Information Asset Management Policy

Classification

Information Management

Table of Contents

Purpose 1
Scope 2
Definitions 3
Policy Statement 4
Special Situations 5
Responsibilities 6
Parent Policy 7
Related Policies 8
History 9

Approval Authority

Board of Governors

Implementation Authority

Information Management

Compliance Officer

Effective Date

April 01, 2006

Latest Revision

October 22, 2007

Purpose 1

The purpose of this policy is to vest authority and responsibility for the Information Management Program. It is also to:

a) identify reasonable internal and external Risks to the security, confidentiality, and integrity of the University’s Information Assets that could result in the unauthorized or accidental disclosure, misuse, modification, disposal, or other compromise of information;

b) assess current security safeguards for ability to control these Risks;

c) institute a process of continual monitoring and analysis of new safeguards that may be more effective in controlling Risks;

d) vest responsibility for conducting Risk assessment.

Scope 2

This policy applies to Employees of the University of Calgary and to University of Calgary Information Assets and information systems.

Definitions 3

In this policy:

a) ‘Business Information Assets’ refers to intangible information and any tangible form of its representation, including printed copies, computer files, and databases that relate to the operation or administration of the University. It does not include information that is considered to be the intellectual property of an Employee.

b) ‘Employee’ means a person employed by the University of Calgary for wages or salary.
c) ‘Health Information Assets’ refers to health information as defined by the Health Information Act (H-5 RSA 2000) when the information is stored on information systems supported by the University of Calgary.

d) ‘Impact’ refers to the magnitude of harm that could be caused by a threat’s exploitation of a vulnerability. The Impact of a threat will be based on the assets targeted, the confidentiality of the assets, and the type and degree of compromise.

e) ‘Information Assets’ means data in any form or media that is placed into a meaningful context for users. These assets may contribute to an organization’s knowledge base and help it to achieve its goals. They may be collected in relation to business or research activity. The term ‘Records’ refers to a special kind of information asset.

f) ‘Records’ refers to Information Assets that are created or received and set aside in a filing system by an office or officer in the course of business. Records are kept as evidence of the office’s functions, policies, decisions, procedures, operations or other activities.

g) ‘Retention and Disposition Rules’ establish how long Records should be kept in an office, how long they should be stored in semi-active storage, and whether they should ultimately be destroyed or transferred to archival storage.

h) ‘Risk’ is a function of threat, vulnerability, and asset value. Risk only exists if a threat can exploit a vulnerability which results in an adverse Impact on a valued information asset.

i) ‘Scholarly Information Assets’ refers to intangible information and any tangible form of its representation, including printed copies, computer files, and databases that relate to the research/teaching/service activity of an Employee of the University when these assets are considered to be the intellectual property of the Employee.

j) ‘Threats’ refers to any circumstance or event with the potential to cause harm to an information asset either through intentional means targeted at the exploitation of a vulnerability, or through unintentional means that accidentally trigger a vulnerability. Threats may be classified as natural or manmade, intentional or unintentional. Examples of natural Threats include lightning, flood, humidity, and time. Examples of manmade Threats include theft, computer viruses, vandalism, sabotage (intentional) and user error, accidental damage, lost documentation, and programmer error (unintentional).

k) ‘Vulnerabilities’ refers to characteristics or weaknesses of systems that allow Information Assets to be compromised

Policy Statement

4 Business Information Assets
4.1 Information Assets created or received by University Employees in the
conduct of the business of the University are considered to be in the custody or under the control of the University.

4.2 Business Information Assets in the custody or under the control of the University are the property of the University and will be managed in accordance with the Information Management Program as well as any other information management and security policy objectives.

**Scholarly Information Assets**

4.3 Scholarly Information Assets stored on University systems will be classified in accordance with the Information Asset Identification and Classification Policy and managed in accordance with information security policy objectives.

4.4 The retention period for Scholarly Information Assets will be established by the researcher in accordance with research requirements as well as contractual or other legal obligations if they exist.

4.5 Scholarly Information Assets containing personal health information will be stored in systems or facilities that are operated or managed by the University.

