POLICY TITLE:	**Vulnerability Management Policy**
APPROVED BY / DATE:	**Robert Devries, CIO – October 4, 2023**
Last Revised Date:	**October 4, 2023**
Next Review Date:	One year after Approval
BRIEF DESCRIPTION:	This document describes the required usage of a centrally administered vulnerability management process. The CCS Information Security team coordinates the service to assist University departments in managing system vulnerabilities.

Table of Contents

Introduction

Vulnerability Management is a foundational component of the University of Guelph's information security program which includes the identification, assessment and remediation of discovered IT security vulnerabilities. Responsibility for the on-going effort to reduce vulnerabilities on University-owned information technology assets is shared between service/system/application owners and CCS.

Vulnerabilities represent a risk to the University as they could be exploited by attackers to gain unauthorized access to the campus network or to deny services to the broader campus community. This policy covers the centrally administered vulnerability assessment and management service provided by the CCS Information Security team. This service uses software tools to examine the operating system, software, ports, and services on servers and other endpoint devices, and then compares the results with a database of known vulnerabilities.

Scope

All devices owned by the University, devices connected to the University network, and devices that store University-owned data are in scope of this policy regardless of ownership. This includes personally-owned devices connected to the University network and third-party hosted services utilized by the University.

Policy Statements

1. Vulnerability management services will be provided by the CCS Information Security team across the University's technology infrastructure. This is an integral component of the University's information security program.

2. Centrally managed vulnerability management tools will be utilized to discover vulnerabilities internal to the University of Guelph technology environment and to monitor compliance.

3. External vulnerability scanning tools will be leveraged to identify publicly exploitable vulnerabilities in University systems. Information Security may also engage third-party security vendors to run periodic penetration tests against a representative set of systems or networks, as determined by the Chief Information Officer (CIO) and Chief Information Security Officer (CISO). These results will be compared to the internally generated reports, and system owners will be contacted to address any significant findings.

4. The CISO will have oversight capabilities sufficient to monitor compliance with this policy and the vulnerability standard practice found in Appendix A. Any significant outstanding vulnerabilities will be communicated to the applicable system administrator and may be escalated to the senior leader responsible for that service.

5. The CISO is responsible for account privileges within the vulnerability management application. Authority to perform vulnerability scans and access scan results will be granted to designated personnel within University departments and restricted to only those systems within the department's accountability.

6. Discovered vulnerabilities will be evaluated using the Common Vulnerability Scoring System (CVSS) and rated as Critical, High, Medium, Low, or Informational. Ratings may be adjusted by Information Security based on compounding or mitigating factors.

7. Systems found to have vulnerabilities, regardless of ownership, may be disconnected from the network at any time with little or no notice in the event that a discovered vulnerability poses an immediate risk to the University.

8. System owners are responsible for timely response to and remediation of all discovered vulnerabilities on systems under their administration in accordance with the practice standard below. Based on the risk, failure to address vulnerabilities may result in vulnerable systems being denied network access.

9. Risks that cannot be remediated or adequately mitigated will require written risk acceptance from the appropriate business owner of the unit/department such as the VP, Dean, or Chair. Risk acceptance is subject to the exception approval process within this policy, which includes approval by the CISO and CIO. Requests may be denied if they represent too great of a risk to the University, including technical, financial, or reputational risk.

10. While personally owned devices are not specifically in-scope of this policy, they may be scanned for known vulnerabilities when connected to the University network. In the event of a critical vulnerability or significant risk discovered on a personally owned device, Information Security will contact the owner to remediate the issue. Depending on the risk associated with the issue, network access may be suspended with little or no notice for that device.

11. Third-party hosted applications and services will be monitored for publicly disclosed vulnerabilities, but are not actively scanned by Information Security. In the event of a significant vulnerability, the system/service owner is responsible to coordinate with the vendor and Information Security to ensure timely remediation and protection of University data.

12. This policy will be enforced by CISO on behalf of the CIO. Non-compliance may result in suspension of network access for applicable devices.

Related Policies, Guidelines, and Processes

- Acceptable Use Policy
- Data Storage Guidelines
- Security Risk Assessment Process

Responsibilities

1) **Server and Application Owners and those responsible for managing Endpoint Computing Devices**
    i) Understand and adhere to the requirements of this policy, related polices and guidelines, and departmental procedures for those servers and applications within their unit.
    ii) Keep all systems and applications updated with the latest security updates.
    iii) Review and remediate all vulnerabilities identified by Information Security in a timely manner according to the standard practices in Appendix A.
    iv) Notify the Information Security team regarding any false-positive detections.
    v) Monitor vendor security advisories related to services managed or contracted by their unit, and address all security vulnerabilities according to the standards in Appendix A with both the vendor and Information Security. When in doubt about the severity of a vulnerability, contact Information Security for assistance.
    vi) Monitor security compliance for devices and endpoints under their management. Security best practice is to enable automatic updates for the operating system and applications on all managed endpoint devices.
    vii) Contact Information Security promptly regarding any vulnerabilities that cannot be resolved or mitigated.

