UNIVERSITY of GUELPH

Information Technology Security Policy Framework

Office of the Chief Information Officer

APPROVED

December 24, 2009

Information Technology Security Policy Framework

CONTENTS

Information Technology Security Policy Framework

Preamble

This document (the IT Security Policy Framework) represents a formalized organizational structure for Information Technology policies, standards and processes. The Framework, also known as an Information Security Management System (ISMS), provides a risk-based architecture for consistent IT security practices that govern the entire University. The document provides a summary context, scope, components and linkages to specific enterprise IT security policies and supporting references.

Definition and Purpose

This IT Security Policy Framework describes the approach taken by University management for administering information technology security, and reflects management's commitment to a visible and clear set of responsibilities for ensuring IT security is coordinated across the organization.

The Policy Framework goals include: sustaining a cost-effective secure computing environment for the protection of confidential or sensitive information; maintaining personal information privacy; and preventing disruptions that impact the use of the University of Guelph computing facilities.

The Framework specifies the over-arching model and components for providing appropriate levels of protection for the University's information technology assets, including the major business applications, technology infrastructure services and information data stores.

The Framework supports and underpins an enterprise risk management strategy as developed by the University's Risk Management Steering Committee (RM-SC). The RM-SC is responsible for the institutional risk assessment process, including assessing internal and external threats, information management and technology vulnerabilities and risks, and prioritizing the business systems that require preventive controls and risk mitigation.

Information Technology (IT) Security ensures that:

- Information systems are available and usable when required, and can appropriately resist attacks and recover from failures **(availability)**

- Information is observed by or disclosed to only those who have the right to know **(confidentiality)**

- Information is protected against unauthorized modification or errors so that accuracy, completeness and validity are maintained **(integrity)**

Ownership and Maintenance

This IT Security Policy Framework is subject to approval by the President of the University. Responsibility for on-going maintenance, sponsorship and coordination of IT policies rests with the Chief Information Officer (CIO) of the University. This document will be reviewed and supported by the University's Information Technology Strategy Committee (ITSC) prior to submission to the President for approval. The ITSC will periodically review the Framework, and assist the CIO in formalizing new IT security policies.

Specific on-going IT security responsibilities are described in the policy document entitled Roles and Responsibilities for Information Technology Security.

All institutional IT security policies, standards and guidelines will be referenced and accessible from this Framework document. Drafting, revision, approval, and periodic review will be documented as an Appendix to this document.

Scope and Statement of Applicability

The scope of this IT Security Policy Framework includes the entire University enterprise, including the regional colleges, Guelph-Humber, all administrative, academic, research and ancillary units, and the entire University networking environment (including remote and mobile users). The Framework is intended to guide cost-effective protection of all systems infrastructure, applications, services, databases and computing accounts (i.e. information assets).

This Framework reflects the risk management and risk assessment priorities of the Enterprise Risk Management Steering Committee (RM-SC), and documents the connection between risk assessment and identification of appropriate controls. The Framework references guidance of the international 'code of practice' for information security contained in ISO/IEC 27002:2005.

Security Framework Components

This document utilizes the organizational structure of the ISO 27002 standard, with each of the eleven categories referenced in the standard included in this document as individual components.

The eleven components introduce focus areas of security practice and control. Components include: allocation of information security responsibilities, access control, physical, network and environmental security, security incident management, and systems development and maintenance.

As new policies are developed, this document will include hyper-text links to individual policy documents (both draft and approved) mapped to the appropriate component within the Framework.

The ISO standard also includes guidance (not included in this document) on the essential first step of information security risk management, enabling a holistic approach to IT security based on management's risk assessment, security requirements and prioritized security controls (i.e. risk mitigation).

Component #1: Information Security Policy

This section summarizes the institution's approach to managing information security. This component also specifies targets for regular formal reviews of IT security policy including compliance feedback, continuing suitability, and effectiveness.

This IT Security Policy Framework represents the institution's over-arching IT security policy document. In accordance with recommended practice, this enterprise-level policy will be reviewed annually. Approval and revision history will be recorded in Appendix I within this document.

