Policy Name:	University Information Security
Originating/Responsible Department:	Information Technology Services (ITS)
Approval Authority:	Senior Management Committee
Date of Original Policy:	November 2008
Last Updated:	November 2023
Mandatory Revision Date:	November 2028
Contact:	Associate Vice-President Information Technology Services and Chief Information Officer

---

Policy Statement:
To ensure the confidentiality, integrity and availability of information and information systems at the university, security requirements must be in place to secure the university's information assets. Carleton University is committed to protecting the university's information assets. This Policy defines the information security and information technology 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, or on behalf of, Carleton University must be protected using safeguards commensurate with the confidentiality, integrity, and availability requirements of the information.

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

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

- Prevent unauthorized access to confidential, sensitive, or proprietary information, including personal 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 privacy and data protection 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:
The policy applies to all individuals, including but not limited to faculty, staff, researchers, students, visiting scholars, visitors and any authorized third-party agents that support or use Carleton University's information systems.

Carleton University's information systems include, but are not limited to:

- The core campus network, departmental networks as well as other networks used by academic and non-academic affiliates of the university;
- Computing systems and applications purchased by the university;
- IT services, including cloud computing and IT services provided on behalf of the university;
- Information and data processed by these systems and/or applications.

Interpretation

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

Procedure:

All users of Carleton University information systems 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 a manner that supports the Data Protection and Risk Management policy and the Corporate Records and Archives policy. Information must be protected in accordance with best practices for continuous security risk management.

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;
- A formal plan for managing the system/software development life cycle;
- 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
    - Records creation, retention and disposition processes

    - Identification and retention of permanent archival records

- A risk assessment must be performed by appropriate departmental IT personnel 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) with ITS will define what network services and types of connectivity are to be provided by the campus network to the isolated departmental network.

- Protection of research data plan that considers the impact of the loss of confidentiality, integrity, or availability of the data.

- Legislative compliance plan, including consideration of privacy and data protection legislation, developed in collaboration with the university's Privacy Office.

- ITS Information Security may implement network restrictions for any device or network segment that reduces the security posture of other IT systems or services to an unacceptable level.

- ITS Information Security may remove user account access and/or terminate all network connections for any account that is believed to be compromised or performing activities that contravenes the Acceptable Use of IT and Email policy.

- In the event of a cyber incident that poses an immediate threat to the confidentiality, integrity or availability of university IT infrastructure or systems, the CIO, in consultation with the Vice-President (Finance and Administration) and the Director of Information Security or their delegate, may take reasonable actions to protect the institution's systems and data.

- Agreements with providers for IT services or equipment must have procurement approved standard contractual language that supports the information security requirements in university policies including but not limited to appropriate Cyber liability insurance, liability and indemnification provisions, cyber incident notification and adhere to the IT Procurement policy.

Specific Information Security Requirements

A. User Device Security Requirements

Schedule A sets out the authorized methods for protecting confidential and personal information processed, accessed and stored. The University will ensure that appropriate safeguards are in place and maintained, in order to protect sensitive University data being processed, accessed and stored on user device technologies and to comply with legal, regulatory and contractual obligations.

B. Password Requirements

Passwords are a critical part of information and network security at Carleton University. Poorly chosen and stale passwords, if compromised, may result in unauthorized disclosure, modification or destruction of university information assets. To mitigate this risk, unique user accounts with strong, secure passwords are required at all times as set out in **Schedule B**. In any scenario where password controls cannot comply with established password standards; e.g.; due to technology limitations, the risk must be mitigated through appropriate compensating controls.

C. Remote Network Access Requirements

Carleton University requires that remote access to non-public, confidential and/or administrative data of the on-campus network use necessary safeguards to protect the confidentiality, integrity and availability

of the data. **Schedule C** defines the standards for connecting to any campus network or system from an off-campus location. These standards are intended to minimize the risk of damage to Carleton including unauthorized use, loss of data, disclosure of intellectual property, damage to public image, to internal systems, or any other undesired consequence.

Roles and Responsibilities:

Information Technology Services (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, including consultation with Corporate Records and Archives on system retention and disposition requirements.
- 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 responding to information security incidents on the core network and attached information systems.
- Ongoing IT security verification 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 and training on security awareness for electronic information assets.

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 system 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, including consultation with Corporate Records and Archives on records retention and disposition requirements.
- Implementing security controls that are based on industry best practices and standards.
- Monitoring for and responding to information security incidents on their departmental network and attached information systems.
- Providing information and coordinating activities in response to information security incidents with ITS and other IT units.
- Preserving system audit information for forensic analysis.
- Reporting suspected information security incidents to the Cyber Incident Steering Committee via ITS.

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 as outlined in the Data

Protection and Risk Management policy.
- Not disclosing or destroying any information except as properly authorized.
- Reporting to the Privacy Office any activity that may compromise personal information.
- 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.

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.
- Ensuring personnel are aware of retention and disposition requirements and procedures that support information protection.
- Implementing 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 ensuring 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 if a recommended security control cannot be implemented.

Corporate Records and Archives 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 appropriate retention and disposition of records and archives.

