Encryption FAQ

Updated: February 5/19

Do I need it?

There are several compelling reasons why you may want to encrypt portable computing devices such as laptops. The information contained on the laptop may require protection under legislation such as the Personal Health Information Protection Act (PHIPA), the Freedom of Information and Protection of Privacy Act (FIPPA), or as required by industry practices such as the Payment Card Industry Data Protection standard (PCI). Under these acts and standards, the University is **obligated** to make sure that sensitive data you control is protected against accidental disclosure.

Data properly protected by encryption is considered safe if the laptop is lost or stolen. If not, then you are required to disclose that this sensitive data has been compromised. A lost device which contains 'personally identifiable data' may require **notification** of any affected individuals and may result in an investigation and fines (refer to University Secretariat Access and Privacy web pages). Most importantly, data privacy breaches generally result in negative press coverage that can damage the reputation of the institution.

There is other sensitive data that may not necessarily be covered under legislative requirements, but their accidental exposure may also result in unwanted media coverage or require notification of all the individuals involved. Research contracts, performance reviews, budgets, personal records, passwords, banking accounts, intellectual properties, etc., all may be exposed due to a stolen or lost laptop or storage device. The extra effort to protect this data by encrypting it is something each individual (and their manager) should consider.

How is Data Classified?

In 2017, CCS Information Security introduced the Data Storage Guidelines. This document provides four data classifications along with examples of each type along with the acceptable storage locations and additional considerations including encryption. More detail is available in existing policies/guidelines such as the Research Data Classification Guideline

How does it work?

Full disk encryption protects all data on an encrypted computer not just selected files or folders. Encryption software takes all of the data on a hard drive and then scrambles it so that it can only be accessed with a private key.

Our centrally managed encryption service makes use of your operating system's native encryption – BitLocker for Windows, and FileVault for macOS.

Windows systems will make use of the following solutions:

- Active Directory to escrow Bitlocker Recovery Keys
- System Center Configuration Manager for encryption reporting and monitoring
- Central Active Directory (CFS) to set the encryption policies

Windows systems must meet the following criteria to be considered encrypted with the central encryption service:

- OS must be Windows 10 Professional or above
- Be bound (joined) to the Central Active Directory (CFS)
- Computer name follows the standard naming convention when joining computers to the Central Active Directory
- Hardware must have a working Trusted Protection Module (TPM) chip
- Hardware BIOS must be password protected and have UEFI and SecureBoot enabled

Some Windows systems come with Bitlocker pre-enabled. These systems have the encryption cipher level set at 128-bit. This level does not meet the University encryption standard. In order to remediate this, the system will need to be decrypted and then re-encrypted at the 256-bit encryption cipher level. The central group policy set by Active Directory will ensure that the proper cipher level is set.

Apple macOS systems will use the following:

- JAMF Pro to escrow FileVault Recovery Keys, set the appropriate encryption policies, and for encryption reporting and monitoring

Apple macOS systems must meet the following criteria to be considered encrypted with the central encryption service:

- macOS version must be current and supported by Apple (generally the most recent three macOS versions)

In all cases, once the system is encrypted, there is no difference in how the systems looks or operates for end users and there should be minimal performance impact.

Who supplies the software?

Support for the Central Encryption Service is provided by CCS Managed Desktops. When you apply for the encryption service, you will be put into contact with your local departmental IT admin who will work CCS Managed Desktops to ensure encryption is setup correctly on your computer.

What is key escrow?

The University of Guelph's CIO has approved an enterprise encryption policy that requires the passwords to decrypt data be stored at a secure central location. This is called key escrow and it means that there is always an option to be able to recover the data in cases where the password was forgotten or the individual is unavailable due to accident, etc. Without this protection, critical data would effectively be lost since only the password key can unlock the data once it is encrypted.

Who pays for the service?

CCS is funding the cost for encrypting sensitive data. There is no cost to departments for the use of this service.

Where do I get help?

If you have any issues with the encryption service, you should contact your local IT support technician or the CCS Help Desk at ext. 58888 for assistance. It is also recommended that you make a backup of your data before configuring encryption on your system.

How do I apply?

Contact your local departmental IT admin and they will initiate the process of applying for the encryption service.

What impact will it have on my computer?

There is a very small overhead on your personal computer as encryption translates the encrypted data being read off the disk. This is typically 4-5% and is not noticeable on modern systems. Once the system has booted, the only indication that there is an encryption program running will be a small lock icon on the drive in Windows Explorer for Windows systems and "Filevault is turned on for the disk" for macOS systems in the Security & Privacy applet in Systems Preferences.

Can I protect USB drives and DVDs?

CCS offers a centrally managed USB solution for users that need to transport sensitive data. This solution does have a cost associated with it. More information on the program can be found here.

Bitlocker and FileVault can also be used to encrypted external drives such as USB keys, etc. There are similar policies available for these drives on both Windows and MAC systems.

What systems can be protected?

CCS has solutions for all versions of Windows and macOS.

Can my data be seen by the encryption service?

The only data that is stored centrally is the encryption key. None of your data resides anywhere other than on your computer.

How do I un-encrypt my disk?

If you no longer need to protect your system, then contact then contact your local IT support contact and they can liaise with Managed Desktops and Information Security to have encryption removed.