University of Guelph Information Security Documents

This document provides the current list of approved Information Security Policies, Standards and Guidelines for the University. **AS OF: October, 2013**

The policy numbering structure reflects the organizational framework of ISO 27002, the international best practice guideline for information security. References shown are the applicable ISO 27002 section as well as the Payment Card Industry Data Security Standard (PCI DSS), and where applicable the SANS 20 'Critical Security Controls'.

Approved Policies, Standards and Guidelines

Reference Number	Policy/Standard/Guideline	Associated Standards/Regulations	
0.0	**Formalized Information Security Policy Framework** (Approved Dec. 24, 2009) 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.	**ISO 27002**	3.1 Information Security Policy
		PCI	12.1 Establish, publish, maintain, and disseminate a security policy

3.1	**POLICY:** **Acceptable Use Policy** (Approved Dec. 3, 2012) The AUP (full name University of Guelph Acceptable Use Policy for Information Technology) defines the acceptable use and breaches of acceptable use of information technology resources at the University. The policy applies to anyone who uses or accesses any IT resource belonging to, or under the control of or in the custody of, the University of Guelph.	**ISO 27002**	7.1.3 Rules for acceptable use of information and assets should be identified, documented and implemented
		PCI	12.3 Develop usage policies for critical technologies and define proper use of these technologies.
6.2	**POLICY: Roles & Responsibilities for Information Security** (Approved Dec.4, 2009) Excerpt: "The Chief Information Officer (CIO) is responsible for sponsoring, developing, and implementing a comprehensive information technology security strategy and policy framework 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."	**ISO 27002**	6.1 Internal Organization for Information security
		PCI	12.5 Assign to an individual or team responsibility for account administration and access monitoring.
7.4.2	**POLICY:** **Wireless Network Policy** (Approved April 23, 2010) This policy applies to all uses of WLAN technologies at all physical locations on the University campuses, both inside buildings and outdoor areas. Exceptions may only be granted by the Chief Information Officer (CIO). It does not apply to cellular wireless technology.	**ISO 27002**	10.6.1 Special controls should be established to protect confidentiality and integrity of data passing over public or wireless networks.
		SANS 20	#7 Wireless Device Control
		PCI	11.1 Test for presence of unauthorized wireless access points on a quarterly basis.
8.6	**POLICY:** **Vulnerability Management** (Approved Dec. 4, 2009) Excerpt: "Vulnerability management is an important foundational component of the University's security program. The process of network discovery/scanning, identification of vulnerabilities, assessment, patching and mitigation is referred to as vulnerability management. A centrally-administered vulnerability assessment (VA) service will be utilized to discover vulnerabilities anywhere within the university technology environment, manage remediation of identified vulnerabilities, and monitor compliance."	**ISO 27002**	12.6.1 Timely information about technical vulnerabilities of information systems being used shall be obtained, and appropriate measures taken to address the associated risk.
		SANS 20	#4 Continuous vulnerability assessment and remediation.
		PCI	6.1 Ensure all system components and software are protected from known vulnerabilities. 6.2 Establish a process to identify and assign a risk ranking to newly discovered security vulnerabilities. 11.2 Run internal and external network vulnerability scans at least once a year.

8.6	**STANDARD:** This document lists the detailed standard practice and responsibilities associated with information technology infrastructure vulnerability assessment and vulnerability management activities. The standards and activities are in operational support of the University's Vulnerability Assessment Policy (CIO-ITSecurity-08.6).	**ISO 27002**	12.6.1 Timely information about technical vulnerabilities of information systems being used shall be obtained, and appropriate measures taken to address the associated risk.
8.3	**POLICY: End-point Encryption** (Approved Dec. 4, 2009) Excerpt: "Encryption supports data privacy and integrity by providing a method to convert electronic information into a format that is readable only by authorized individuals. This policy establishes that use of whole disk encryption for electronic information in storage shall be consistent with legislative requirements and the university's need for protection against accidental disclosure. This policy applies to all academic and administrative electronic information stored on portable devices, and information custodians."	**ISO 27002** **PCI**	12.3 Deploy formal encryption standards 15.1 Important records shall be protected from loss, destruction and falsification, in accordance with statutory and business requirements. 11.5 Deploy file integrity monitoring tools on all system components.
9.1	**POLICY: Major Incident Response and Management** (Approved May 4, 2011) Excerpt: "This Policy defines a standard University-wide process for managing major information technology security incidents, references related University Policies, outlines preparations in advance of incidents occurring, and specifies a coordinated and managed response and escalation process. A Policy Appendix charters an Information Security Incident Coordination Team (ISICT)."	**ISO 27002** **SANS 20** **PCI**	6.3 Responding To Security Incidents And Malfunctions 8.1.3 Incident management procedures 12.1 Compliance With Legal Requirements #18 Incident response and management 12.9 Implement an incident response plan
n/a	**POLICY: Mass Electronic Mail** (Approved Nov. 21, 2003) For the purposes of this policy, mass email shall be considered to be any unsolicited electronic mailing in which the message is sent to members of the University community using the CCS database of email addresses. This policy does not apply to individual email-based distribution and discussion groups such as listservs or established data bases that serve University learners/clientele.		

n/a	**POLICY: Record Retention and Disposition** (Approved Jan. 2006) Excerpt: "The overall purpose and objective of a record retention system is to ensure that all University records are managed in conformance with acceptable information and document management practices. A record retention system includes the identification, classification and retrieval, storage and protection, receipt and transmission, retention, and disposal or archival preservation of the recorded information."		
	Guideline: IT Asset Management and Disposal (Issued April, 2010) IT Assets require distinct tracking and disposal procedures for security and legislative compliance reasons. The Guideline provides advice focused on preventing inadvertent disclosure of sensitive information stored on computing equipment including desktop and portable computers, mobile devices and printers/copiers.	**ISO 27002**	7.1.1 All assets shall be clearly identified and an inventory of all important assets maintained.
	Guideline: Software-as-a-Service (Issued April, 2008) SaaS deployment options often bring faster business benefits and return-on-investment (ROI); frequent, automatic software updates; and potential independence from IT (and installed infrastructure). The SaaS delivery model (also known as 'on demand' applications) is an increasingly attractive alternative, however it is important to recognize risks, strengths and weaknesses of the SaaS approach, and this is the purpose of this paper.	**ISO 27002** **PCI**	
	Guideline: IT Contracting (Issued April, 2010) Departments should **consider risk and contingency plans** when engaging third-parties, assessing potential over-reliance on technical expertise, specifying how security incidents will be dealt with, escalation procedures and performance issues.olicy Purpose	**ISO 27002** **PCI**	6.2.1 Risks to information and processing facilities from business processes involving external parties should be identified and appropriate controls implemented before granting access. 12.8 Manage service providers' use of cardholder data.
	IT Policy Development Process		