Privacy Office is responsible for:

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

Compliance:

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

Contacts:
AVP (ITS) & Chief Information Officer

Related Policies:

This Policy is intended to outline the University's information security requirements and should be read in conjunction with other applicable University policies, guidelines or standards, including but not limited to

- Access to Information and Privacy Policy

- Corporate Records and Archives Policy
- Acceptable Use of IT and Email Policy
- Data Protection and Risk Management Policy
- Information Technology Procurement Policy
- Electronic Monitoring Policy

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

Schedule A: User Device Requirements

Computers (PCs, Tablets, Laptops, Notebooks, Netbooks)

Portable computers must employ safeguards that protect information being stored or processed from the unique threats of mobility. Portable computers must employ logical security controls for the purpose of protecting sensitive data in the event that the device is lost. These security controls include:

- Firewall software;
- Enterprise antivirus;
- Automated security patch management;
- User authentication to gain access to portable computers must enforce the use of passwords that comply with ITS password standards;
- Disk encryption.

Computers must be physically secured when unattended; e.g.; locking the computer in a secure area or using a locking cable.

When off campus, computers meeting the requirements outlined in this policy may access the Carleton University network using Virtual Private Network (VPN) services with Multi-factor Authentication (MFA).

Users of computers may store sensitive data only for the duration of a valid business justification for doing so. Users must ensure that sensitive data is removed from devices in a secure manner when it is no longer needed. Due to the potential for accidental loss, the use of local storage media is discouraged. Instead, it is recommended that network drives or services including Microsoft Teams, OneDrive or ShareFile be used to store sensitive data.

Official university records stored on computers must be treated in compliance with the Corporate Records and Archives Policy and follow the retention guidelines established in the Carleton University Retention Schedule.

University owned computers must be disposed of through ITS Hardware Services. In accordance with the Information Technology Procurement Policy, ITS Hardware Services ensures that all data is securely erased from portable computers prior to disposal.

Portable Storage Media

Due to the potential for accidental loss, the use of portable storage media is discouraged. Instead, it is recommended that network drives or services including Microsoft Teams, OneDrive and ShareFile be used to store sensitive data. Occasionally, circumstances arise where portable storage media must be used. The following controls must be observed when using portable storage media:

- Sensitive data stored on removable media and storage devices must always be under continuous care and control of the user, or locked in a secure area.

- Only use a secure portable media for storage of sensitive data – secure media includes devices such as USB thumb drives and hard drives that employ encryption to protect data in the event that the device is lost or stolen.
- Only store sensitive data on mobile devices for the duration in which there is a valid business justification for doing so.
- Ensure that sensitive data is removed from devices when it is no longer needed.
- Portable data storage devices must be managed in accordance with the highest level of information sensitivity of any individual data element. The level of information security handling cannot be reduced even if the data is deleted from the device.

Smartphones and Tablets

There are a wide variety of smartphones and tablet computers that can be used to process and store data. The following controls must be observed by users when using smartphones and tablet computers to process sensitive university data:

- Smartphones and tablets must require authentication to access data on the device.
- Only store sensitive data on mobile devices for the duration of a valid business justification for doing so.
- Access to sensitive information owned by or entrusted to the University must not be divulged to unauthorized individuals.
- When storing sensitive data on removable media, the removable media must employ encryption.
- Ensure that sensitive data is removed from smartphones and tablets when it is no longer needed.
- Never use unsecure networks/technologies; e.g.; SMS, instant messaging, email and messaging apps to transmit sensitive data.
- In the event that a university owned smartphone or tablet device is lost, report it immediately to ITS Service Desk.

Screen Locking

For all computer devices that have human input and displays (portable and desktop computers, smartphones and tablets, etc.) a screen locking mechanism must be enforced upon 15 minutes of non-usage/idle time that requires re-authentication to access data on the device. Exceptions to this policy may be granted where there is an explicit need (e.g.: displays used for monitoring purposes)

Schedule B: Password Requirements

Password requirements are grouped into three categories:

- Regular (non-privileged) accounts.
- Privileged accounts that have elevated privileges or are used in automated system processes (e.g.: Administrator, System level, Service Accounts, Root).
- Accounts used on IT systems that are in-scope for the Payment Card Industry Data Security Standard.
- Password standards are confidential and are held in the ITS Internal Network

For all passwords, the following are common requirements:

Parameter	Standard
Complexity	• At least 1 lowercase character • At least 1 uppercase character • At least 1 numeric character • At least 1 special character *All four of these standards must be met
Parameter	**Standard**
Prohibited content	• Password must not contain account ID, email, words found in common dictionaries
Password history	• No reuse of last 10 passwords
Change Frequency	• Permitted once per day *common practice to subvert the policy and get back to the current password is multiple changes in one day
Incorrect password entries before lockout	• After 5 incorrect password entries within 20 minutes, the user will be locked out of the account

Note: Identities must be verified before any authentication credential can be reset.

Passwords for first-time use (temporary) and upon reset must be set to a unique value for each user, and changed immediately after the first use.

