POLICY TITLE:	**Vulnerability Assessment Policy**
POLICY #:	CIO-ITSecurity – 08.6
Initial Draft By - Position / Date:	Doug Badger - Director, IT PMO / Feb.26, 2009
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 a centrally administered vulnerability assessment process. The Office of the CIO/Portfolio Management Office coordinates the service to assist University departments in managing system vulnerabilities.

Table of Contents

Introduction

Vulnerability management is an important foundational component of any information security program, which includes network protection (e.g. firewalls, virtual private networks VPN’s), access controls, physical security, etc. The process of network discovery/scanning, identification of vulnerabilities, assessment, patching and mitigation is referred to as vulnerability management.

This policy covers a centrally-administered vulnerability assessment (VA) service, provided by the IT Portfolio Management and Systems Assurance Office (PMO). The VA service uses a software tool which examines the services, ports, accounts and programs on servers and other ‘end-point’ devices, and compares the results with a database of known vulnerabilities. These vulnerabilities are the same exposures that are commonly used by hackers to gain unauthorized access or to deny services to a system.

The exposures are often identified by their Common Vulnerability and Exposure identifiers (CVE) which are unique codes for publicly known security vulnerabilities. The vulnerability assessment tool also applies a rating to the vulnerability that is proportional to the relative ease, severity of exploit or frequency of occurrence. A ticket may be created to track the vulnerability until it is resolved.

Policy Statement

1. Vulnerability assessment will be provided by the Portfolio Management Office across the University’s technology infrastructure as a service to the university community, and as an integral component of the University’s IT security program.

2. A CIO-approved and centrally managed vulnerability management tool will be utilized to discover vulnerabilities anywhere within the University of Guelph technology environment; manage remediation of identified vulnerabilities, and monitor compliance.

3. The IT Security Officer will have oversight capabilities sufficient to monitor compliance with vulnerability standard practice (separately documented). Any significant outstanding vulnerabilities will be communicated to the applicable system administrator, and may be escalated to the senior manager responsible for the applicable service or network sub-net.

4. The IT Security Officer is responsible for account privileges within the vulnerability management application. Authority to perform vulnerability scans will be granted to designated personnel within University departments, and restricted to only those systems within the department's accountability.

5. External vulnerability scans will be run periodically by a third-party computer security company against a representative set of systems or sub-nets, as determined by the Chief Information Officer (CIO). These results will be compared to the internally generated reports. Any major discrepancies will be escalated to the vulnerability assessment tool vendor's technical support group.

6. This policy will be enforced by the CIO/Portfolio Management and Systems Assurance Office; non-compliance may result in suspension of network access to/from applicable devices.

A procedural Practice Standard describing utilization of the vulnerability scanning tool, scheduling network/sub-net discovery and server/device scans, and addressing identified vulnerabilities (i.e. remediation), is documented separately from this Policy (reference Vulnerability Assessment Practice Standard).

Exceptions

Any exceptions to this policy, (such as utilization of a departmental tool, or requesting exemption from the VA service), should be submitted to the University's Chief Information Officer (CIO) for consideration.

Version, Change and Approval History

Final Draft Revision: November 25, 2009 (minor editing)

Draft Revision: February 26, 2009 (minor editing and formatting changes and document re-numbering in accordance with IT Security Policy Framework)

First Draft published: March 20, 2008