Policy Name:	**Data and Information Classification and Protection**
Originating/Responsible Department:	**Information Technology Services (ITS)**
Approval Authority:	**Senior Management Committee**
Date of Original Policy:	**May 2016**
Last Updated:	**March 2022**
Mandatory Revision Date:	**March 2023**
Contact:	**AVP (ITS) & Chief Information Officer**

Policy Statement:

This policy will outline requirements on the classification and protection of Carleton University information assets.

Purpose:

The purpose of this policy is to establish a framework for classifying, the appropriate handling and the use of University data and information, based on its level of sensitivity, value and criticality to the University as required by the University's Information Security Policy. Classification will aid in determining baseline security controls for the protection and use of data and information to ensure:

a) **The University's statutory, regulatory, legal, contractual, privacy and data protection obligations are met.**
b) **The University's proprietary data and information is kept confidential to the institution as required.**
c) **University Information and data is appropriately available for internal decision making as required.**
d) **Government and regulatory agency reporting are conducted in accordance with any legislative, regulatory, and legal requirements; and**
e) **Appropriate data and information are shared with partner institutions and organizations with necessary safeguards.**

Scope:

This Policy applies to all faculty, staff, researchers, students, visiting scholars, and any authorized third-party agents, that access, process, or store University-owned data, excluding research data. For research data, it is required that researchers manage their data as per funding agency policy and provincial and federal requirements. Where funding agency policy is unavailable to provide guidance, this policy applies in the protection of confidential or sensitive information.

Procedure:

1.0 Data Classification

The classification of data and information helps determine what baseline security controls are appropriate for safeguarding that data. The classification system presented in this Policy is comprised of components that work together to assist faculty members, staff, etc. (the "data owner") in assessing the data to determine the appropriate security controls for use, storage, and destruction.

All University data and information must be classified into one of three sensitivity levels or classifications as soon as possible after the creation or acceptance of ownership by the University. The three levels are:

a) **Sensitive or Confidential**
b) **Internal**
c) **Public**

Appendix I outlines the definitions and examples of each of the three classification levels for information and data.

2.0 Labelling

All data or information in electronic or hardcopy format that is not Public information must be labelled as Confidential, Sensitive, or Internal.

Appendix II outlines the requirements and guidance in labelling data.

3.0 Risk Level Assessment

Data owners must assess the level of risk according to the magnitude of harm and the probability that this harm will occur should the data or information be lost, stolen, or accessed by unauthorized parties.

Appendix III indicates the minimum level of risk relative to the probability and magnitude of harm.

4.0 Collections of Data

Data owners or custodians may wish to assign a single classification to a collection of data that is common in purpose or function. When classifying a collection of data, the most restrictive classification of any of the individual data elements must be used. For example, if a data collection consists of a combination of publicly available information and sensitive or confidential information, the resulting data collection (information) must be classified as Sensitive or Confidential.

Special Considerations:

Under certain circumstances, aggregated data and information may result in a collection that is even more sensitive than any individual element and could result in a classification higher than that of any individual element. For instance, a large collection of internal information could warrant being classified and protected as Confidential. When classifying, consider the overall sensitivity of the aggregated data and information.

Data and information may be compiled in aggregate form where groups of individual elements are replaced with summary statistics on those elements. For example, while an individual's age would be considered confidential information, the average age of students at the university would be considered public information.

There may be standards and guidelines that pertain to specific data collections that outline guidance for the classification of specific data or information collections. Such standards and guidelines, where they exist, may assist with the classification exercise.

5.0 Data Safeguards

Departments are responsible for implementing appropriate managerial, operational, physical, and technical controls for access to, use of, transmission of, and disposal of Carleton University data and information (print and electronic) in compliance with this Policy, as well as developing the appropriate labeling procedures to fit them. Sensitive/Confidential data and information requires the highest level of protection. This Policy provides examples of safeguards; however, departments may implement procedures more restrictive than the ones identified in this Policy.

General safeguards for all data and information consist of the following:

- **Once classified, University data or information may only be reclassified with a proper assessment that takes into consideration change in usage, sensitivities, law, or other relevant circumstance.**
- **Any physical or logical collection of data, stored, or during electronic transfer (e.g., file, database, in "the Cloud", emails and attachments, filing cabinet, backup media, electronic memory devices, sensitive operation logs or configuration files) containing differing classification levels must be classified at the highest data classification level within the collection or higher if necessary.**
- **Destruction of data and information (electronic or physical) or systems storing data when the data or information is no longer required for the original intended purpose in accordance with University policies.**

Appendix IV include examples (non-exhaustive) of the kind of data and information that could be classified in each Information Category and at each Risk Level.

6.0 Data Reclassification

When there is a change in classification of data or information by another party: e.g., supervisor, department head, Research Ethics Board, etc., that change must be documented with the reason for the reclassification.