Regular Accounts

In addition to the common requirements identified above, the following additional requirements exist for IT system passwords for regular, non-privileged accounts:

Parameter	Standard
Length	• At least 8 characters in length
Password change frequency	• Must be changed every 120 days

Privileged Accounts

In addition to the common requirements identified in the section above, the following requirements pertain to:

- System accounts or services accounts used to facilitate IT system functions; e.g.; batch processes, system tasks, etc., and not associated with an individual
- Accounts with elevated privileges (root level, administrator level, backup operator, etc.)

Parameter	Standard
Length	• At least 15 characters in length
Password change frequency	• Must be changed every 120 days • Not required for *automated* system or service accounts

Accounts and Passwords for Systems In-Scope for PCI DSS Compliance

The Payment Card Industry Data Security Standard (PCI DSS) specifies compliance requirements for all systems and supporting infrastructure that process, store or transmit credit card information. In addition to the requirements in the section above, the following PCI DSS specific requirements exist:

Parameter	Standard
Length	• At least 12 characters in length
Password change frequency	• Must be changed every 90 days

In the event that other forms of authentication mechanisms are employed, those mechanisms must be assigned to the individual account for which it was created and not shared among multiple accounts.

Account Uniqueness

Non-system accounts must be unique and identifiable as belonging to a specific individual. Documented processes must exist to ensure the identity of individuals is confirmed before granting credentials. This applies to the entire University community including guests, visitors and vendors.

The only established exception to this statement is for the provisioning of temporary wireless access to support University business. Provisioning of wireless network services may be established conditional upon the following requirements:

- The wireless service is being provisioned on behalf of a staff or faculty member of Carleton University.
- The requesting staff or faculty member assumes responsibility for the use of the wireless service for the duration of the service in accordance with the University's Acceptable Use of Information Technology and Email Policy.
- The duration of the service does not exceed 5 business days.
- The wireless service uses a unique Service Set Identifier (SSID) and password that is associated with the staff or faculty member.

Password Protection Requirements

Protection of the confidentiality of passwords is crucial to securing confidential and sensitive information on IT assets. To ensure password protection:

- Support staff must never request user passwords.
- Passwords must be treated as confidential/sensitive information.
- If someone demands your password, refer them to this Policy or have them contact the relevant IT Department; e.g., ITS.

- The use of group and shared IDs and/or passwords or other shared authentication methods are prohibited without a strong and valid business justification.
- Wireless passwords or passphrases are not to be shared except as noted above.
- Passwords are not to be transmitted or stored in insecure manners such as via “post-it-notes”, e-mail or unencrypted network services (eg: file transfer protocol (ftp)).
- Industry standard encryption must be used for electronic storage and transmission.
- Physical security controls must restrict access to hardcopy records of passwords.
- Passwords used to gain access to university systems must not be used as passwords to access non-university accounts or information or personal log-ins.

If an individual suspects that their password has been compromised, it must be reported to ITS or the appropriate IT group and the password must be changed immediately.

Schedule C: Remote Network Access Requirements

A Virtual Private Network (VPN) provides secure access to a remote network. Accessing the Carleton network via a VPN connection places your computer or device on the network as if it was directly connected while on-campus. As such, this reduces various risks to the confidentiality, integrity and availability of the information and services that Carleton provides. The requirements to offer and use VPN services at Carleton include:

- ITS provides a centrally supported VPN service; when this central VPN cannot satisfy a departments specific needs then an approved departmental VPN service may be used.
- Computers used for remote access must have an up-to-date endpoint security solution installed and activated as well as firewall protection (hardware or software based). Remote Access solutions must use an industry standard IPSEC or SSL/TLS VPN solution, using strong encryption and centralized user authentication.
- Unique credentials and Multi-factor Authentication (MFA) are required for each VPN user.
- Processes and procedures must be in place to ensure user provisioning and de-provisioning exists and is aligned to Human Resources termination and retirement procedures.
- Authentication systems must offload logs to a central logging server and retain the logs.
- Remote access servers must offload logs to a central logging server and retain the logs.
- Remote access sessions must force a re-authentication of the user to the VPN service at least every 8 hours.
- Remote access technologies used by vendors requires the use of multi-factor authentication and are activated only when needed, and are deactivated immediately after use.
- Usernames and passwords for remote access must not be shared with anyone (including family members) for any purpose – University staff will NEVER ask you to disclose your username or password.
- All University relevant policies normally adhered to when on-campus shall also be adhered to while off-campus while using a VPN.
- Client VPNs must not store the password portion of VPN credentials, requiring the user to enter their password each time the VPN is established.
- Carleton VPN will only be used for accessing IT resources of the university.

Additional Payment Card Industry Data Security Standards (PCI DSS) Requirements:

For IT infrastructure that is within the scope of PCI DSS compliance requirements, the following are also required:

- Sessions for remote access technologies will be automatically disconnected after 15 minutes of inactivity.
- Remote access technologies used by third parties must only be activated when needed, and must be deactivated immediately after use.
- Remote access must use ITS approved multi-factor authentication.

- It is strictly prohibited to copy, move or store cardholder data onto local hard drives and removable electronic media when accessing such data by remote access technologies