Carleton UNIVERSITY
Canada's Capital University

Policy Name:	Information Security
Originating/Responsible Departments:	Information Technology Services (ITS), General Counsel
Approval Authority:	Senior Management Committee
Date of Original Policy:	October 2009
Last Updated:	January 2018
Mandatory Revision Date:	January 2019
Contact:	Chief Information Officer (CIO), General Counsel

Policy:

Carleton University is committed to protecting the University's information assets. This Policy defines the information security requirements for the protection of those assets. It is the responsibility of all employees to manage risk and to safeguard the security and integrity of the University's information assets. Information collected, classified, stored, and processed by Carleton University must be protected using safeguards commensurate with the confidentiality, integrity, and availability requirements of the information.

This Policy deals with information security in general terms and is to be read in conjunction with the information handling and security procedures set out in the following University policies:

- Corporate Records and Archives Policy
- Acceptable Use Policy for Information Technology
- Information Technology (IT) Security Policy
- Mobile Technology Security Policy
- Data and Information Classification and Protection
- Password Policy for Information Systems
- Remote Network Access Policy
- Cloud Computing Policy

This Policy is not incompatible with the principles of academic freedom and the free exchange of ideas that characterise post-secondary institutions; and is not intended to limit or restrict these principles.

Purpose:

The objective of the Policy is to identify the requirements necessary to:

- Prevent unauthorized access to confidential, sensitive or proprietary information without unnecessarily limiting University operations
- Apply security measures commensurate with the information classification
- Ensure that all information systems have owners responsible for defining the sensitivity of information assets and systems

- Ensure that appropriate safeguards are implemented as required by the information owner, and according to the security requirements of the information
- Support the application of both access to information and protection of privacy legislation by ensuring personal information is created, used, maintained and disposed of in an appropriate and legal manner
- Define the principles to which all faculty, staff, researchers, students, visiting scholars, and any authorized third-party agents must adhere when handling information owned by or entrusted to the University in any form

Scope:

This Policy requires consistent application throughout the University by all faculty, staff, researchers, students, visiting scholars, and any authorized third-party agents. This Policy applies to all information whether administrative, academic or research.

The provisions of this Policy extend to all information custodians including third party service providers. Third party agreements must have procurement approved standard language that supports the information security requirements in University policies.

Procedures:

All users of Carleton University information must employ appropriate technical, physical, and operational (procedural) controls to protect the confidentiality, integrity and availability of the University's information assets.

These controls must be implemented in conjunction with records and information management procedures for classification according to business function and scheduling for destruction or retention.

Procedures must be designed in consideration of requirements for, but not limited to:

- Legislative compliance, including freedom of information and protection of privacy legislation, and with the advice of the University's Privacy Office
- Protection of research data that considers the impact of the loss of confidentiality, integrity or availability of the data

Information must be protected in accordance with best practices for continuous security risk management. A risk assessment approach must be used to determine the appropriate mix of technical, physical, and operational security controls to be implemented.

Roles and Responsibilities:

Researchers are responsible for:

- Identifying research data sensitivity
- Implementing appropriate procedures and controls to protect research data and information based on data sensitivity and the impact it could have if data confidentiality, integrity or availability were compromised

Information Users are responsible for:

- Protecting information from unauthorized disclosure or tampering by protecting the information in accordance with its information classification
- Not disclosing or destroying any information except as properly authorized
- Reporting to the Privacy Office any activity that may compromise personal information

Information Owners and Information System Owners are responsible for:

- Protecting assets assigned to their control through compliance with supporting IT security policies, procedures, and standards and through consideration of technical, physical and operational security requirements
- Ensuring personnel are aware of information protection requirements and procedures
- The implementation of practices and procedures in accordance with established policy including the definition of requirements for confidentiality, integrity and availability, and in consultation with the Director of Information Security and the General Counsel
- Assessing risks to information assets and for insuring the continued availability of information to support critical business processes
- Imposing controls on business information to prevent loss of integrity, auditability and control
- Rendering unusable any information scheduled for destruction
- Implementing procedures to designate access to information for those who need such access to perform their assigned role or job function for all confidential information assets including personal, confidential and proprietary information
- Implementing compensating information controls to reduce risk to an acceptable level in the event that a recommended security control cannot be implemented

Information Technology Services is responsible for:

- Ongoing security audits and assessing compliance with security policies
- The development and administration of security policies and procedures for the protection of electronic information assets according to recognized standards or best practices
- The promotion of security awareness for electronic information assets

General Counsel is responsible for:

- Consultation regarding the classification of records and the information they contain according to sensitivity to disclosure, critical importance to institutional operations and the need for archival retention

Privacy Office is responsible for:

- Providing advice so that appropriate controls are in place to meet legislative, policy and contractual requirements
- Reviewing and remediating any suspected privacy breaches

Compliance:

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

Contacts:

Chief Information Officer, ITS
General Counsel

Links to Related Policies:

Secretariat Policies - http://carleton.ca/secretariat/policies/

- Corporate Records and Archives Policy
- Acceptable Use Policy for Information Technology
- Information Technology (IT) Security Policy
- Mobile Technology Security Policy
- Data and Information Classification and Protection
- Password Policy for Information Systems
- Remote Network Access Policy
- Cloud Computing Policy

ITS Policies - https://carleton.ca/its/about-its/policies/

- Glossary of Terms for Information Security

Privacy Policies - http://carleton.ca/privacy/privacy-policies/

- Carleton's Privacy Policies

https://www.ontario.ca/laws/statute/90f31

- (FIPPA) Freedom of Information and Protection of Privacy Act

https://www.ontario.ca/laws/statute/04p03

- (PHIPA) Personal Health Information Protection Act

http://laws-lois.justice.gc.ca/eng/acts/P-8.6/index.html

- (PIPEDA) Personal Information Protection and Electronic Documents Act, Canada