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: November 2013
Mandatory Revision Date: November 2018
Contact: Chief Information Officer (CIO)

Policy: Information Technology (IT) Security

Purpose: The purpose of this Policy is to outline Carleton University’s approach to campus-wide IT security for networks, enterprise information assets, and enterprise IT systems. In order to provide proper IT security to the CU network, controls must be put in place to ensure secure and controlled access for system users, and management for systems and network devices. ITS (Information Technology Services) is accountable for enterprise wide IT security across the University.

Scope: The Carleton University (CU) technology environment is comprised of:

- Departmental networks as well as other networks used by academic and non-academic affiliates of Carleton, all connected to a core campus network.
- IT systems and applications.
- Information and data processed by these systems and applications.

The scope of this Policy includes enterprise IT networks, systems, applications, and data. This Policy does not cover departmentally managed information technology.

Procedures:

ITS is accountable for securing the core campus network, enterprise IT systems and information assets. Using risk management methodology, ITS implements appropriate technical, physical, and procedural security controls to ensure the continued confidentiality, integrity, and availability of these resources. The following section describes the guiding principles for the implementation of security controls:

- Following a layered security design approach, the controls should be adequate to ensure operation of the IT in a secure manner.
- Security controls may be technical, procedural, and physical.
- ITS will implement security controls to protect against all networks and systems which do not employ appropriate security controls.
- IT system administration functions will be granted only to a limited number of authorized staff who have a demonstrated understanding of the security issues in administering the University’s IT security policies and standards.
• Security controls implemented within IT networks and systems must be appropriate and sufficient to ensure the continued confidentiality, integrity, and availability of the information being processed. For network segments comprising systems with different security requirements, controls will be based on the most sensitive system in that network segment.

• All connections to the CU network must adhere to established security standards. The level of security control placed on different areas of the CU network is determined by the classification of systems and information that reside in those areas.

• 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.

As necessary, ITS will provide guidance to isolated departmental networks to determine the appropriate security controls to be implemented for connection to both the core campus network and other departmental networks.

Compliance:

The following is a list which includes, but is not limited to, actions that are violations of the IT Security Policy:

• Connecting devices to the network that do not meet security standards.
• Connecting external or isolated departmental networks without appropriate security controls in place.
• Disabling or bypassing IT security controls.
• Utilizing Carleton University’s IT resources to attempt unauthorized access to Carleton’s or another organization’s information.

Carleton University reserves the right to monitor the use of resources provided and/or managed by the University for the purposes of determining adherence to this Policy. Monitoring will be performed in accordance with University privacy policies as well as federal and provincial privacy legislation.

Offenses which are a violation of this Policy, other University policies, or provincial or federal laws are subject to discipline as appropriate, and may result in the restriction of access to computing and network resources. Offenses will be reported to University or law enforcement authorities as appropriate. Complaint processes are outlined in the University Human Rights Policies and Procedures Policy. In addition, disciplinary action may be applicable under other University policies, guidelines, implementing procedures, or collective bargaining agreements.

Contact:  Chief Information Officer, ITS

Links to related Policies:  http://carleton.ca/secretariat/policies/

• Acceptable Use Policy for Information Technology (IT)
• Information Security