UNIVERSITY OF TORONTO
FACULTY OF MEDICINE

Request for Local Document Storage

In the course of standardizing the configuration of personal computers at the Faculty of Medicine, an issue that comes up with some regularity is that of network vs. local document storage. While each user and department is free to make their own decisions about how they manage the work documents they create or have responsibility for, there are certain guidelines that IT staff at the Faculty of Medicine must adhere to that may limit their ability to configure their computing environment exactly the way it was before the upgrade. This document is intended to explain those guidelines.

When the Faculty invested in Exchange in 2007, we also set up an enterprise-grade network file server, with terabytes of available storage space. Since that time, our standard configuration for all users is to store their confidential work files on the M drive, and their shared files on their department's N drive. This configuration has a long list of benefits, which include:

- Makes repairs, upgrades, and replacements much faster and safer
- Ensures that all of the Faculty's important / confidential documents are backed up
- Allows for any configuration of internal file sharing, within or between departments
- Makes our document storage FIPPA compliant re. Personal Information (PI)

As part of the current Windows/Office upgrade project we continue to apply this standard configuration to users who may not yet be configured this way. However, in some cases we have been asked to leave work documents local for reasons of confidentiality or offline access, or to set up "synchronization" processes which keep local copies of documents that are located on the network drive.

Keeping work documents local (i.e. on your computer's hard drive) can be likened to keeping your life savings in cash under your mattress, rather than in a bank. It feels secure because it's close by, but in fact it is much more likely to be lost due to theft (do you have armed guards at your house?) or disaster (fire, flood). Like a bank vault, network file storage is designed with many layers of security, including:

- Physical security – The servers are large boxes mounted in racks in a locked server room, itself located in the center of a workspace protected by proximity card locks.
- System Reliability – The file servers are server-class machines with fully-redundant disk arrays used for storage. If any single hard drive dies, the system keeps running, and no data is lost.
- Network Security – The servers are all located behind a firewall which protects them from even being seen from the outside; they also require specific username/passwords to log on, access is logged, and rights are assigned on a very granular (folder-level) basis.
- Backups – All the data on the network file servers and the Exchange servers is backed up every day, and backups are kept (in a rotation) for six weeks, one of them in a secure offsite location.

It's also important to recognize that, in the case of PI, it is in fact not permissible under FIPPA to keep it outside of a "secure server" environment unless the computer is encrypted.

So, based on all of the information above, here are the options available:

1. **Our strong recommendation is to store all work documents on the network file servers**, with confidential files on the M drive and shared files on the N drive. If remote access is required, use properly-configured Remote Desktop Access, or an encrypted laptop or USB key. This model of usage requires no addition steps, nor does it require this form to be submitted.
2. **If you do require work documents to be kept locally on a desktop computer, for any period of time, it must be encrypted**. This will involve an additional step in the upgrade process, and can take 2 or more hours to complete the encryption the first time. The upgrade process itself may take longer as well, depending on the volume of local files to be backed up and restored during the process. This model of usage requires this form to be completed and submitted.

Please note that, based on long experience with file synchronization systems (and their pitfalls), **Faculty of Medicine IT staff cannot set up file synchronization** for users. From a technical perspective, the risks outweigh the benefits, and better options are available. If users do wish to copy files locally, this should be communicated to the technician so that the computer can be encrypted as per option 2 above.

Send the completed, signed form to discovery.commons@utoronto.ca, or fax it to 416-971-2482.

Person Requesting Local Document Storage Date: _____

Requestor Name: _____

Requestor Department: _____

Requestor Email: _____

Location of local document storage: _____

Local files are the sole responsibility of the requestor, and are not backed up by the Discovery Commons.

Supervisor Approval

Supervisor Name: _____

Supervisor Email: _____

Supervisor Signature: _____

For Technician Use Only

Technician Name: _____

Computer Encrypted with BitLocker: ☐

BitLocker Recovery Key: _____

(Enter here or attach separate page)

BitLocker Encryption Tested: ☐