POLICY TITLE:	**End-point Encryption Policy**
POLICY #:	CIO-ITSecurity-08.3
Initial Draft By - Position / Date:	ISC Architecture Sub-Committee- 01/23/2008
APPROVED BY / DATE:	**Michael Ridley, CIO – December 4, 2009**
Last Revised Date:	**Final Draft – November 25,2009**
Next Review Date:	One year after Approval
BRIEF DESCRIPTION:	This document describes the required usage of encryption technology and encryption key management to protect sensitive information stored on portable or insecure electronic devices.

Table of Contents

Introduction

Utilization of encryption software supports data privacy and integrity by converting electronic information into a format that is readable by authorized individuals only. This policy establishes that use of whole disk encryption for electronic information stored on portable or insecure devices shall be consistent with legislative requirements and the University's need for protection against accidental disclosure or unauthorized access.

Scope

This policy applies to all University of Guelph academic and administrative electronic information stored on portable or insecure devices, and information custodians.

Policy Statements

1. Sensitive data (including personally identifiable data—see Definitions) should not be stored on portable electronic devices (e.g. laptops, PDA's) or other electronic media unless absolutely necessary, and approved by department heads. If operationally necessary, steps should be taken to limit the duration of the storage and comply with the following requirements.

2. Encryption must be used when required by federal and provincial legislation. The University Data Classification standard (approval pending) will also be used to define restricted electronic information that needs to be encrypted, based upon specific content and location.

3. Whole disk encryption must be used to secure sensitive or confidential electronic information stored on any computers and electronic storage media for which physical security controls are limited due to the mobile nature of the computer or storage media. Whole disk encryption must also be used for desktop computers storing sensitive or confidential electronic information that are located in areas with minimal public access restrictions and/or physical theft deterrents.

4. Authorized access to encrypted University information must be preserved through administrative procedures governing encryption key management.

5. Department heads must ensure that when encryption is required within their units as prescribed by this policy, the centrally administered infrastructure cryptography service is utilized, unless an exception has been approved by the Chief Information Officer (CIO).

Responsibilities

1) Users and System Administrators:

   i) Safeguard encryption security pass-phrases, encryption keys and/or authentication devices.

   ii) Use encryption in accordance with University policies.

   iii) Ensure that all sensitive or confidential data, whether electronic, printed, emailed, etc. is maintained in a secure manner and only stored on portable media or devices for the absolutely minimum time necessary.

2) Provost (or designate):

   i) Receive and review requests by a department to access encrypted data with the appropriate VP or A/VP.

   ii) Approve the request to release of the key from the escrow facility to the department to un-encrypt data.

3) Department Heads:

   i) Ensure that any electronic information classified as sensitive or confidential by University privacy policies, data classification standard, and/or federal or provincial legislation, which is stored on portable or insecure devices be properly encrypted.

   ii) Approve applications for use of the centrally-administered encryption mechanism within his/her unit consistent with this policy or departmental business need to protect information stored on electronic devices.

   iii) Request the Provost approve the use of key escrow service to access encrypted devices, consistent with this policy.

4) ISC Architecture Sub-Committee:

   i) Undertake periodic reviews of this policy and processes for whole disk encryption.

   ii) Establish the technical requirements for any encryption implementation.

   iii) Review the University data classification standard.

5) Office of the CIO (or designate):

   i) Develop, administer and maintain hardware and software supporting cryptography infrastructure or maintain a contractual arrangement with an external agency to provide encryption and key escrow services.

   ii) Develop and publish training resources on the use of the supported cryptography service.

   iii) Forward requests related to key usage (i.e. password recovery) to restrict or recover access to data to the Provost for approval.

   iv) Monitor encryption service utilization, service costs, and procedure for removing encryption software as required.

6) Audit Services:

   i) Review compliance on campus through periodic audits of departments administering sensitive or confidential electronic information.

Exceptions

Exceptions can be approved for a unit that has a technical requirement to use another encryption solution, or compensating control, to protect their data consistent with the intent of this policy. Approval for the exception rests with the CIO, who will need the following information to assess the request:

1. Requesting campus unit.
2. Requesting campus unit director/manager contact information.
3. Technical representative contact information.
4. Date of request.
5. Description of proposed solution.
6. Description of why proposed solution is being requested rather than use of the centrally supported encryption and key escrow service.

7. Description of the security controls/practices in place to ensure that unauthorized activity threatening the confidentiality of electronic data and/or stored encryption key(s) will be logged, subject to timely review and, if appropriate, reported to IT Security.

Definitions

Cryptography – a method used to encode information so that only authorized individuals can read the information.

Data at rest – Data residing on a server, within a database, or on secure desktop systems.

Data in Transmission – Data being transmitted from a source to another system using networks. The transfer may occur using a login screen, web pages, file transfers or application to application.

Data on Portable Devices – Any portable device that can store data such as a laptop computer, unsecured servers/desktops, tablet, smart phone, PDA, USB drives; also, portable media such as CD/DVD and floppy disks.

Encryption – Transforming information using a secret key so that the information is unintelligible to unauthorized parties.

Key escrow – mechanism that permits an authorized third party to recover encrypted information.

Sensitive Data – Sensitive electronic information includes but is not limited to personally identifiable information and is defined by the University Secretariat's Directory of Records and Personal Information Banks Directory of Records and Personal Information Banks | University of Guelph. In addition, federal and provincial legislation specifies data elements which require protection from unauthorized creation, reading, modification and/or deletion.

Whole disk encryption – the application of encryption process to encrypt each data bit on an electronic storage system or device.

Version, Change and Approval History

Final Draft published:	November 25, 2009
Circulation Draft Published:	February 18, 2009
Initial Draft Circulated:	May 2, 2008