

Encryption FAQ

Updated: June 20/2018

Encryption FAQ.....	1
Do I need it?.....	1
How is Data Classified?.....	2
How does it work?	2
Who supplies the software?	2
What is key escrow?	3
Who pays for the service?.....	3
Where do I get help?.....	3
How do I apply?.....	3
What impact will it have on my computer?	3
Can I protect USB drives and DVDs?	3
What systems can be protected?	4
Can my data be seen by the encryption service?	4
How do I un-encrypt my disk?.....	4

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 laptop, 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 (where possible) – [BitLocker](#) for Windows, and [FileVault](#) for macOS.

Windows systems will make use of a software package called WinMagic [SecureDoc](#). This software is necessary to manage the encryption, centrally store keys, and monitor the status of encryption for audit purposes.

Older Windows systems, ones that do not support BitLocker, or systems that do not have the necessary hardware will require a different SecureDoc package. In this model, the program is installed on the boot sector of the hard drive and when the system is started, you are prompted for the password in order for the system to start running and for the data to become available. Without this password, the data will remain inaccessible.

Systems running macOS have historically used WinMagic SecureDoc, however beginning in 2018, management of encryption on new Mac systems will use [JAMF Pro](#) instead. This change will simplify the support for encrypted Macs and improve the ability to keep systems updated.

In all cases, once the system is encrypted, there is no difference in how the systems looks or operates.

Who supplies the software?

The server and support for the product are maintained 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 install the software on your machine.

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 the installation.

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 the encryption software 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 icon located on the toolbar. Clicking on the icon brings you a menu of options.

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](#).

SecureDoc also provides an option that allow for portable media such as USB drives, CDs and DVDs to be encrypted. The data on these devices is encrypted in the same way that the hard drive is encrypted, but you can use a separate password to protect this data. The software also allows for you to install a small program that allows those who don't have SecureDoc to be able to read and modify the data, provided they know

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 laptop. Once every 5 hours, your system will automatically contact the server briefly to check for any updates.

How do I un-encrypt my disk?

The implementation of encryption here at the University of Guelph doesn't allow for un-encryption as part of its default configuration. 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 the software removed.