a place of mind
THE UNIVERSITY OF BRITISH COLUMBIA

# INFORMATION SECURITY STANDARD M5
# Vulnerability Management

## 1. Introduction

1.1 This document defines standards for protecting UBC Systems through vulnerability management, which is a security practice designed to proactively reduce the chance of exploitation of IT vulnerabilities. Effective vulnerability management includes patch management, vulnerability scanning, vulnerability mitigation, malware protection and secure configuration of systems, particularly firewalls. Unless otherwise stated in this standard, vulnerability management is the responsibility of University IT Support Staff.

1.2 This standard applies to UBC Systems containing Medium, High or Very High Risk Information, and may also be applied to UBC systems containing Low Risk Information where appropriate.

1.3 University IT Support Staff with access to Privileged Accounts, and all IT professionals must also comply with the System Administrators' Code of Ethics.

1.4 The Chief Information Officer has issued this standard under the authority of Policy SC14, Acceptable Use and Security of UBC Electronic Information and Systems. Questions about this standard may be referred to information.security@ubc.ca.

## 2. Patch Management

2.1 University IT Support Staff are responsible for subscribing to the Appropriate Notification Services to ensure they are aware of new vulnerabilities and corresponding patches as soon as they are available.

2.2 Patch management procedures must prioritize patches based on the severity of the vulnerability being patched, the sensitivity of the data in the system, and the criticality of the system to University Business. For additional guidance on patching prioritization, refer to the Vulnerability Awareness & Patching Prioritization guide. A back-out or roll-back procedure should also be in place so that the patch can easily be removed in the event of a serious problem.

2.3 Backups should be completed before applying any significant patches, in case of unexpected problems.

2.4 Operating system and application updates/patches must be installed as follows:

2.4.1 to the extent possible, desktops, laptops and servers must be configured to install these updates and patches automatically;

2.4.2 where automatic installation is not feasible, all security-related updates and patches must be manually installed at the earliest opportunity, in accordance with their severity, as outlined in section 2.5 below;

2.4.3 where it is impractical or impossible to install security-related updates and patches, the risks must be mitigated with compensating controls approved by the CISO; and

2.4.4 where the system is at end of life and security-related updates and patches are no longer available from the vendor, then you must either upgrade the system or implement compensating controls approved by the CISO.

2.5 Unpatched software is frequently exploited by malicious individuals to access information or resources. To mitigate this threat, vendor provided patches for UBC Systems (e.g. operating systems, applications, databases, etc.) must be patched, with service outages where required, in accordance with Severity Ratings for Vulnerabilities (CVSS) or as defined by the vendors or other third parties as follows:

2.5.1 Critical-Severity Vulnerabilities as soon as possible, preferably within 72 hours of the patch release;

2.5.2 High-Severity Vulnerabilities as soon as possible, preferably within 14 days of the patch release; and

2.5.3 Medium-Severity Vulnerabilities as soon as possible once all Critical and High-Severity Vulnerabilities have been resolved.

2.6 Instrumentation systems that are network-connected and run Windows embedded operating system or any other embedded operating system that can only be patched by the hardware vendor are examples of IoT Devices or appliances (including virtual appliances), and frequently will have vulnerabilities for which there are no patches to protect the system. In this case, it is important to look at compensating controls, which will protect the system and reduce the risk of unauthorized access to information or resources. A possible compensating control may be to isolate the system, so that it has no access to the internet or other systems, with the exception of a "proxy" system. The proxy system will be able to access other computers and the internet and through a dedicated interface, it can communicate with the system. Provided the proxy system can be well patched and secured, the risk of access to the unpatched system is reduced to a reasonable level by this control. For additional information on securing IoT Devices, see the Securing Internet of Things (IoT) Devices standard.

## 3. Vulnerability Scanning

3.1 The Office of the CIO is responsible for ensuring that all operational UBC Systems attached to the UBC network are scanned with a network vulnerability scanning tool (e.g. Nessus) at least every quarter.

3.2 The Office of the CIO is responsible for scanning Web Applications on UBC Systems attached to the UBC network with a web application scanning tool.

3.3 University IT Support Staff have the responsibility to obtain a vulnerability scan for all new or substantially modified Internet-facing servers and applications attached to the UBC network prior to going into production. Any detected vulnerabilities must be resolved in accordance with their severity, as outlined in section 2.5 above; rescans are required until passing results are obtained.

3.4 University IT Support Staff must not block UBC's Vulnerability Scanners.

## 4. Penetration Testing

4.1 It is highly recommended that Penetration Testing be conducted for UBC Systems containing or processing High or Very High Risk Information. To find a qualified penetration testing service, contact information.security@ubc.ca.

## 5. Malware Protection and Hardening

5.1 Anti-malware software protects against malicious code and is another layer of defense to help protect against exploitation of vulnerabilities.

5.2 Desktops, laptops and servers connected to UBC's network or other networked resources must have anti-malware software installed and configured, so that the virus definition files are updated daily. The anti-malware software must be actively running on these devices and kept up-to-date.

5.3 Unused services on servers should be disabled, and operating systems and applications should be hardened against external threats, see the UBC Systems and Applications Hardening Guides for recommended configurations.

5.4 Applications should be appropriately hardened against attacks. For configuration guidance on your specific application, see the Mozilla Observatory. For additional help, contact UBC Cybersecurity.

## 6. Firewall Configuration

6.1 Firewalls provide an effective compensating control for many types of vulnerabilities for which patches are not readily available; these are known as zero-day vulnerabilities. UBC Systems storing Medium, High or Very High Risk Information must be protected by a firewall.

6.2 Firewalls are only as effective as their Access Control List (ACL) rule set, which determines how traffic is blocked or passed. Firewall ACL rule sets must be configured as follows:

6.2.1 a "Deny by Default" policy must be implemented on all firewalls;

6.2.2 services that are not explicitly permitted must be denied;

6.2.3 firewalls must use ingress filtering at a minimum and must use egress filtering if it is used to protect High or Very High Risk Information;

6.2.4 ACLs must restrict traffic to the minimum necessary to conduct University Business; and

6.2.5 rule sets must be reviewed annually for optimization and validation of effective rules.

6.3 Network-based firewalls configured to control access to different zones must be dedicated firewalls. Firewalls should never be used for multiple purposes beyond access control and monitoring. Next Generation firewalls, Unified Threat Management (UTM) and virtual firewalls are still considered to be dedicated.

6.4 Where high availability is required, standby firewalls should be configured to take over the services of primary firewalls in the event that the primary fails. This also implies that standby firewalls must be kept up to date with changes made to the primary firewall to properly support this capability.

6.5 If a firewall becomes a single point of failure, it must fail in a closed state and not allow passage of data traffic through it.

6.6 The firewalls must be capable of “stateful packet inspection” and this capability must be turned on.

6.7 All firewall critical alarms must generate an automatic notification to the firewall administrator.

6.8 Host based firewalls should be used if available, in addition to network firewalls; this facilitates defense in depth.

6.9 All firewall logs should be sent to a separate machine solely dedicated to the collection of logs at an appropriate level.

## 7. Related Documents and Resources

System Administrators’ Code of Ethics

Policy SC14, Acceptable Use and Security of UBC Electronic Information and Systems

Appropriate Notification Services guideline

Vulnerability Awareness & Patching Prioritization *(with CWL credentials)*

Severity Ratings for Vulnerabilities (CVSS)

Securing Internet of Things (IoT) Devices standard

UBC’s Vulnerability Scanners *(with CWL credentials)*

UBC Systems and Applications Hardening Guides

Mozilla Observatory