Policy Name:	Data Protection and Risk Management Policy
Originating/Responsible Department:	Office of the General Counsel
Approval Authority:	Senior Management Committee (SMC)
Date of Original Policy:	November 2023
Last Updated:	November 2023
Mandatory Revision Date:	November 2028
Contact:	Manager, Privacy and Access to Information

Purpose:

The purpose of this Policy is to define the requirements for classifying and protecting the university's physical and digital data assets in order to mitigate information security risks. The confidentiality, integrity and availability of the university's data and information must be preserved when stored, processed, or transmitted through software, systems and processes. Any information security and data protection risk to the university must be evaluated to determine if the risk can be avoided, accepted, mitigated or transferred.

Scope:

This Policy applies to anyone that uses, accesses, or connects to university records or managed software, systems, processes and data.

Interpretation:

1. This Policy shall read in conjunction with other policies that may, in certain circumstances, govern data protection and risk management matters, including collective agreements, IT and information security policies, and records management policies and procedures.
2. This Policy shall be read in conjunction with any directives, guidelines and procedures that are established concerning data protection.

Policy:

Establishing a framework for classifying the appropriate handling and use of university records, data and information, based on its level of sensitivity, value and criticality to the university is mandatory. 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 applicable legal requirements; and
e. Appropriate data and information are shared with partner institutions and organizations with the necessary safeguards.

Procedures:

1. Data and Information Classification Requirements

a) University data and information assets must be classified to ensure their

confidentiality, integrity and availability.

b) The university has established a Data and Information Classification Framework in Schedule 1 to determine the appropriate handling and the use of university data and information, based on its level of sensitivity, value and criticality to the University.
c) Data Custodians are responsible for classifying and securing information as per the Framework in Schedule 1 of this Policy.

2. Cloud Computing Security Requirements

a) The confidentiality, integrity and availability of the university's data and information must be preserved when stored, processed, or transmitted through the use of a third-party cloud computing provider, regardless of the financial cost of the service.
b) The use of external cloud computing resources presents risks that must be understood and considered in the selection of cloud computing providers. Risks include but are not limited to the:
    - Loss of information confidentiality and potential reputational damage to the university; e.g., data breaches;
    - Non-compliance with federal and provincial privacy legislation, regulation and guidelines;
    - Cloud computing providers' unilateral change of their terms of service;
    - Loss of information; e.g. disappearance of cloud provider, with no adequate backup of service or data;
    - Loss of information ownership;
    - Unavailability of information; e.g. Denial of Service;
    - Loss of control over information; e.g. information stored using non-university cloud accounts;
    - Inability to investigate the change in integrity, confidentiality or availability of the service or information;
    - Inability to satisfy timely information requests for legal, investigatory or compliance purposes;
    - Hijacking of cloud computing account or service;
    - Inability of the university to control information access controls;
    - The ability to repatriate data and/or ensure proper data disposition at the end of an engagement; and
    - The imposition of legal or regulatory compliance requirements in conflict with Carleton legal, regulatory or policy requirements.
c) The university has established minimum administrative, physical and technical requirements for university data and information being processed, stored, or transmitted by cloud computing services, to ensure risks to the University are identified and appropriately managed.
d) Schedule 2 – Cloud Computing Security Requirements in this Policy identifies the processes and procedures to be followed for the acquisition and implementation of third-party cloud computing services.
e) Data custodians and users must undertake a Data Protection Risk Assessment as set out in Schedule 2 prior to using a third-party cloud computing provider.
f) Data custodians and users must enter into a formal written agreement containing appropriate safeguards with any third-party cloud computing provider prior to using their services.
g) The Data Protection Risk Assessment process and a written acceptance of any residual risk must be completed before university data can be stored or processed in

the cloud.

3. Incident Response

a) The university must respond to, and handle information security incidents in a timely manner to limit the potential impact to its information assets, legal liability, and reputation.
b) The university has established the requirements for responding to information security incidents that threaten the confidentiality, integrity, and availability of the university's data and information technology assets. The requirements outline the responsibilities of the university community in respect of reporting and managing incidents.
c) The university has established the Cyber Incident Response Steering Committee and related Terms of Reference.
d) 'Schedule 3 – Incident Response Framework' identifies the processes and procedures related to managing incident response activities for incidents involving university data and information assets.

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 IT systems and associated data;
- For maintaining a cyber security program;
- Collaborating with other institutions and government institutions in cyber security initiatives, including sharing confidential/sensitive data and information related to IT security incidents within data sharing agreements;
- 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 in compliance with corporate records retention and disposition scheduling; 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; and
- Managing the Data Protection Risk Assessment (DPRA) report process.

The Corporate Archivist is responsible for:

- Advising on retention and disposition of data associated with records retention and disposition scheduling in the Carleton University Retention Schedule (CURS); and
- Collaborating with stakeholders and custodians to update and document retention and disposition changes covered by CURS.

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.

Contacts:

Director, Information Security, ITS
Manager, Privacy & Access to Information
Corporate Archivist, Corporate Records and Archives

Schedules:

- Schedule 1 – Data and Information Classification Framework
- Schedule 2 – Cloud Computing Security Requirements (Non-technical)
- Schedule 3 – Incident Response Framework

Links to related Policies:

This Policy is intended to outline the university's requirements for classifying and protecting the university's physical and digital data assets and should be read in conjunction with other applicable university policies, guidelines or standards, including but not limited to:

- Access to Information and Privacy
- Administrative Data Collection, Access and Usage
- Corporate Records and Archives
- Acceptable Use of Information Technology and Email
- Information Technology Procurement
- University Information Technology (IT) Security
- Electronic Monitoring

Schedule 1 – Data and Information Classification Framework

1.0 Data Classification

The classification of data and information helps determine what minimum 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.

