Carleton UNIVERSITY
Canada's Capital University

Policy Name:	Mobile Technology Security
Originating/Responsible Department:	Information Technology Services (ITS)
Approval Authority:	Senior Management Committee
Date of Original Policy:	November 2014
Last Updated:	November 2019
Mandatory Revision Date:	November 2024
Contact:	AVP (ITS) & Chief Information Officer

Policy:
To ensure the confidentiality, integrity and availability of information and information systems at the University, information security requirements must be placed on the use of mobile technology within the operations of the University.

Purpose:
The purpose of this Policy is to define the authorized methods for protecting confidential and personal information processed, accessed and stored on mobile technologies. 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 mobile technologies and to comply with legal and contractual obligations.

Scope:
This Policy states the security controls that must be observed during the processing, accessing or storage of sensitive University data for any of the following mobile technologies:

- Portable computers; e.g.; laptops, notebooks, netbooks
- Portable storage media; e.g.; USB storage devices, flash memory cards, CD/DVD ROM
- Mobile devices; e.g.; cellular smartphones, tablet computers

Procedures:
Management of Faculty and Staff Mobile Technologies
Mobile technologies must meet the security standards outlined in this Policy. The University provides enterprise technologies; e.g.; CUNET infrastructure, to manage and enforce the implementation of the security standards for some mobile technologies. Where technically feasible, these enterprise technologies must be leveraged.

Some faculty and staff use mobile technologies that are not owned or managed by the University, known as Bring Your Own Device (BYOD). In these cases, the owner of the device must ensure that appropriate safeguards in accordance with this Policy are employed to protect sensitive data.

Portable Computers (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

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

When off campus, portable computers may access Carleton University network using Virtual Private Network (VPN) services in accordance with the ITS Remote Network Access Policy.

Users of portable 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.

Official university records stored on portable 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 portable computers must be disposed of through ITS Hardware Services. In accordance with the Desktop and Notebook Computer Equipment 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 cuCollab, Microsoft Teams and OneDrive 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

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 BlackBerry PIN-to-PIN, to transmit sensitive data
- In the event that a University owned smartphone or tablet device is lost, report it immediately to ITS Service Desk to have the device remotely wiped

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 (ex: displays used for monitoring purposes)

Roles and Responsibilities

When using mobile devices to access, process, or store University data, users are responsible for:

- Ensuring that sensitive information is secured from unauthorized disclosure through continuous care and control by the user, or stored in a physically secure area
- Ensuring that safeguards and protection mechanisms intended to protect data on mobile technologies are not tampered with or modified
- Reporting suspected privacy breaches to the Privacy Office
- Reporting immediately the loss or theft of a mobile device to ITS Service Desk

ITS is responsible for:

- Ensuring that users are adequately informed and aware of their responsibilities for protecting sensitive data
- Promoting the awareness of security risks associated with processing and storing data on mobile devices
- Ensuring that controls are designed and put in place to safeguard sensitive data
- Developing standards for the secure destruction of data
- Enforcing technical, physical, and procedural security standards to protect sensitive data
- Wiping lost mobile devices that have been issued by them, or any mobile device including BYOD that is connected to the Microsoft Exchange server

The Carleton University Privacy Office is responsible for:

- Ensuring compliance with University policies and applicable laws governing the protection of sensitive data; e.g.; FIPPA

University Secretariat (Corporate Archives) is responsible for:

- Advising users on retention guidelines for university records, including the transfer of permanent records to the Corporate Archives.

Department Chairs, Directors and Management in all Departments are responsible for:

- Collecting university-owned mobile technologies upon the departure of an employee from the University, and ensuring that these devices are returned to ITS Service Desk
- Ensuring that University-owned mobile devices that were upgraded are returned to ITS Service Desk

Human Resources is responsible for:

- Reporting employee departures to ITS to ensure that corporate and Bring Your Own Device (BYOD) access to University infrastructure is disabled

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

Contacts:
AVP (ITS) & Chief Information Officer

Links to Related Policies:
- Acceptable Use Policy for Information Technology
- Password Policy for Information Systems
- Data and Information Classification and Protection
- Desktop and Notebook Computer Equipment
- Remote Network Access
- Access to Information and Privacy Policy