POLICY TITLE:	**Roles and Responsibilities for Information Technology Security**
POLICY #:	CIO-ITSecurity-02.1
Initial Draft By - Position / Date:	Doug Badger - Director, IT PMO / March, 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 Policy defines the roles and responsibilities of the groups and individual members of the University community who are responsible for information technology assets and security processes at the University of Guelph.

Table of Contents

Introduction

Information technology assets (including application systems and IT infrastructure) of the University of Guelph will be protected through IT management policies, recognized best practices for information security, and compliance with applicable federal, provincial, regulatory, or contractual requirements.

Policy Statement

The Chief Information Officer (CIO) is responsible for sponsoring, developing, and implementing a comprehensive information technology security strategy and policy framework (CIO-ITSecurity-00) which reflects the asset value of information and includes the entire technology infrastructure of the University. This Policy specifies the groups and individuals responsible and accountable for various elements of IT Security practice.

President

The President has overall responsibility for approving the University's strategy and administrative structure for managing information technology assets and infrastructure. The President approves the information technology security policy framework (CIO-ITSecurity-00), and delegates responsibility for administration and compliance to the University's Chief Information Officer.

Chief Information Officer

The Chief Information Officer (CIO) is responsible for overall strategy, policy administration, risk management, and compliance of the University's information technology, information services and information resources. Reporting to the Provost and Vice President (Academic), the CIO will:

1. Be accountable for the development and use of information systems (IS) and information technology (IT) to further the academic mission and to support the administrative requirements of the University.
2. Establish standards for use of information and technology on campus.
3. Escalate security incidents to the appropriate executive level.
4. Coordinate IT disaster recovery and emergency response planning.
5. Monitor IT compliance to meet legislative requirements.
6. Analyze and manage institutional information technology risks.
7. Chair the Information Technology Steering Committee (ITSC).

Information Technology Steering Committee (ITSC)

The Information Technology Steering Committee, chaired by the CIO, is the senior constituent body within the IT Decision Making Framework. The Committee is responsible for advising the CIO regarding the information technology governance program, including overall IT principles, policies, and investment priorities.

The ITSC may delegate assignments, research and infrastructure management to the Information Services Council (ISC), which comprises representatives from academic, academic support, and administrative stakeholders. The ITSC advises the CIO regarding enterprise information policies, applications, and IT infrastructure including security issues.

Enterprise Risk Management Steering Committee

The Risk Management Steering Committee (RM-SC) has overall coordinating responsibility for the risk management process of the University. This includes identification of vulnerabilities and threats to the institution, analyzing risk probabilities, performing risk assessments, and determining appropriate controls to mitigate risk. The CIO is a member of RM-SC and is responsible for coordinating risk management activity relating to information technology assets and underpinning technology services.

CCS Executive

The Computing and Communications Services (CCS) Executive consists of the CIO, the Associate Directors of CCS, and the Director, Organizational Services. The Executive interprets strategic directions and priorities outlined by the ITSC and other IT Decision Framework constituents. As the major information technology service provider for the University, CCS has primary responsibility for infrastructure services and technical support responsibility for the University's major academic and administrative application systems.

Director, IT Portfolio Management and Systems Assurance

This position is responsible for directing implementation of the enterprise information technology security strategy. The Director, IT Portfolio Management and Systems Assurance, reporting to the CIO, will:

1. Coordinate the development, approval process, and maintenance of enterprise information technology security policies, standards and guidelines.
2. Liaise with all constituents comprising the Information Technology Decision-Making Framework regarding systems assurance initiatives.
3. Coordinate information technology compliance initiatives in a holistic manner, encompassing security, privacy, legislative, and risk mitigation controls.

IT Security Officer

This position is responsible for operational coordination of security incident responses and IT security policies spanning the enterprise. The IT Security Officer, reporting to the Director, IT Portfolio Management and Systems Assurance will:

1. Investigate IT security incidents and coordinate their resolution as defined in the University of Guelph Acceptable Use Policy.
2. Administer security-related services (e.g. vulnerability scanning) on behalf of the CIO.
3. Develop and implement an enterprise information security awareness program.
4. Liaise with CCS, ISC and ITSIG on information security issues and initiatives.
5. Collaborate with campus police, physical resources, external agencies, audit services, and University administration on IT security issues.
6. Coordinate investigation and responses to external and internal IT security threats or compromises.
7. Consult with University departments on maintenance of their Disaster Recovery Plans and align them with the risk management strategy developed by the University Risk Management Steering Committee.

Organizational Unit IT Support and the Information Technology Special Interest Group (ITSIG)

ITSIG is a formalized grouping of individuals across the University with interest or responsibilities related to information technology. Representing individual departments/units, ITSIG members act as liaison for timely and relevant information flow between the CIO, CCS and the University campuses.

Within the IT security domain, ITSIG members and other Departmental IT support staff will:

1. Receive notifications or tickets regarding security incidents relevant to departmental/unit computer systems and disseminate such information to appropriate technical personnel for resolution.

2. Receive network alerts, outage notifications, vulnerability advisories, or other infrastructure service notifications which affect the department/unit and disseminate such information to appropriate personnel.
3. Coordinate departmental responses to computer security incidents.
4. Liaise with the University IT Security Officer on related issues.

Individual Responsibilities

Every member of the university community is responsible for protecting the security of university information and IT systems by adhering to the objectives and requirements stated within published university-level information technology and IT security policies. In addition, individuals are required to comply with the additional security policies, procedures, and practices established by their respective colleges, departments or other units.

Specific responsibilities for all individuals employed at the University include the following:

1. Maintain awareness of and abide by the conditions set out in the University's Acceptable Use Policy (AUP).
2. Maintain awareness of and abide by IT policies set out by the University, and their department or college
3. Maintain computing accounts, application access and individual computing devices in a secure manner.
4. Report any security incidents or privacy breaches to the appropriate area.

Exceptions

Any exceptions to this policy should be submitted to the CIO for review and possible approval.

Version, Change and Approval History

Final Draft published: November 25, 2009 (minor editing only)

Third Draft published: June, 2009 (minor revisions as per ITSC review)

Second Draft published: May, 2009 (Clarified terminology regarding Policy Framework)

First Draft published: February, 2009