The creator/acceptor of data and information is responsible for classification/reclassification as outlined in this policy.

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/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 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/Sensitive. 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 required by data aggregation.
- 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.

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/ 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 • Detailed information related to IT security controls.
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/ 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 (e.g. watermark). • 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 (e.g. watermark). • 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
The integrity of payroll information is compromised resulting in an employee not being paid	MODERATE	MODERATE	MEDIUM 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

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/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 CCCS approved 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]. • Media or storage 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 CCCS approved 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 Canadian Centre for Cyber Security provides Information Technology Security Guidance on Media Sanitization provides guidance for the sanitization of sensitive information.
2 The Canadian Centre for Cyber Security provides Information Technology Security Guidance on Media Sanitization provides guidance for the sanitization of sensitive information.

Schedule 2 – Cloud Computing Security Requirements

Agreements with External Providers

Formal agreements with third parties where internal or confidential/sensitive information are involved are required to ensure these services are provided in compliance with university policies and applicable privacy legislation. This applies also to the personal information exchanged with third parties for the purposes of service provisioning.

These agreements and their implementation must include the following requirements on the use of cloud computing for the storage, processing, or transmission of university data assets:

- Clear confidentiality, integrity and availability requirements including the treatment of internal, confidential and sensitive information.
- Employee security awareness and training.
- Limitations on information collection, use and disclosure.
- Information ownership must remain solely with the University.
- Vulnerability management requirements including periodic vulnerability assessments and penetration testing.
- Suitability requirements on the third party, including the provision of independent audits and audit attestations on information security controls.
- Provisions governing the return and destruction of information in the third party's possession in compliance with the university Corporate Records and Archives Policy.
- Provisions on the protection of information in accordance with the Ontario's *Freedom of Information and Protection of Privacy Act* (FIPPA) and *Personal Health Information Protection Act* (PHIPA) and their associated formal request for information requirements.
- Provisions on the protection of information in accordance with *FIPPA, PHIPA and* PIPEDA, as applicable.
- If necessary, provisions on the limitation of use of contact information in accordance with Canada's Anti-Spam Legislation and Carleton's Anti-Spam Compliance Policy.
- Information Security incident response, management and notification requirements.
- Limits and requirements on subcontracting.
- When credit card data is involved, the requirement to demonstrate ongoing compliance as a service provider to the Payment Card Industry Data Security Standard (PCI DSS).
- Appropriate Cyber liability insurance, liability and indemnification provisions and cyber incident notification.

Data Protection Risk Assessments

Where any internal, confidential, or sensitive information is involved, Data Protection Risk Assessments must be performed prior to the exchange of information, awarding of a contract and implementation of services. Assessments must be conducted by the ITS Security Governance team and the University's Privacy Office.

Standards, Compliance, and Reliability

Service providers housing data considered internal, confidential, or sensitive under Carleton's Data and Information Classification and Protection policy are required to provide evidence of data center certification against acceptable industry standards (i.e., NIST, HECVAT, SAS 70

Type II, SSAE 16, SOC 1, SOC 2, SOC 3, or ISO) which are appropriate in the circumstances. Likewise, if a service provider's role is deemed critical to university operations, its data center must be at least Tier 3 according to the industry recognized Data Center Tier Classification Standard which categorize Data Center reliability.

Schedule 3 – Incident Response Framework

Procedure:

Reporting
Anyone using or accessing university information technology services or resources must report suspected information security incidents to the ITS Service Desk in a timely manner. Examples of potential incidents include:

- Malicious activity;
- Events which impact Payment Card Industry (PCI) compliance;
- Ineffective security controls;
- Breach of information confidentiality, integrity or availability expectations;
- Non-compliance with policies or guidelines;
- Breaches of physical security arrangements of IT systems or IT equipment rooms;
- Uncontrolled system changes;
- Malfunctions of software or hardware; and/or
- Access violations.

Malfunctions or other anomalous system behaviour may be an indicator of a cyber event or an actual cyber security breach, and should therefore be reported as an information security incident.

Identification of Incidents
Information security incidents must be categorized based on their severity and impact on the university's operations by ITS Information Security.

Incident response process
The university must maintain and follow detailed procedures for responding to suspected information security incidents. The ITS Incident Response Procedures document must be available to staff involved in incident response and must be reviewed annually.

Institutional Decision Capability
The impact and risk to the university will be assessed and triaged procedurally by the Director – Information Security or designate. The assessment will include provisions and criteria for engaging the university's institutional decision capability and crisis management process.

Documentation
Information security incidents must be fully documented. Detailed tracking of each step taken to resolve the incident will include specific and relevant dates, times actions taken, by whom, and the outcomes of each action. Supporting artifacts such as logfiles must also be preserved as part of the incident record.

Communication
The Incident Response Team will communicate details of the incident to appropriate community members based upon the "need to know" principle and will maintain open, effective communications for the duration of the information security incident. Indicators of compromise (IoC) and threat actor tactics and techniques may be shared within shared intelligence agreements.

Training

Members of the university's Cyber Incident Steering Committee and teams responsible for cyber incident response will conduct practice security incident exercises to maintain their awareness of current processes and procedures. These exercises must be conducted annually.

Cyber Incident Steering Committee

The Incident Response Team consists of the following members:

- Associate Vice-President (Information Technology Services) and Chief Information Officer (Chair)
- Director of Information Security
- Executive Director of Risk and Insurance
- Privacy and Access to Information Manager
- General Counsel
- Associate Vice President (Communications and Public Affairs) or their designate
- Assistant Director – Strategic Initiatives and Communications, OVPFA
- Other subject matter or data custodians as may be appropriate in the circumstances of the incident response