University of Alberta
Faculty of Medicine & Dentistry

Encryption Policy

This policy is governed by its parent policy: Information Technology Security Policy (UAPPOL)

Office of Accountability: Office of the Dean
Office of Administrative Responsibility: Office of the Dean
Approver: Faculty Management Committee (April 2011), Chairs Committee (October 5, 2011)
Scope: Compliance with this policy extends to all members of the Faculty community (faculty academics, support staff, trainees, etc)
Effective Date: November 1, 2011

Overview

The Faculty of Medicine & Dentistry (FoMD) is critically dependent on its information technology resources to fulfill its academic and business responsibilities and must comply with applicable government regulations. Failure to protect sensitive information can negatively affect the Faculty’s ability to fulfill these responsibilities, its mandate, and can be damaging to the Faculty’s and University’s reputation.

Personal and confidential information (sensitive information) stored on personal computers or mobile computing devices are at risk from unauthorized access and disclosure, when the device is lost or stolen.

Encryption is a method of protecting data by converting it to a format that is unreadable by anyone except for those authorized. It is accomplished by using software- or hardware-based solutions that convert the information using protected algorithms. The benefits of encryption include ensuring the information can only be accessed and changed by authorized individual(s). Encryption is the industry standard and non-compliance with this standard places the University at considerable risk.

The best way to protect data is not to place it at risk by storing it on local computer hard drives, personal computers or mobile computing devices that can be lost or stolen. Instead, using the Faculty’s secure data storage servers ensures data remains on protected servers with backup and high availability capabilities. Sensitive information should be retained on local devices only when necessary and only when the local device is encrypted.

Encryption is not, however, a panacea. It is not a substitute for other security measures that must be used in concert with encryption to provide the layers of controls necessary for adequate information privacy and security protection. Some of the other measures are access controls, physical security controls, and the awareness of and compliance with secure information handling and management practices. These practices would recognize the Freedom of Information and Protection of Privacy Act (FOIPP) as it relates to sensitive information regarding faculty, staff, and students and the Health Information Act (HIA) when health information is involved.
**Policy:**

Whenever any sensitive information that is deemed private and confidential, including e-mails, confidential documents, data, personnel files, etc., are stored in a personal computer or mobile devices, encryption methods must be used to protect it.

**Purpose**

The purpose of this policy is to define the encryption mandate required for protecting sensitive data. The use of encryption is intended to mitigate the risk of data being inadvertently disclosed to unauthorized third parties, and to comply with Government of Alberta data protection directives. Most commonly, this involves a laptop, memory stick, or other portable device that is stolen, lost, or disposed of improperly. These practices are not intended as a way to mitigate compromised data by any other means, such as intentional compromise by a threat attacking the laptop’s software, its hardware, or its user's identity.

**POLICY DETAILS**

| Compliance with this policy extends to all members of the Faculty community. |

1. The individual will be held responsible for any information disclosure from his/her personal computers or mobile devices, whether accidental or not; and must therefore exercise all necessary cautions such as the use of encryption.

2. The storage or use of any sensitive information on local hard disk devices such as personal computers or mobile devices must be avoided unless absolutely necessary. The recommended mechanism for using such data is to keep the data on the Faculty's secure data storage servers and access the information remotely.

3. All personal computers and mobile computing devices (regardless of whether University-provisioned, owned, or not) that are used to store and transact sensitive information must deploy encryption.

4. Information should only be accessed from off-campus using the Faculty's virtual private network (VPN) services. Remote access of Faculty information technology resources must not leave any residual or cached sensitive data on the local machine.

**DEFINITIONS**

| Information technology resources | Information technology resources refer to all hardware, software, and supporting infrastructure that is used to create, retrieve, manipulate, transfer and store electronic information. This includes (but is not limited to), central and non-centrally supported computers, file systems attached to these computers, operating systems running on these computers, software packages supported by these operating systems, wired and wireless networks, telecommunication and hand-held devices, data stored on or in transit on the above, as well as electronic identities used to identify and authenticate the users of the aforementioned resources. |

Any definitions listed in the following table apply to this document only with no implied or intended institution-wide use.
Sensitive information

Sensitive information refers to all information that can lead to the identity of an individual, and thereby needs to be protected in accordance to the Alberta Government Freedom of Information and Protection of Privacy (FOIPP) Act, and other applicable legislation. Sensitive information also refers to proprietary and/or privileged information, such as confidential business or financial documents, that can cause serious harm to the organization owning it, if compromised by unauthorized disclosure, theft, loss, corruption, misuse, or other actions. Examples of sensitive information includes:

- Identity information (Social Insurance Numbers, Birth Date, Driver’s license, Employee ID)
- Financial account information (checking, savings, credit card account numbers, salary information)
- Student record information (grades, financial aid information)
- Medical record information (diagnoses, treatment information, identity information included in medical records, health insurance information)
- Donor record information and non-public gift amounts

Encryption

It is a method of protecting data by converting it to a format that is unreadable by anyone except those authorized. It is accomplished by using software- or hardware-based solutions that convert the information using protected algorithms. It is usually used to protect sensitive information stored in an electronic device or transmitted between devices.

Faculty community

Includes individuals of FoMD including academic staff, support staff, trainees (undergraduate students, postgraduate students, post docs, summer students, etc), and volunteers.

RELATED LINKS

Should a link fail, please contact FoMD MedIT. [▲ TOP]

- Code of Student Behavior (University of Alberta)
- Conditions for Use of Campus Computing ID (CCID) Authentication (AICT)
- University Wireless Service (UWS)
- Information Technology Use and Management Policy (UAPPOL)
- Information Technology Security Policy (UAPPOL)
- Freedom of Information and Protection of Privacy Act (FOIPP)
- Health Information Act (HIA)
- IT Standardization Policy (FoMD)
- Physical Security Policy (FoMD)