imits

Information Management / Information Technology Services

One person. One record. Better health.

Data Encryption Guideline

PREAMBLE

Encryption enhances the security of information by scrambling it and then making it legible only to authorized, authenticated users.

Encryption can be applied to USB keys, hard drives, specific files and mobile devices.

This guideline provides recommendations for options and best practices with encryption.

ENCRYPTION STRENGTH, SETTINGS & SPECIFICATIONS (the techy stuff)

Strength

Use AES-256 bit encryption for USB keys, hard drives, specific files and mobile devices.
Where AES-256 is not available, AES-128 bit is the next best alternative.

USB key Compliance

A USB key should be TAA-compliant and adhere to FIPS 140-2 Level 2
https://en.wikipedia.org/wiki/FIPS_140-2

Other USB Key Configuration-settings

Enable data erasure after 10 failed login attempts
Ensure complex password strength is enforced

USB KEYS - Encryption Ready

The recommended device for Organization provided (IMITS/BCCSS) computers at VCH, PHC & PHSA is the Kingston IronKey D300.

The D300 can be purchased through the IMITS Service Catalogue on POD

Please note that computers provided through the organization (IMITS/BCCSS) are secured in such a way that only certain USB keys will work.

For use with non-Organization provided (IMITS/BCCSS) computers:
(These are FIPS 140-2 compliant)

- Kingston DataTraveler 4000G2
- Kingston IronKey D300
- Kingston Ironkey S1000
- Kanguru Defender Elite300
- Apricorn Aegis Secure Key

INTERNAL HARD DRIVE ENCRYPTION (IMITS/BCCSS issued Desktops and Laptops)

The hard drives of all Windows 7 and 10 computers issued by the organization (IMITS/BCCSS) are encrypted by default using software called Bitlocker.

Bitlocker is bundled free with the Windows 7 and 10 operating systems.

Most Windows XP computers will be configured with encryption software called PointSec.

If you are uncertain about whether or not your windows XP computer hard drive is encrypted please contact the Service Desk for assistance. By providing the Service Desk your hardware number they can verify the encryption status of your device.

INTERNAL HARD DRIVE ENCRYPTION (BYOD / non organization issued devices)

Windows 7 and 10:
Use Bitlocker. It is bundled with the operating system.
A guide on how to configure Bitlocker:
https://www.beencrypted.com/how-to-encrypt-your-hard-drive/

Windows XP:
Use PointSec
Inquire with the Service Desk

MAC OS X:
Use FileVault. It is bundled with the Operating System.
A guide on how to use FileVault: http://support.apple.com/kb/HT4790

EXTERNAL USB HARD DRIVE ENCRYPTION (BYOD / non organization issued devices)

- Axcrypt (Windows)
- Veracrypt (Windows & MAC)

MOBILE DEVICE (Ipads, phones, etc.)

Most mobile devices offer encryption options within the “settings”.
On Apple devices enabling a passcode will automatically enable encryption.
For Android such as Samsung, Acer and others we recommend visiting the manufacturer’s web site for details on how to enable encryption.

FILE ENCRYPTION

- Winzip
  Winzip can be purchased through the IMITS Service Catalogue on POD
- 7zip
- MS-Word for encrypting Word documents
- Adobe Acrobat for encrypting PDF documents

PASSWORDS

Create a Complex Password:

- Passwords must contain a minimum of 8 characters.
- If the device does not have the automatic wipe feature, a minimum of 12 characters is recommended.
- Passwords must use a minimum of 3 of the following: upper case letters, lower case letters, numbers, special characters e.g. !,$,&,*

Secure Password Suggestions:

- Create a password that is difficult to guess. Avoid using your name or birth date.
- Put your passwords in context using a meaningful phrase. Consider lyrics from your favourite song, a favourite saying, a movie title.
- Modify your phrase by removing spaces and replacing vowels with numbers or special characters. E.g. replace the letter ‘O’ with zero or replace an ‘A’ with ‘@’.
  Sample Phrase: I like to move it!
  Sample Password: Ilike2m0veit!
- Memorize your password and protect it! Always keep the password separate from your device.