4.6 Scholarly Information Assets stored off-site will be managed under the Information Management Program.

**Health Information Assets**

4.7 Health Information Assets stored on University systems will be classified in accordance with the Information Asset Identification and Classification Policy and managed in accordance with information security policy objectives and applicable laws and regulations.

4.8 Health Information Assets will be retained as long as is required under applicable law or standard codes of practice in the Province of Alberta.

4.9 The University is not responsible for the security of Health Information Assets in systems that are not operated or managed by the University.

**Information Management Program**

4.10 The University Archives will be responsible for the development, implementation, and management of the Information Management Program. The program will include the following elements:

a) identification and classification of Information Assets;

b) establishment and execution of record Retention and Disposition Rules for Business Information Assets;

c) storage of semi-active and inactive Information Assets, including off-site storage solutions;

d) evaluation of system design elements relating to security of data;

e) the design, implementation and management of effective systems for access to information;
f) the protection and preservation of Information Assets of permanent value; and
g) any additional elements necessary to support these and other information security policy objectives.

4.11 Record Retention and Disposition Rules for Business Information Assets will be approved by the Information Management Compliance Officer and the University Records Committee before they are considered authoritative.

4.12 Business Information Assets created, received, or stored by a university office or officer will be dealt with by that office or officer in accordance with the record Retention and Disposition Rules approved by the Information Management Compliance Officer and the University Records Committee.

4.13 University departments will appoint at least one officer to serve as Records Coordinator for the department. The Records Coordinator will be responsible for discharging the duties of the department with respect to information management.

**Risk Assessment**

4.14 Current security safeguards designed to protect Information Assets owned by and/or in the custody of the University will be analysed for adequacy and appropriateness on a regular basis. New safeguards that may be more effective in controlling Risks will also be regularly assessed.

4.15 The Risk to Information Assets in the custody or under the control of the University will be formally assessed at least once annually.

4.16 The Risk assessment may include the identification of
   a) Information Assets
   b) potential Threats to those assets
   c) points in the system where Vulnerabilities may exist that Threats can exploit
   d) probabilities of Threats exploiting the Vulnerabilities
   e) Impact, in terms of cost estimates and value losses, should a potential threat be realized.

4.17 The Risk assessment will also rank the severity of possible threat scenarios and analyze the probability and Impact of the exploitation of a vulnerability.

4.18 A cost-benefit analysis comparing the cost of implementing additional security safeguards with the value to the organization of the reduced level of Risk will be prepared at the same time.

4.19 A database of recognized Threats and threat event history will be maintained and used in Risk assessment and analysis.
**Risk Management**

4.20 Risks will be managed on the basis of the results of the Risk assessment and the cost-benefit analysis.

4.21 Results of the Risk assessment will be provided to the V.P. (Finance and Services).

4.22 A summary report will be submitted to the Audit Committee through the V.P. (Finance and Services) once annually.

---

**Special Situations**

5 In the absence of a formal retention and disposition rule, the Information Management Compliance Officer has the authority to require the transfer of business Records of permanent value to the University Archives for permanent preservation or to authorize the destruction of Business Information Assets that are inactive and are not deemed to have any continuing legal, administrative, financial, or archival value.

---

**Responsibilities**

6 6.1 Chief Information Officer, Information Management Program Manager, Insurance and Risk Management Manager (or their designates)
   a) conduct regular Risk assessments;
   b) analyze results and take action or recommend action as appropriate; and
   c) create a database of recognized Threats and threat event history.

6.2 Records Coordinator
   a) implement the Information Management Program as outlined by the University Archives.

6.3 University Archives
   a) provide leadership in planning, developing, and maintaining the university-wide Information Management Program.

---

**Parent Policy**

7 Information Management Compliance Program Policy

---

**Related Policies**

8 Information Asset Identification and Classification Policy
   Acceptable Use of Information Assets Policy
   Information Asset Security Monitoring Policy
   Information Asset Protection Policy
   Records Retention and Disposition Policy

---

**History**

9 Approved: February 10, 2006

Effective: April 1, 2006

Revised: editorial revisions effective October 15, 2006

Revised: October 22, 2007 (Board of Governors: Meeting #2, 2007-08)