Encrypting Personal and Confidential Information

Did you know that the University's policy is to require encryption of all personal and confidential electronic information kept outside of a secure server at the University of Toronto?

Recent data breaches at other organizations have resulted in serious consequences including reputational harm, financial liability and terminations of employment.

In June 2011, the Provost issued a Guideline requiring personal and other confidential information to be protected by effective security consistent with University policy and information security and privacy practices.

Confidential information is any information that is not intended to be publicly available, including personal information, which is any information about an identifiable individual, e.g. student number and grades.

Personal and other confidential information in electronic form must be kept in a secure server environment with appropriate restricted user rights. If it is outside a secure server environment, personal and other confidential information in electronic form must at all times be protected with properly implemented encryption.

Privacy is an overarching institutional responsibility shared by all at the University. It is everybody's responsibility at the University to protect personal and other confidential information. The University takes privacy protection very seriously and is subject to the *Freedom of Information and Protection of Privacy Act* (FIPPA).

The University's Freedom of Information and Protection of Privacy Office emphasizes these expectations and requirements in privacy training across all three campuses.

The Information and Privacy Commissioner/Ontario (IPC) is investigating a privacy breach at Elections Ontario involving personal information of up to 2.4 million Ontarians. The matter involves the loss of two USB keys containing unencrypted names, home addresses, dates of birth, gender and whether or not the person voted in the last election. The IPC's findings will include guidance that organizations can use to limit the possibility of this type of breach happening in the future.

The Information and Privacy Commissioner, Dr. Cavoukian said, "I am deeply disturbed … It is my expectation that personally-identifiable information will not be stored on USB keys, laptops or other mobile devices – full stop. That is the message I have repeatedly given over the years. If it is absolutely necessary to transfer personal information to a mobile device, it should first be de-identified or protected with strong encryption." The Ontario Provincial Police were also called in to investigate. The employees responsible for losing the USB keys were let go.

There have been a number of other incidents where unencrypted data in desktops, hard drives, smart phones, laptops, USB keys etc. have been lost or stolen. The IPC has ruled that organizations have contravened FIPPA when personal information has not been de-identified or encrypted.

These incidents illustrate why the University's Freedom of Information and Protection of Privacy Office has emphasized encrypting non-public electronic information kept outside of a secure server at the University of Toronto during its current round of privacy training across all three campuses. If you are interested in a training session for your division/department, please contact Howard Jones, Coordinator, Freedom of Information and Protection of Privacy Office, (416) 946-7303 howard.jones@utoronto.ca

Your local IT support unit can assist you with encryption. There are also encryption resources that can be found at:

http://encrypt.utoronto.ca/

Security of Personal and Confidential Information Checklist

Is it public or non-public information?

Public
Does not need to be protected

Non-Public
Personal and confidential information needs to be protected

Is it hard copy or electronic non-public information?

Hard Copy
Lock it in a secure institutional environment

Electronic
Protect it in a secure server environment

Can I take electronic non-public information out of a secure server environment?

Only with
Official authorization,
Operational need,
No other reasonable means to do the task, and
Strong encryption