Policy Name:	**Information Technology (IT) Security**
Originating/Responsible Department:	**Information Technology Services (ITS)**
Approval Authority:	**Senior Management Committee**
Date of Original Policy:	**November 2008**
Last Updated:	**December 2021**
Mandatory Revision date:	**December 2022**
Contact:	**AVP (ITS) & Chief Information Officer**

Policy:

To ensure the confidentiality, integrity and availability of information and information systems at the university, security requirements must be in place to secure the confidentiality, integrity and availability of the university's information assets

Purpose:

This policy outlines Carleton University's approach to the security of its information systems. In order to provide proper security to Carleton information systems, controls must be put in place to ensure the secure use and management of information systems. Maintaining proper security of information and information systems are essential for Carleton's compliance with legal and contractual obligations.

Scope:

The policy applies to individuals that support or use Carleton University's information systems. Carleton University's information systems are comprised of:

- The core campus network, departmental networks as well as other networks used by academic and non-academic affiliates of Carleton;
- Computing systems and applications; and
- Information and data processed by these systems and/or applications.

Procedure:

Using a risk management methodology, the university must implement appropriate administrative, technical, and physical security controls to ensure the continued confidentiality, integrity, and availability of information systems. The following section describes the guiding principles for the implementation of these security controls:

- Security controls may be any combination of the following: administrative, technical, or physical;
- Security controls implemented must be appropriate and sufficient to ensure the continued confidentiality, integrity, and availability of the information being processed;
- Network segments comprised of systems with different security requirements must have security controls based on the most sensitive system within that network segment;

- Network zoning must be implemented to ensure that public networks such as the Internet do not directly connect to sensitive information systems but utilize a demilitarized zone and appropriate security technologies;
- The level of security controls placed on different network segments is determined by the classification of information systems within the specific network segment;
- Formalized system/software development life cycle for the development and deployment of information systems;
- Processes are in place to ensure that information systems and their data are secured throughout the information system operational life cycle including commissioning, operation, and decommissioning, including but not limited to:
    - System acceptance processes
    - Change management processes
    - Vulnerability and patch management processes
    - Incident response processes
    - System decommissioning processes
- A risk assessment must be performed to confirm that departmental networks meet the equivalent security requirements as the campus network layer to which it is attached;
- For isolated networks and systems, a Service Level Agreement (SLA) will define what network services and types of connectivity are to be provided by the campus network to the isolated departmental network.

Roles and Responsibilities:

ITS is responsible for:

- Ensuring appropriate network segmentation and zoning is implemented for information systems within their control;
- Ensuring appropriate processes are in place for the secure commissioning, operation, and decommissioning of information systems;
- Implementing security controls that are based on industry best practices and standards;
- Assisting departments and faculties with the identification of required security controls;
- Monitoring for and response to information security incidents on the core network and attached information systems.

Departments that deploy or manage their own IT infrastructure are responsible for:

- Ensuring a risk assessment has been carried out prior to the connection of an information systems to the Carleton University network;
- Ensuring appropriate network segmentation and zoning is implemented for information systems within their control;
- Ensuring appropriate processes are in place for the secure commissioning, operation, and decommissioning of information systems;
- Implementing security controls that are based on industry best practices and standards'
- Monitoring for and response to information security incidents on their departmental network and attached information systems;

- Reporting suspected information security incidents to the Incident Response Steering Committee via ITS.

Users of the Carleton information systems are responsible for:

- Notifying ITS or their local support staff when a vulnerability in the information system has been discovered;
- Using the information systems for their intended purpose only.

Compliance:

Non-compliance to this Policy may result in disciplinary action.

Contacts:

AVP (ITS) & Chief Information Officer

Related Policies:

https://carleton.ca/secretariat/policies/

- Acceptable Use Policy for Information Technology (IT) Policy
- Information Security Policy
- Data and Information Classification and Protection Policy
- Vulnerability Management Policy
- Information Security Incident Response Policy
- Mobile Technology Security Policy
- Remote Network Access Policy

https://carleton.ca/its/about/policies/

- CUNET Domain Membership and Access Policy