Vulnerability Assessment Standard Practice

Effective: December 4, 2009

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).

1. All automated security scans to determine compliance with the Vulnerability Assessment Policy will use the highest practical level of scanning. For production machines or critical services, 'aggressive mode' and 'Denial of Service' attacks should **not** be run. However, for development or test systems, all scanning levels should be run to identify exposures in their production counterparts.

2. The IT Security Officer is responsible for setting scheduled scan times in conjunction with applicable system/network administrators; ensuring scans do not interfere with other services.

3. Designated system/server administrators responsible for individual or groups of systems will determine the appropriate scanning levels to be used, in consultation with the IT Security Officer.

4. Each department should run discovery sweeps on their subnets at least once a month to identify all active systems. Any discrepancies between the results and their inventory of authorized, installed systems on their subnets should be communicated to applicable department management for investigation.

5. Each department is responsible to ensure that the scans for systems that they are accountable for are carried out with a frequency agreed with the IT Security Officer.

6. By default, most systems will be scanned weekly or after any changes that could compromise the security of the system (such as applying an untested patch), or upon notification of a potential vulnerability. Designated systems administrator(s) will determine if changes are significant enough to warrant a new ad hoc scan.

7. Vulnerabilities designated as **High** or **Medium** as identified by scheduled and/or ad hoc scans will generate open 'tickets' within the vulnerability assessment application. Open 'tickets' will be monitored by the IT Security Officer.

8. **High** vulnerabilities (as defined by the scanning tool) should be addressed (i.e. patched) within **14** days or an exception discussed and agreed with the IT Security Officer.

9. **Medium** vulnerabilities (as defined by the scanning tool) should be addressed (i.e. patched) within **60** days or an exception discussed and agreed with the IT Security Officer.

10. If a ticket remains open beyond the above indicated time period, the IT Security Officer will first notify the designated system/server administrator about the overdue ticket. If necessary, this issue will be escalated to management if excessive time to fix the problem is encountered.

11. Any **High** or **Medium-level** exposure that is considered to be a **'false-positive'** and to be systematically ignored for any area of the University requires documentation indicating that the exposure/exploit is not applicable or invalid, and agreement with the IT Security Officer.

12. All **'false positive'** documentation/explanations should be e-mailed to the IT Security Incident mail-box (incident@uoguelph.ca) or recorded within the VA application ticket.

13. The IT Security Officer will verify compliance with this Practice Standard, report non-compliance to the applicable departmental manager, and escalate unresolved issues within **thirty days** to senior management, including the Chief Information Officer (CIO).

14. The IT Security Officer will produce a **monthly report** to the CIO, summarizing the Vulnerability Assessment service, including the number of devices being regularly scanned and the number of devices 'discovered' by the VA tool. The report should highlight the number of open and overdue vulnerabilities (tickets).

Version, Change and Approval History

Final Draft Revision:	November 25, 2009 (minor text changes)
Draft Revision:	February 26, 2009 (simplified and streamlined text, revised mitigation response dates, documented escalation and reporting required); document re-numbered in accordance with the IT Security Policy Framework.
First Draft published:	March 20, 2008