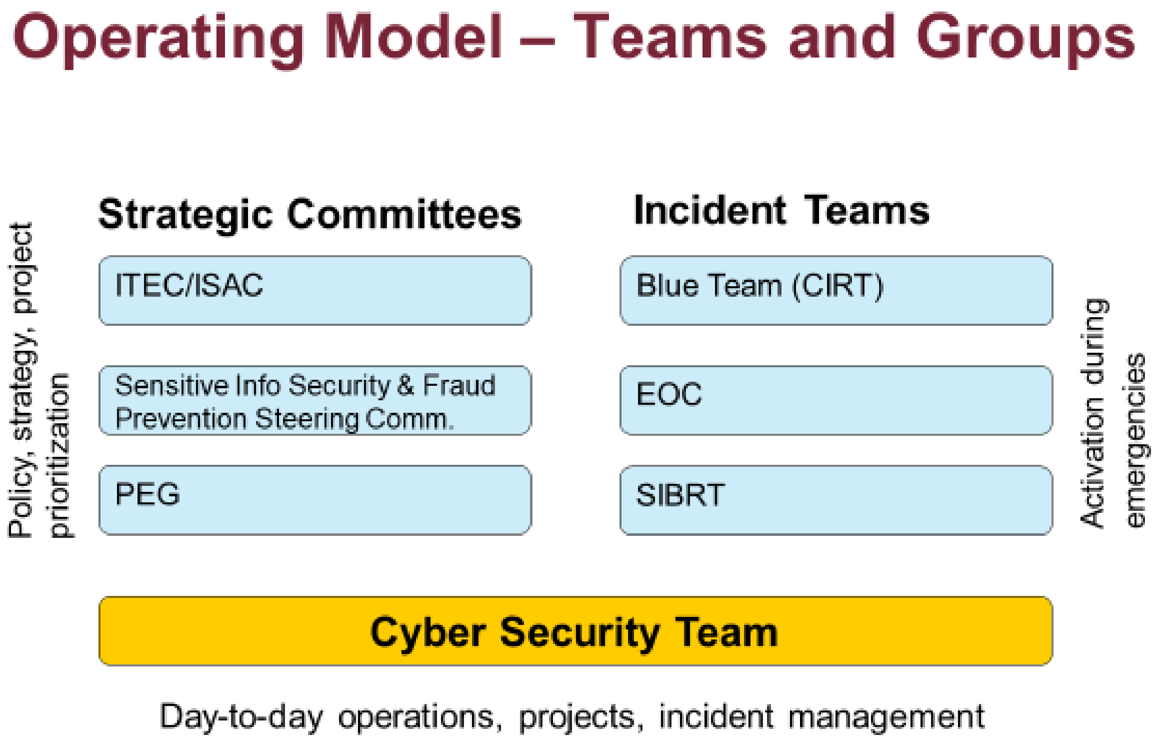
Approved by the Board of Governors on December 9, 2020.

APPENDIX A

Governance Structure

The Associate Vice-President, Information Systems and CIO and the CISO are responsible for coordinating efforts with relevant institutional committees and initiatives.

The information security governance structure is as follows:



Operating Model – Teams and Groups

Policy, strategy, project prioritization

Strategic Committees

ITEC/ISAC

Sensitive Info Security & Fraud Prevention Steering Comm.

PEG

Incident Teams

Blue Team (CIRT)

EOC

SIBRT

Activation during emergencies

Cyber Security Team

Day-to-day operations, projects, incident management

Strategic Committees

1. Information Technology Executive Committee (ITEC)

The mandate of the ITEC is to provide strategic directions relating to information systems and technology as well as to monitor IT performance based on established metrics and to provide recommendations for improvements. The ITEC may also be asked to validate funding requests that are of University-wide importance.

Members of the ITEC are responsible for:

- the review of the overall strategic initiatives related to the Information Security Program and investment roadmap;
- the review of the information security risks to be reported to the Enterprise Risk Management Committee;
- the review of IT policies; and
- providing recommendations to the President's executive group (PEG) and the Board of Governors for required approvals relating to information security.

2. Information Systems Advisory Committee (ISAC)

The mandate of the ISAC is to monitor and optimize the expected outcomes relating to the IT roadmap delivery (business cases and projects), the Asset life-cycle management and IT user services, and to provide recommendations to the ITEC on strategic directions.

Members of the ISAC are responsible for the review of business cases and projects that are part of the Information Security Program and for providing recommendations to the ITEC on strategic directions.

3. Sensitive Information Security and Fraud Prevention Steering Committee

The mandate of the Sensitive Information Security and Fraud Prevention Steering Committee is to ensure proper governance of information security at the University through oversight of the Information Security Program.

Members of the Committee are responsible for:

- the review of the Information Security Program including policies, directives, rules, procedures and best practices.
- the review of major information security incidents and appropriate responses when required.

4. President's Executive Group (PEG)

PEG will be alerted and will participate in a strategic capacity during a major cyber security incident involving a data breach or a severe loss of service. PEG will also review and provide input to policies or directives related to information security.

Incident Teams

5. Blue Team or Computer Incident Response Team (CIRT)

The Blue Team is an incident response team that is assembled during incidents, tabletop exercises and/or mock incidents. The composition of the team is fully technical and draws from IITS resources and other areas as needed. The information security manager or equivalent will liaise with the CISO so that other teams such as the Emergency Operations Committee (EOC) are updated as to the Blue Team's response to an incident.

6. Emergency Operations Committee (EOC)

The EOC is composed of representatives from all major University units and assembles on a regular basis to review emergencies that have occurred on campus. The EOC also assembles to coordinate the response to an active emergency. In a cyber emergency, the EOC would serve as a central point of coordination with all other University units and assist with the response to the emergency.

7. Sensitive Information Breach Response Team (SIBRT)

The SIBRT is activated by the Vice-President, Services and Sustainability or delegate when a sensitive information breach occurs. The SIBRT evaluates the severity and impact of the incident. Should the investigation warrant action, it may call on the EOC for support.

Operational Team

8. Cyber Security Team

The Cyber Security Team is comprised of information security analysts in IITS who have operational duties and project responsibilities related to cyber security. In the event of a cyber security incident, the Cyber Security Team would be part of the Blue Team.

Incident Reporting Procedure

All Users are expected to report confirmed and suspected incidents via the incident report application in the MyConcordia portal. Incidents will then be triaged and treated as per the incident management procedure.