2) **Managers, Department Chairs, Unit Heads, and Directors**
    i) Accountable for the management and regular updating of servers and applications within their respective units, including the remediation of identified vulnerabilities according to the standards in Appendix A.
    ii) Follow the exception process within this policy for any risks that cannot be remediated or adequately mitigated.

3) **Information Security**
    i) Provide effective methods and resources to users, IT administrators, and departments to ensure that this policy can be effectively and efficiently implemented.
    ii) Undertake annual reviews of this policy and associated processes in collaboration with supporting IT groups.
    iii) Maintain the vulnerability scanning infrastructure.
    iv) Manage vulnerability scans to ensure full coverage of the University network.
    v) Schedule scan times in conjunction with applicable system/network administrators and ensure scans do not interfere with University services.
    vi) Provide the necessary account privileges within the vulnerability management application to designated personnel within University departments, and ensure they are restricted to only those systems within the department’s accountability.
    vii) Communicate discovered vulnerabilities to system owners and escalate as needed.
    viii) Collaborate with system owners as needed to understand detected security threats and potential mitigations.
    ix) Monitor vendor advisories for select core University systems and evaluate their relevance to the University. Advise affected departments when a significant vulnerability is announced which has the potential to impact University systems.
    x) Review advisories from higher education and research organizations (i.e. CanSSOC, ORION, etc.) and government organizations (i.e. Canadian Centre for Cybersecurity, RCMP, etc.). Share those advisories internally as needed and coordinate the response to all security threats and vulnerabilities.
    xi) Promote a culture of cyber security where all members of the University community follow security best practices, regularly review security advisories, and update systems and applications within their control on a regular basis.

4) Chief Information Security Officer (CISO)

i) Enforce this policy on behalf of the CIO.
i) In collaboration with the CIO, review and approve vulnerability management exception requests.
ii) Oversee the vulnerability management service and monitor compliance with the standard practice.
iii) Assist Managers, Department Chairs, Unit Heads, and Directors in understanding the risk associated with detected vulnerabilities and security threats.

5) CIO

ii) Review and provide final approval for vulnerability management exception requests.
iii) Review and approve changes to this policy.

Exceptions

Any exceptions to this policy, such as requesting an exemption from scanning or from remediation of a vulnerability, must be approved by both the CISO and CIO.

Exception requests submitted by the business unit are an indication that the business is willingly accepting the risk associated with not scanning or resolving a vulnerability. Requests will be reviewed by the CISO and CIO to ensure that the exception does not exceed the risk tolerance of the University and does not represent too great of a risk to the institution, including technical, financial, or reputational risk.

Exception requests should be sent to the CCS Information Security team (infosec@uoguelph.ca) and must include the following information:

1. Requesting campus unit
2. Requesting Manager, Department Chair, Unit Head, or Director
3. Contact information and business-level risk acceptance
4. Technical representative contact information
5. Date of request
6. Duration of the exception request
7. Description of the exception request
8. Reason for exception request

Definitions

Common Vulnerability and Exposure identifiers (CVE) – Vulnerabilities are commonly identified by their Common Vulnerability and Exposure identifiers (CVE) which are unique codes for publicly known security vulnerabilities. The CVE system is maintained by United States' National Cybersecurity FFRDC, operated by The MITRE Corporation. https://cve.mitre.org/

Common Vulnerability Scoring System (**CVSS**) – An industry standard for assessing the severity of computer system security vulnerabilities. CVSS assigns severity scores to vulnerabilities (0 to 10, with 10 being the most severe). Scores are calculated based on a formula that depends on several metrics that approximate ease and impact of an exploit. https://www.first.org/cvss/specification-document

False Positive – A false positive is a security alert incorrectly categorized as suggesting a threat when there is none.

Threat – A potential danger to an asset such as data or the network itself.

Vulnerability– A weakness in a system or its design that could be exploited by a threat.

Exploit - The mechanism that is used to leverage a vulnerability to compromise an asset.

Risk – The likelihood that a particular threat will exploit a particular vulnerability of an asset and result in an undesirable consequence.

Appendix A - Vulnerability Management Standard Practice

This appendix outlines the standard practice associated with the Information Security vulnerability management program. These standards and activities are in operational support of the University's Vulnerability Management Policy and describe the utilization of a vulnerability scanning tool, scheduling discovery and system scans, and the remediation of identified vulnerabilities.

1. The Information Security team will schedule scan times in conjunction with applicable system/network administrators, and ensure scans do not interfere with University services.