Roles and Responsibilities:

All members of the Carleton University community have a responsibility to protect the confidentiality, integrity, and availability of data and information generated, accessed, modified, transmitted, stored, or used by the University, irrespective of the medium on which the data resides and regardless of format:
e.g., electronic, paper, or other.

ITS is responsible for:

- **Ensuring that users are adequately informed and aware of their responsibilities for protecting confidential/sensitive data and information.**
- **Ensuring that controls are designed and put in place to safeguard confidential/sensitive data and information.**
- **Maintaining standards for the secure destruction of data and information; and**
- **Enforcing technical, physical, and procedural security standards to protect confidential/sensitive data and information.**

The Carleton University Privacy Office is responsible for:

- **Ensuring compliance with University policies and applicable privacy and data protection laws.**
- **Managing the Data Protection Risk Assessment (DPRA) report process.**

Department Chairs, Directors and management in all departments are responsible for:

- **Appropriate use of data and information.**
- **Good data and information management; and**
- **Authorizing access to sensitive or confidential and internal data and information.**

Compliance:

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

Contacts:

AVP (ITS) & Chief Information Officer

Links to related Policies:

- **Information Security Policy**
- **Access to Information and Privacy Policy**
- **Corporate Records and Archives Policy**
- **Risk Management Policy**
- **Canadian Centre for Cyber Security - https://cyber.gc.ca/en/guidance/it-media-sanitization-itsp40006 (Provides guidance on media sanitization based on sensitivity of information)**

Appendix I

1.0 Classifying Your Data

All University data and information must be classified into one of three sensitivity levels or classifications as soon as possible after the creation or acceptance of ownership by the University.

Information Category	Definition	Examples (non-exhaustive)
Sensitive or Confidential	• Any information protected by government legislation (i.e. Ontario Freedom of Information and Protection of Privacy Act (FIPPA), Personal Health Information Protection Act (PHIPA), etc.) • Any information that is contractually protected as confidential by law or by contract. • Any other information that is considered by the University as appropriate for confidential treatment including unreleased financial information and intellectual property. • Sensitive/confidential information requires the highest level of security controls with varying degrees of access control. • Unauthorized information disclosure could result in a significant level of risk to an individual, the University, or affiliates, and cause serious financial impact or damage to the reputation of the University, or affiliates.	• Personally Identifiable Information (PII) – any information about an individual that can be used to distinguish or trace their identity, such as name, date and place of birth, social insurance number, credit card number, etc., which if lost, compromised, or disclosed without authorization, could result in harm to that individual. • Student education records that are directly related to prior, current, and prospective University students and maintained by Carleton University, such as student's name, address, degrees, and awards, subject to certain requirements as specified in FIPPA and University privacy policies. • Human resources information such as salary and employee benefits information. • Results of Threat and Risk Assessments, Information System Vulnerability Assessments and Penetration Tests.
Internal	• Any information that is proprietary or produced only for use by members of the University community who have a legitimate purpose to access such data. • Internal information requires a reasonable level of security controls with a varying degree of access control.	• Internal operating procedures and operational manuals. • Internal memoranda, emails, reports, and other documents. • Technical documents, such as system configurations and floor plans.
Public	• Any information that may or must be made available to the general public, with no legal restriction on its access or use. • While little or no controls are required	• General access data on Carleton.ca. • University financial statements and other published reports. • Copyright materials that are publicly available.

Appendix II

2.0 Labelling Your Data

All data and information in electronic or hardcopy format that is not Public information must be labelled as Confidential, Sensitive, or Internal.

Information Category	Labelling Requirement
Sensitive or Confidential	• Individual documents with multiple pages are to have the classification clearly identifiable on each separate page. Example is in the footer of a standard office document. • Where a standard footer is not possible, electronic documents must have the classification clearly visible. • Emails containing this classification of information must have a classification statement as the first statement of the email. • In instances where there is not a traditional "electronic document" or communications mechanism, all reasonable measures must be taken to make the classification of the information known.
Internal	• Individual documents with multiple pages are to have the classification clearly identifiable on each separate page. Example is in the footer of a standard office document. • Where a standard footer is not possible, electronic documents must have the classification clearly visible. • If not labelled, day-to-day business communications are to be assumed to be Internal unless released.
Public	• There are no specific labelling requirements.

Appendix III

3.0 Risk Level Assessment

The following table indicates the minimum level of risk relative to the probability and magnitude of harm should the confidentiality, integrity or availability of the data or information be compromised. This applies to all types of data and information except research data.

PROBABILITY OF HARM		MAGNITUDE OF HARM		
		MINIMAL	**MODERATE**	**SUBSTANTIAL**
	SUBSTANTIAL	**MEDIUM RISK**	**HIGH RISK**	**HIGH RISK**
	MODERATE	**LOW RISK**	**MEDIUM RISK**	**HIGH RISK**
	MINIMAL	**LOW RISK**	**LOW RISK**	**MEDIUM RISK**

A designation of Low Risk should only be used for instances where the magnitude and probability of potential harm is no greater than that which could reasonably be expected to encountered in day-to-day business operations.

