Carleton UNIVERSITY

Canada's Capital University

Policy Name:	Vulnerability Management
Originating/Responsible Department:	Information Technology Services (ITS)
Approval Authority:	Assistant Vice-President (ITS) & Chief Information Officer
Date of Original Policy:	September 2015
Last Updated:	June 2018
Mandatory Revision Date:	June 2019
Contact:	Director, Information Security, ITS

Policy:

To ensure the confidentiality, integrity, and availability of information and information systems at the University, information security controls must be placed on the use of all technologies connected to the University, whether personal or University-owned.

Purpose:

The purpose of this Policy is to define the requirements for notification, testing, and installation of security-related patches, as well as procedures for the receipt, monitoring, triage, scanning, mitigation, and management of the vulnerabilities within the University network. The University will ensure that appropriate safeguards are in place and maintained, in order to protect sensitive data being processed, accessed and stored.

Scope:

This Policy applies to all departments and administrators who are responsible for electronic devices connected to the University network, including but not limited to, desktop and personal computers, servers, network switches, and routers. It states the security controls and processes that must be observed during the processing, accessing, or storage of sensitive University data (as defined in the Data Classification Policy).

Procedures:

1.0 Receipt and Monitoring of New Vulnerabilities

Owners of information systems and services are responsible for their proper maintenance. This maintenance includes the identification and remediation of security vulnerabilities.

There are numerous means to be notified of new vulnerabilities. One common method is through vendor alerts. Another method is through subscription services that provide all-in-one alerting services.

2.0 Vulnerability Triage

A risk ranking (*critical*, *high*, *medium*, or *low*) must be assigned to newly discovered security vulnerabilities based on the NIST (National Institute of Standards and Technology) Common Vulnerability Scoring System (CVSS) v2 rating system. The risk rankings will be assigned based on the following criteria:

- Exploitability

- Potential impact on the confidentiality, integrity, and availability of University systems, networks, and data
- Attack complexity
- Level of authentication needed to exploit the vulnerability

Vulnerabilities are considered **critical** if they pose an imminent threat to the environment, impact critical systems, would result in a potential compromise of confidential or sensitive information, or would impact the University's reputation if not addressed. All critical security vulnerabilities must be addressed within 30 days or sooner depending on risk assessment.

For more information on risk ranking and CVSS scores, consult http://nvd.nist.gov/.

3.0 Scanning for Known Vulnerabilities

Vulnerability scans must be performed quarterly on information systems and network infrastructure that:

- Provide business critical functions
- Contain confidential or sensitive information such as Personally Identifiable Information
- Contain sensitive or unpublished research data
- Are in scope for the Payment Card Industry Data Security Standard (PCI DSS)

For information systems and network infrastructure that are in-scope for compliance to PCI DSS, external vulnerability scans (originating from outside the University network) must be performed quarterly, and after any significant change in the network, via an Approved Scanning Vendor (ASV) approved by the Payment Card Industry Security Standards Council (PCI SSC). Follow-up scans must be performed to validate mitigation effectiveness.

At the completion of vulnerability testing, all discovered vulnerabilities must be documented, assigned a risk ranking, and then one of the following actions must be taken and documented. The vulnerability must be:

- Remedied or eliminated
- Determined to be a false positive
- Mitigated using compensating controls
- Accepted with its associated risk

Critical vulnerabilities that are *accepted* must be approved by the Director, Information Security, ITS or the Chief Information Officer.

System configuration standards must be updated when vulnerabilities require configuration changes.

4.0 Vulnerability Mitigation

Anti-virus and/or host-based intrusion software must be deployed on all systems that support such software, particularly personal computers and servers. The anti-virus software must be actively running on these devices and kept up-to-date.

Applicable vendor-supplied security patches must be installed to ensure that all system components and software are protected from known vulnerabilities. *Critical* security patches must be applied within 30 days of release or sooner based on the outcome of a risk assessment.

Specific vulnerability mitigation control requirements include:

- A firewall must be installed at each Internet connection and between any de-militarized zone (DMZ) and the internal network zone
- Internet ingress traffic must be permitted using a white list approach

- Firewall stateful inspection, also known as dynamic packet filtering, must be implemented (that is, only “established” connections are allowed into the network)
- Private IP addresses and routing information must never be disclosed to unauthorized parties

For systems in scope of PCI DSS:

- Firewall and router rule sets must be reviewed at least every 6 months
- Inbound and outbound traffic must be restricted to that which is necessary for the cardholder data environment, and all other traffic must be specifically denied.
- Perimeter firewalls must be installed between all wireless networks and the cardholder data environment, and they must be configured to deny or, if such traffic is necessary for business purposes, permit only authorized traffic between the wireless environment and the cardholder data environment

Roles and Responsibilities

ITS is responsible for:

- Ensuring that, for systems supported by ITS:
    - Anti-virus mechanisms are current vendor supported versions and are actively running and cannot be disabled or altered by users, unless specifically authorized by management on a case-by-case basis for a limited time period
    - Anti-virus and intrusion detection or prevention capabilities are maintained at current signature levels
    - Maintain operating system, firmware and applications at current security patch levels
- Ensuring that anti-virus programs are capable of detecting, removing, and protecting against all known types of malicious software
- For systems considered to be not commonly affected by malicious software, performing periodic evaluations to identify and evaluate evolving malware threats to confirm whether such systems continue to not require anti-virus software
- Ensuring that all anti-virus mechanisms are maintained as follows:
    - Are kept current
    - Perform periodic scans and updates
    - Generate audit logs which are retained as per PCI DSS
- Ensuring that security policies and operational procedures for protecting systems against malware are documented, in use, and known to all affected parties
- Reviewing firewall and router rule sets at least every six months

Department and System Administrators are responsible for:

- Ensuring that, for systems supported by departments or CSUs:
    - Anti-virus mechanisms are actively running and cannot be disabled or altered by users, unless specifically authorized by management on a case-by-case basis, and for a limited time period
    - Anti-virus and intrusion detection or prevention capabilities are maintained at current signature levels
    - Patching of information systems, including all aspects of operating system, firmware, and software, are maintained at current security patch levels
    - Ensuring that vendor products that are support discontinued are:
        - Updated to current vendor support levels;
        - Replaced with products that are vendor supported; or
        - Have appropriate mitigation applied that adequately protects the information system.

Compliance
Non-compliance to this Policy may result in disciplinary action.

Contacts:
Director, Information Security, ITS

Links to Related Policies:
http://www.carleton.ca/secretariat/policies/

- Acceptable Use Policy for Information Technology
- Data and Information Classification and Protection Policy
- Desktop and Notebook Computer Equipment
- Mobile Technology Security Policy
- Password Policy for Information Systems
- Remote Network Access

http://carleton.ca/privacy/privacy-policies/

- Carleton's Privacy Policies