Purpose

The purpose of this Policy is to ensure that personal information, personal health information and other sensitive information in the University’s custody or control is properly safeguarded from those not entitled to have access as well as protecting University systems from the introduction of malicious software. Information contained on portable storage devices (PSD) is subject to the same policies and laws as other University information. However, because of their size and portability they are easily lost or stolen and therefore present increased privacy and security risks when sensitive or personal information is stored on the device.

Security of Personal Information (PI) and Personal Health Information (PHI)

Personal information and personal health information are both classified as “Confidential” under the UTS Information Classification Matrix Policy Statement.

All University employees must ensure that PI/PHI in the University’s custody or control is protected against theft, loss and unauthorised use or disclosure and ensure that the records containing the information are protected against unauthorised copying, modification or disposal.

Minimum guidelines when using a mobile device.

- PI/PHI should not be stored on mobile devices. However, in the event that there is no alternative to local storage, all such information must be encrypted using approved encryption techniques and/or password protected.
- PI/PHI must not be transmitted via wireless communication to or from a mobile device unless approved wireless transmission protocols along with approved encryption techniques are utilised.
- All remote access to McMaster University information resources must use an approved communication mechanism.
• All mobile devices must have approved virus and spy ware detection/protection software along with personal firewall protection (where applicable).

User Responsibilities and Procedures

Password-protect your Mobile Device:
Physical security is a major concern for mobile devices, which tend to be small and easily lost or misplaced. If your mobile device is lost or stolen, a device password may be all that stands in the way of someone reading your E-mail or PI/PHI of another individual(s).

• Choose a strong password. Strong login passwords are comprised of at least eight characters with 14 or more being ideal. These should include a combination of upper and lower case letters, numbers and symbols. DO Not use passwords that are predictable i.e. Birthday.

Verify Encryption Mechanisms:
Any PI/PHI must be encrypted. On its own, password protection is not sufficient should the mobile device become lost or stolen.

Protect your passwords and encryption key by:
• Not writing them down or storing them on the device
• Not using the same password to log into your computer and to unlock encrypted files.

Enable Auto Lock Feature:
Enable the automatic lock feature of your device after five minutes or less of idle time.

Use Antivirus Software:
If you have PI/PHI on your mobile device then at a minimum you should have personal firewall, anti-virus and anti-spyware programs that are up-to-date with the latest security patches.

Storage:
Portable storage devices should be used for the temporary storage of information only and must not be used as permanent document repositories to store University information. Confidential data or personal information contained on portable storage devices may only be a copy of data stored on a secure University system.

Data Erasure and Disposal of PSDs:
Confidential and personal data held on PSDs must be erased sufficiently to prevent information recovery using tools normally available on the university system. Simple deletion or erasure of the files or reformattting does not clear the portable storage device, because commands such as undelete or un-format may permit the recovery of the information. Contact University Technology Services for additional information

Promptly Report a Lost or Stolen Device:
If your mobile device has been lost or stolen promptly report this to the McMaster University Security Services. Additionally, advise the Privacy Officer if the device has any PI/PHI on it.
Storage Case:
Ensure that the case does not bear any visible identification of the University. Include an “if found, return by calling [phone number]” card inside the case with no other identifying information.

Related Documents:
Policy for Handling of Personal Health Information
Policy for Handling of Personal Information
UTS Information Classification Matrix Policy Statement
Information and Privacy Commission – Fact Sheet on Health-Care Requirement for Strong Encryption
Information Privacy Commissioner - Safeguarding Privacy in a Mobile Workplace
Privacy Breach Protocol