Component #2: Organization of Information Security

This section includes documents which outline management's commitment to information security, and coordinating information security activities. Examples of content to be developed include: authorization of new information processing facilities, confidentiality agreements, independent reviews of security, and addressing security in third party agreements.

Coordination of information security and allocation of information security responsibilities are specified in the following policy document:
Roles and Responsibilities for Information Technology Security.

Component #3: Asset Management

All information processing assets should be inventoried, assigned ownership, and have specified rules relating to acceptable use. Information should be classified in terms of its value, sensitivity, and criticality to the institution.

A preliminary IT asset inventory, prepared by the RM-SC for their risk assessment process, is being maintained and enhanced by the Office of the CIO/IT Portfolio Management Office. The asset inventory identifies business owners/custodians of each major IT asset (i.e. enterprise business applications and infrastructure services). The RM-SC determines business continuity priorities.

University of Guelph Acceptable Use Policy:

http://www.uoguelph.ca/web/aupg.shtml (http://www.uoguelph.ca/web/aupg.shtml).
The Acceptable Use Policy (AUP) describes the expectations for all members of the University community for appropriate use of technology, protection of privacy, and protection of academic freedoms. The AUP includes examples of unacceptable use, a complaint and violation resolution process. The AUP is administered by the Office of the CIO.

Component #4: Human Resources Security

This section includes recommendations regarding information security awareness, education, and training. Additional content includes responsibilities during employment (e.g. Acceptable Use Policy), security provisions in third-party contracts, and termination of employment (e.g. removal of access rights)

Raising the level of awareness of security issues in the community is an important component of IT security management. The CIO's Office and Computing & Communications Services (CCS) works with Communications and Public Affairs and student groups to deliver guidance on IT security practices.

It is also important that the community is aware of Security Policies and their responsibilities. The CIO's Office is responsible for communicating IT security issues to the community, and developing IT security education and training.

This Security Program will also be published through a web page accessible from the CIO's web-site, and kept current.
http://www.uoguelph.ca/cio/content/introducing-universitys-it-security-program

Computing & Communications Services (CCS) provides regular communication via a security web page http://www.uoguelph.ca/ccs/security/index.shtml, periodic articles in the campus newspapers, meetings and targeted emails.

Component #5: Physical and Environment Security

The overall physical security objective is to prevent unauthorized physical access, damage, and interference to the organization's premises and information. This section will include recommendations on personnel working in secure areas, and the secure disposal or re-use of equipment.

Computing & Communications Services (CCS) maintains a well-controlled physical environment to house systems, data and network resources.

In response to a 2009 review by the University's internal Audit Services department, guidelines and recommended software/services on IT asset management and disposal are under development.

Component #6: Communications and Operations

This section will reference enterprise-level operational procedures, segregation of duties, managing third-party services, capacity management, information and software back-up, security of network services, media handling, the exchange of information between systems, e-commerce, and system monitoring.

Content to be developed.

Component #7: Accounts and Access Controls

This section will include policies and guidance regarding user responsibilities, rights and privileges, network access control, operating system and application access controls, and mobile computing.

The following identifies policies and practices related to the accounts, passwords and access controls that are used to identify an individual, to make sure they are only given access to the information they need, describes their roles and responsibilities and how they should respond to security problems.

Identification: The standard format and usage for central accounts (user names) is described in the draft CCS Central Account Policy (unpublished).

Authentication: (in development).

Access control: A draft document, describing a proposed classification scheme for institutional data, and the data handling controls required for each level of data, has been developed, and publication is pending. This policy will cover regulatory compliance for data control such as PIPEDA and FIPPA.

Network Policy: The Network Security Architecture describes the tools and designs used to protect University of Guelph assets from threat that originate from the network. This includes the Wireless Access Policy.
http://www.uoguelph.ca/cio/content/wireless-networking-policy
The policy is designed to control the implementation and management of wireless access points on campus.

Component #8: Systems Acquisition and Development

This section provides guidance on control of application input and internal processing, cryptographic controls, key management, application development and change management, and technical vulnerability management.