2. At a minimum, the following scans will be performed:
   a. A monthly discovery scan of the entire University network.
   b. Weekly scans of all servers and workstations.
   c. A bi-weekly scan of the networks in-scope of the PCI-DSS standard.

3. Continuous external scanning of the public University IP ranges will be undertaken using third-party tools and services. Information Security will regularly review the results of these scans and engage with system owners to take appropriate action when vulnerabilities are identified based on the risk.

4. Each department will be given access to the vulnerability management platform and are responsible for reviewing scan results for their servers and services on a regular basis.

5. Each department should review discovery scan results 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.

6. 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 Information Security team. Any scan delays or issues should be reported to the Information Security team for investigation.

7. By default, systems will be scanned weekly. Ad hoc scans may be scheduled at any time by contacting the Information Security team. This may include scanning after a change has been implemented or upon notification of a potential vulnerability. Designated systems administrators will determine if changes are significant enough to warrant an ad-hoc scan.

8. All automated security scans to determine compliance with the Vulnerability Management Policy will use the highest practical level of scanning. For production machines or critical services, ‘aggressive mode’ and ‘denial of service’ attacks are not to be run. However, for development or test systems, all scanning levels should be run to identify exposures in their production counterparts.

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

10. Vulnerabilities identified by scheduled and/or ad hoc scans will be tracked within the vulnerability management application. Unresolved vulnerabilities will be monitored by the Information Security team and regularly followed up on with the responsible administrator.

11. When notified of a vulnerability in a hosted application or service, the service owner and Information Security must jointly coordinate with the respective vendors to ensure vulnerabilities are addressed according to these standards.

12. Vulnerabilities will be assessed using the current version of the Common Vulnerability Scoring System (CVSS). Ratings may be adjusted higher or lower by Information Security based on compounding or mitigating factors. Action must be taken according to the following timelines:

	Risk Rating	**CVSS Score**	**Patching Timeline**
🟥	Critical	9.0 – 10.0	Within 48 hours
🟧	High	7.0 – 8.9	Within 14 days
🟨	Medium	4.0 – 6.9	Within 30 days
🟩	Low	0.1 – 3.9	Within 90 days
🟦	Informational		Not required

    If security updates are not available or cannot be applied in a timely manner, other security mitigations should be implemented. These mitigations could include, but are not limited to vendor suggested workarounds, blocking internet-facing services, restricting access to specific networks, and disabling specific services and accounts.

    Exact timing to address vulnerabilities will be influenced by several factors, including the availability of vendor updates and mitigation strategies, ease of exploit or active exploitation of a vulnerability in the wild, internal resourcing, and overall impact to the University. System owners should collaborate with Information Security on a patching strategy based on the criticality and risk involved.

13. Vulnerabilities and threats will be evaluated by the Information Security team based on the following criteria:
    a. Total number of affected systems and stake-holder population,
    b. Sensitivity and criticality of the system, application or data involved,
    c. Likelihood of the vulnerability causing a security incident,
    d. Operational impact to the department, the University or other stakeholders,
    e. Potential that this vulnerability will be exploited or if an exploit is already available, and
    f. Other potential impacts or mitigating circumstances

14. While dealing with multiple vulnerabilities simultaneously, system owners should consult with the Information Security team to determine the priority and take appropriate actions to remediate the risk associated with affected systems.

15. If a vulnerability remains unresolved beyond the above indicated time period, the Information Security team will first notify the designated system/server administrator about the overdue finding. If necessary, this issue will be escalated to management if excessive time to fix the problem is encountered. Issues must either be remediated or the risk accepted by the appropriate VP or Dean. Failure to remediate or accept the risk will result in systems being removed from the network until they can be addressed.

16. In instances where Information Security assesses that the vulnerability is significant, and time is of the essence, the CISO may request immediate security measures be put in place temporarily to mitigate the risk related to the vulnerability. In certain cases, such temporary security measures may be implemented prior to notifying the system owner in order to mitigate risks associated with the vulnerability.

17. Any exposures that are considered to be a 'false-positive' and which should be systematically ignored, require documentation indicating that the exposure/exploit is not applicable or invalid, and must be agreed upon with the CISO.

18. All 'false positive' documentation/explanations should be e-mailed to the Information Security team (infosec@uoguelph.ca).

19. The CISO will verify compliance with this practice standard, report non-compliance to the applicable departmental manager, and escalate unresolved issues to senior management, including the CIO.

20. The CISO will produce a monthly report to the CIO and Internal Audit summarizing the vulnerability management landscape, including the number of devices being regularly scanned and the number of open and overdue vulnerabilities.

21. In accordance with the policy, all exception requests, including those requests to exclude systems from scanning or to defer remediation of a specific vulnerability, must be submitted in writing by the appropriate manager, department chair, unit head, or director, and approved by the CIO.