Approval Date: May 11, 2011

Parent Policy: IT Security Policy

Encryption Procedure

Office of Administrative Responsibility:	Vice-Provost and Associate Vice-President (Information Technology)
Approver:	Provost and Vice-President (Academic) Vice-President (Finance and Administration)
Scope:	Compliance with this University-wide procedure extends to all members of the University community.

Overview

University **sensitive information** stored on a **mobile computing device** is at risk for unauthorized access and disclosure if appropriate security measures are not implemented to protect the device against loss or theft of information.

The best way to protect University sensitive information is to not store it on a mobile computing device; however, it is recognized that storage of University sensitive information on a mobile computing device may be necessary in certain situations. In these cases, **encryption** provides protection against unauthorized access and disclosure.

Encryption must be used in concert with other security measures to maximize protection of **information technology resources** and of University sensitive information. The Office of the Vice-Provost and Associate Vice-President (Information Technology) has provided a Mobile Computing Security website that contains further information about other security measures.

Purpose

The purpose of this procedure is to describe requirements for encryption of a mobile computing device in order to minimize the risk of unauthorized access and disclosure of University sensitive information.

PROCEDURE

RESPONSIBILITIES

Members of the University community are responsible for protecting University sensitive information, whether accessed from University-owned information technology resources or from personal, external or other resources.

All University mobile computing devices must be encrypted and protected in accordance with standards developed by the Office of the Vice-Provost and Associate Vice-President (Information Technology). These standards can be found on the Mobile Computing Security Website. Best practice calls for encrypting all of an organization's laptops as:

- It is unlikely that a laptop does not currently contain any sensitive information, and/or will not do so in the future,
- Legislative and government bodies mandate encrypting all of an organization's laptops to minimize gaps and exposures,
- It prevents the painstaking and costly investigation and follow-up that ensues from loss or theft of unencrypted laptops.

Any personal, external or non-University computing device (mobile, desktop or other) that is used to store University sensitive information must be encrypted and protected in accordance with standards developed by the Office of the Vice-Provost and Associate Vice-President (Information Technology). These standards can be found on the Mobile Computing Security Website.

Academic Information and Communication Technologies (AICT) and local **system administrators** will provide assistance to members of the University community to ensure that a mobile computing device is encrypted according to the standards developed by the Office of the Vice-Provost and Associate Vice-President (Information Technology). These standards can be found on the Mobile Computing Security Website.

ADDITIONAL REQUIREMENTS

1. Mobile computing devices must run a current, fully patched and modern operating system at all times.
2. Mobile computing devices must be configured to ask for a password after any period of inactivity, including after resuming from suspend/standby/sleep/hibernate status and on start-up of the device.

Please see the University's Mobile Computing Security website for information on other recommended controls for safeguarding against the risks from mobile computing.

NON-COMPLIANCE

Non-compliance with this procedure constitutes misconduct and may be handled under the applicable collective agreements, University policy or law.

DEFINITIONS

Any definitions listed in the following table apply to this document only with no implied or intended institution-wide use. [▲Top]

Sensitive Information	Definition of "sensitive" or "confidential" information (from the University of Alberta Information Access and Privacy Office): 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; − 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; − Any information to which legal privilege including client-solicitor privilege may apply.
Mobile Computing Device	A mobile computing device refers to a portable self-contained electronic device that has data processing, transmitting and/or storage capabilities. Mobile computing devices include, but are not limited to, personal digital assistants, palm tops, smart phones, hand-held/laptop computers, portable external hard drives, tablets and memory sticks.
Encryption	Encryption is a method of protecting data by converting it to a format that is unreadable. Only those authorized can make a particular set of encrypted data readable again through decryption. Encryption is used to protect and uphold data confidentiality and integrity.
Information Technology Resources	Information technology resources refer to all hardware, software, and supporting infrastructure owned by, or under the Custodianship of, the University that is used to create, retrieve, manipulate, transfer and/or 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.
Members of the University Community	University staff, faculty, students and other holders of a valid CCID.
System Administrator	System administrator refers to the person or persons responsible for configuring, installing, maintaining, and supporting information technology resources for a faculty, department, or unit. A system administrator of an information technology resource may also be a user of that resource.

FORMS

There are no forms for this procedure. [▲Top]

RELATED LINKS

Should a link fail, please contact uappol@ualberta.ca. [▲Top]

Code of Student Behaviour (University of Alberta)

Information Technology Use and Management Policy (UAPPOL)

Access to Information and Protection of Privacy Policy (UAPPOL)

Mobile Computing Security (University of Alberta)