Vulnerability assessment and management:

Vulnerability assessments are performed on critical information technology assets of the University of Guelph on a regular basis by the CIO/Portfolio Management Office. The vulnerability assessment service is based on the Vulnerability Management Policy (#CIO-ITSecurity-08.6) and Practice Standard located here Vulnerability Assessment Policy.

Encryption Policy and Service:

The enterprise policy (#CIO-ITSecurity-08.3) on encryption of portable media is located at Encryption Policy. A centrally administered encryption service is provided by the CIO's Office.

Component #9: Security Incident Handling

Guidance on reporting security events, managing security incidents, and building information security into business continuity management.

Incident Response: The University of Guelph will have an incident response capability described in the Incident Response and Escalation Policy, for security incident resolution. (under development)

Incident Management: A Computer Security Incident Response Team, (CSIRT) will be responsible for handling major security problems in an appropriate manner and improve our capability to track and resolve security incidents.

Component#10: Business Continuity Management

This section will link to guidance on including information security in the business continuity management process, and a business continuity planning framework (i.e. specifying owners, escalation plans, temporary operating procedures, resumption priorities, critical assets and resource requirements).

Preventive Measures: Disaster Recovery Plans outline the roles, responsibilities and resources for those who are responsible for restoring computing and network facilities in cases where there is a long term and or major disruption of critical services. The Office of the CIO maintains over-arching responsibility for coordinating major disruptions.

Departmental Disaster Recovery Plans, focused mainly on recovery of major enterprise applications, are maintained by CCS, and reviewed by external auditors annually.

Component #11: Compliance

This section includes identifying applicable legislation, protecting intellectual property rights, protection of organizational and personal information, prevention of misuse of facilities, regulation of cryptographic controls, compliance with security policies, and audit considerations.

The University's approved Acceptable Use Policy is described in Component # 3: Asset Management.

A draft enterprise policy on encryption of portable media is described in Component #8: Systems Acquisition, Development and Maintenance.

Glossary

This section provides brief descriptions of the various items and terms used to describe risk, security, networking and technology issues.

Control: A safeguard, response or countermeasure to manage (i.e. mitigate or reduce) risk, including policies, guidelines, standards, practices or organizational structures.

ISO/IEC: The International Organization for Standardization/International Electrotechnical Commission.

ISO/IEC 27002: Part of the ISO 27000 series on information security. Prepared by the Joint Technical Committee ISO/IEC Information Technology Subcommittee. The current version of the standard was published June 15, 2005 and replaced the previous version ISO 17799:2000.

ISMS: Information Security Management System. The over-arching policy framework and administrative program for guiding IT security within an organization.

Risk: The combination of the probability of a threat materializing (i.e. event) and its consequence or impact. Risk management reflects coordinated activities to direct and control risk, and typically includes risk assessment, risk treatment or mitigation, risk acceptance, and risk communication.

Risk Assessment: The systematic and methodical consideration of: 1) the harm likely to result from a range of business process failures; and 2) the realistic likelihood of such failures occurring. The risk assessment and risk management process includes estimating the magnitude of risks, comparing risk estimates against risk criteria (i.e. risk evaluation), and determining the appropriate controls for reducing risk to an acceptable level.

Threat: A potential cause of an unwanted incident, which may result in harm (i.e. impact) to a system or organization.

Vulnerability: A weakness of an asset or group of assets that can be exploited by one or more threats.

Appendix I

Version, Change and Approval History

Document Approved December 24, 2009
Approved by President and Vice-Chancellor A.J.S. Summerlee

Final Draft published November 25, 2009
Minimal editing/revisions.

Fourth Draft published (for circulation) June 4, 2009
Minor revisions reflecting input from ITSC.

Third Draft (to ITSC): May 11, 2009
Document re-titled Policy Framework.
Minor revisions reflecting input from ITSC.

Second Draft (to ITSC): February 6, 2009
Reflects input from ITSC on Feb.2/09

First Draft (to ITSC): December 3, 2008
Initial draft by D. D. Badger