Encryption FAQ

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 does it work?**

The University of Guelph uses a software package from WinMagic called SecureDoc. This program takes all of the data on the hard drive and scrambles it so that only their program along with a password is able to read it. 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. This is called **full disk encryption** and protects all the data on the laptop, not just selected files or folders. Once the system is running, there is no difference in how the systems looks or operates.

**Who supplies the software?**

The software is provided through an agreement between the University of Guelph and WinMagic. The service uses the **Software as a Service** (SaaS) delivery model where the server and support for the product are maintained by WinMagic at their Mississauga office. When you apply for the encryption service, you are given a link to their site that allows you to download their software as well as detailed instructions on how to install and use the product.

**What is key escrow?**

The University of Guelph’s **Office of the CIO** has approved an enterprise **encryption policy** that requires the passwords to decrypt data be stored at a secure central location (WinMagic Corporation in our case). 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?**

The **Office of the CIO** is funding the cost for encrypting data that is covered under legislative requirements such as PHIPA, FIPPA and others. The cost is currently $10 per month for each laptop that is being protected. Where someone with other types of data wants to take advantage of the protection of encryption, but where it is not legally required, their unit will need to cover the costs.

**Where do I get help?**
The agreement with WinMagic provides full support for installation and usage issues with the SecureDoc product. After our office initiates the set-up process, you (or your authorized technical support person) can contact WinMagic at 1-888-879-5879, ext 1. During the installation process, users are asked to perform a chkdsk and defragmentation of the hard drives in preparation for the software install.

If you have any issues with these two items, 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?**

The application form for the service can be downloaded from the Portfolio Management Office web site. Once the form has been completed, it should be sent to the attention of Aileen Cameron, CIO/PMO Upper Vehicle Services/CCS building via email (aileenc@uoguelph.ca), fax (519-767-1620), or campus mail.

**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?**

The SecureDoc software provides options 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?**

The SecureDoc software will work with all versions of Windows and supports Macs and Linux.

**Which Version should I encrypt my Mac with?**

There are currently two options for encrypting Macs, SecureDoc for Mac and SecureDoc for FileVault. FileVault is the native encryption engine that comes built into OS X and if
you are running OS X 10.8 or above then we recommend you use SecureDoc for FileVault. Anything less and 10.8 and you will have to use SecureDoc for Mac.

**Can my data be seen by the encryption service?**

The only data that is stored with WinMagic is the encryption password as well as the answers to challenge questions that were set up during the installation. None of your data resides anywhere other than on your laptop. Once every 5 hours, your system will automatically contact WinMagic briefly to check for any updates.

**What is an admin account used for?**

Those who have departmental support staff who look after their laptop will need an additional account for the SecureDoc application. This account is given to the technical support staff and allows them to access your system using a separate password from yours. This provides them with access to the system in order to do patches, install new applications, etc. If you don’t have a local technical support person, there is no need for this additional account.

**How do I un-encrypt my disk?**

The implementation of SecureDoc 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 the Portfolio Management Office (Gerrit Bos or Aileen Cameron) at ext. 58006. A new account will be sent to your computer that will allow you to uninstall the software.