Faculty of SCIENCE

Annual Encryption Self-Declaration

Purpose

The purposes of this annual self-declaration are:

1) To increase awareness and understanding about what is considered sensitive information, the responsibilities of a custodian and best practices for protecting sensitive information.

2) To allow everyone associated with the Faculty of Science to declare they are following the University of Alberta procedure on encryption. This procedure applies to all members of the University community.

Since completion of this annual self-declaration is mandatory, individual results will be shared with and reviewed by the chairs of your department.

Please provide the following information:

First Name: _____

Last Name: _____

Primary department or unit: _____

What is sensitive information?

Sensitive information refers to all information that could lead to the identity of an individual, and therefore needs to be protected in accordance with the Alberta Freedom of Information and Protection of Privacy (FOIP) Act, and other applicable legislation.

Sensitive or confidential information refers to all information that has been collected or compiled in the conduct of operating the programs and services of the University and may include, but is not limited to:

- Personal information about an individual as defined in the Alberta Freedom of Information and Protection of Privacy Act (social insurance number, birthdate, driver's licence, employee ID);
- Student records (grades, financial aid information)
- Health information as defined in the Alberta Health Information Act;
- Confidential business information of third parties;
- Confidential information collected or compiled in the process of hiring or evaluating employees of the University;
- Information collected or compiled in the process of law enforcement investigations;
- Advice, proposals or recommendations, consultations or deliberations of the governing and administrative authorities of the University;
- Information, the disclosure of which would harm the economic interests of the University; Sensitive information also includes personal health information, and proprietary and/or privileged information such as confidential

business or financial documents that could cause harm to the organization owning it if compromised by unauthorized disclosure, theft, loss, corruption, misuse or other actions.

How can I protect sensitive information?

Personal and confidential information (sensitive information) stored on desktop computers or mobile computing devices, such as laptops and smartphones, are at risk of unauthorized access and disclosure.

The best way to protect data is not to place it at risk by storing it on desktop computer hard drives, or mobile computing devices that can be lost or stolen. University and faculty-based network data storage and secure remote access services, eliminate (or at least greatly reduce) the need to store sensitive information on local or mobile computing devices.

What is my responsibility if I use or own sensitive information?

Information custodians and managers dealing with University information have the responsibility to ensure the privacy and security of the information under their custody and control. The urgency and requirements to safeguard sensitive University information are even higher, as are the resulting consequences from breach and compromise.

Mobile computing presents further exposures and risks given the increased likelihood of loss and theft of information. Therefore, custodians need to become familiar with and practice mobile device security best practices. See the University's Mobile Device Security Best Practices: http://www.vpit.ualberta.ca/encryption/

Encryption is one of the best practices needed. Encryption is a method of protecting information by converting it to a format that's unreadable by anyone except those with a special key (usually a very long password). If a person doesn't have the key required to decrypt that data, the information remains inaccessible.

Encryption methods must be used to protect any sensitive information deemed private and confidential that is stored on a local computing device (i.e. desktop computer, laptop or mobile device). This includes:

- Email messages
- Confidential documents
- Personnel files
- Student records, including marks

The individual will be held responsible for any information disclosure from his/her desktop computer or mobile devices, whether accidental or not. The individual must therefore exercise all necessary precautions, such as using the Faculty's network data storage and encryption.

Declaration

I declare I have read and understood the University of Alberta procedure on encryption, available from the UAlberta website (http://www.vpit.ualberta.ca/encryption/) and that the information I have provided in this form is true and correct, to the best of my knowledge and belief.

I declare I am complying with the University encryption procedure .

Signed: _____ Date: _____