Examples

The following table provides examples of data and how a risk level is calculated from the table above:

Information	**Probability Of Harm**	**Magnitude Of Harm**	**Resulting Risk Level**
Confidentiality of an individual's objectives and annual performance review (completed performance review document) is compromised	**MINIMAL**	**MINIMAL**	**LOW RISK**
Identified data or information about a highly controversial topic that could put participants at risk if released; SIN numbers, medical, criminal, sexual or employment history.	**SUBSTANTIAL**	**SUBSTANTIAL**	**HIGH RISK**
The integrity of payroll information is compromised resulting in an employee not being paid	**MODERATE**	**MODERATE**	**MEDIUM RISK**

Appendix IV

4.0 Data and Information Safeguards

Data and Information safeguards are determined based on the classification identified in Appendix I and the risk level identified in Appendix III.

Table 4A and 4B include examples (non-exhaustive) of the kind of data that could be classified in each Information Category and at each Risk Level; and is coded to indicate the appropriate Security Level for that data or information. Please note that each colour-coded cell in Table 4A has a security level associated with it that can be used to look up the corresponding storage, transmission and destruction requirements in Table 4B

Table 4A

	LOW RISK	MEDIUM RISK	HIGH RISK
SENSITIVE or CONFIDENTIAL		Identified data about a highly sensitive topic that could cause embarrassment/ psychological harm if released; student records including grades, opinion material, examples of work. **(S-III)**	Identified data about a highly controversial topic that could put participants at risk if released; SIN numbers, medical, criminal, sexual or employment history. **(S-III)**
INTERNAL		De-identified data which would be difficult, though not impossible, to re-identify/link; information shared in a group that is of a moderately personal nature. **(S-II)**	Individual voice or video recordings that, even if not highly sensitive in content, would be impractical or impossible to replace if lost or destroyed. **(S-III)**
PUBLIC	Business contact information; information on public record. **(S-I)**	Information shared in a group that is of a non-personal nature, where the expectation of privacy of the participants is low. **(S-I)**	Compiled information from many public sources from which would be time-consuming or costly to re-compile if lost or destroyed. **(S-II)**

The following table indicates the appropriate safeguards for the storage, transmission, and destruction of data and information based on its designated Security Level (S-I, S-II, S-III) previously identified in Table 4A.

Table 4B

Security Level	Storage (Holding of data and information in either electronic or hard copy format)	Transmission (Transfer of data and information, usually refers to electronic format)	Destruction (Eradication of data and information so it may not be recovered)
LEVEL 3 (S-III)	• Electronic files and/or data must be stored on a University- sponsored shared directory or stationary device (i.e. desktop computer or server) with controlled physical access and role based logical access controls. • Electronic files and/or data must be encrypted when stored on portable or insecure devices. • Confidential or sensitive information shared with third parties must use file-based encryption. • Data must not be stored in a "cloud" environment unless hosted by Carleton University or supported by suitable agreements. • Portable or insecure devices must be stored in a secure location when not in use. • Hardcopy files must be stored in a locked office or file cabinet with controlled access.	• Data must only be transmitted via a secure network. • Data traversing an untrusted (insecure) network must incorporate industry standard cryptography. • Transmission via fax machine or telephone must have limited access and only those authorized can view/hear.	• Electronic files and/or data and media must be degaussed (magnetic information wiped) or rendered unreadable by other means[1]. • Devices may be physically destroyed. • Hardcopy files must be cross-cut shredded. • Data must be retained according to public record requirements. • There must be an appropriate recovery plan in place.
LEVEL 2 (S-II)	• Electronic files and/or data must be stored on a University- sponsored shared directory with controlled physical access and role based logical access controls. • Electronic files and/or data must be encrypted when stored on portable or insecure devices. Data must not be stored in a "cloud" environment unless hosted by Carleton University or supported by suitable agreements. • Portable or insecure devices must be stored in a secure location (i.e. where access is limited) when not in use. • Hardcopy files must be stored in a locked office or file cabinet.	• Data must only be transmitted via a secure network. • Data traversing an untrusted (insecure) network must incorporate industry standard cryptography. • Transmission via fax machine or telephone must have limited access and only those authorized can view/hear.	• Must be destroyed when no longer needed in accordance with University policies. • Electronic files and/or data must be formally removed and media must be rendered unreadable[2]. • Hardcopy files must be cross-cut shredded.
LEVEL 1 (S-I)	• No security controls required for data storage or transmission.		• Files may be recycled or deleted

[1] The Communications Security Establishment provides Information Technology Security Guidance on Media Sanitization provides guidance for the sanitization of sensitive information.
[2] The Communications Security Establishment provides Information Technology Security Guidance on Media Sanitization provides guidance for the sanitization of sensitive information.