Vulnerability & Patch Management Policy

Table of Contents

[Background 3](#_Toc16771913)

[Purpose 3](#_Toc16771914)

[Definitions 3](#_Toc16771915)

[Vulnerability & Patch Management Policy 4](#_Toc16771916)

[Responsibilities 5](#_Toc16771917)

# Background

**[Describe The Background Of Why A Vulnerability & Patch Management Policy Has Come About.]**

The **[Business Name]** acknowledges the need to protect its information technology (IT) assets throughout their lifecycle through effective management of identified vulnerabilities through the timely deployment of appropriate security patches

Therefore, the **[Business Name]** is establishing this Vulnerability & Patch Management Policy and establishing a program to implement a systematic process that joins information security with information technology and IT governance functions to protect IT assets throughout their lifecycle for the **[Business Name]** IT environment.

The main objective is to correct a lack of a formal, vulnerability and patch management, program that has led to an increase of risk of a cyberattack on the **[Business Name]** IT environment. Implementing the vulnerability & patch management program will also achieve compliancy with relevant government mandates, policy, and guidance, including, but not limited to, the following:

**[If Necessary, Mention Any Formal Mandates That Your Business Is Required To Adhere To]**

# Purpose

**[Describe What The Intent Of This Document Will Be.]**

This document establishes the Vulnerability and Patch Management Policy for **[Business Name]**. This policy defines requirements for the management of information security vulnerabilities and the notification, testing, and installation of security-related patches on devices connected to **[Business Name]** networks.

# Definitions

**[Define Any Terms That Are Used Throughout This Document.]**

|  |  |
| --- | --- |
| Terms | Definition |
| Information Resources | **Information Resources**: **[Business Name]** Information and related resources, such as equipment, devices, software, and other information technology. |
| Information System Owner | **Information System Owner**: The individual(s) or Unit responsible for the overall procurement, development, integration, modification, and operation and maintenance of an Information System. This individual or Unit is responsible for making risk tolerance decisions related to such Information Systems on behalf of **[Business Name]** and is organisationally responsible for the loss, limited by the bounds of the Information System, associated with a realised information security risk scenario. |
|  |  |
|  |  |
|  |  |
|  |  |

# Vulnerability & Patch Management Policy

**[Describe What & How The Policy Will Be Implemented, Managed And Measured.]**

All **[Business Name]** IT assets shall be managed in accordance with all Government mandates, and **[Business Name]** policy and procedures. This policy establishes the business rules and guidelines below for the vulnerability and patch management of IT assets throughout their lifecycle.

**Vulnerability Management,**

The **[Business Name]** shall:

Conduct routine scans of devices, systems, and applications connected to **[Business Name]** networks to identify operating system and application vulnerabilities.

All Information System Owners are required to ensure routine review of the results of vulnerability scans of devices, systems, and applications for which they are responsible and to evaluate, test, and mitigate, where appropriate, identified vulnerabilities.

Vulnerability scanning, and review shall be repeated as part of each annual risk assessment conducted pursuant to the Information Security Risk Management and System Security Plan, as well as each time a change is made that may introduce additional vulnerabilities. Information System Owners shall coordinate with the security team to schedule these scans and ensure timely (as determined by risk) review of findings.

**Patch Management,**

The **[Business Name]** shall:

Produce and maintain a Patch Management Standard that defines the minimum information security standards necessary to ensure the protection of **[Business Name]** Information and Information Resources. The minimum standards shall include the following requirements:

* A risk-informed systems patch cycle for all server operating systems (OS) shall be scheduled, as appropriate, for Information Systems and related subsystems.
* Any emergency patching outside of the routine patching schedule shall be done according to level of risk, as determined by the Information System Owner in consultation with the security team.
* Servers, services, or applications shall be maintained with current OS, application, or security patch levels, as recommended by the software manufacturer and informed by risk, to protect **[Business Name]** Information from known information security issues.

**Remediation Schedule,**

The **[Business Name]** shall upon receipt of the vulnerability reports:

* Review Results
* Develop Remediation Pan

Vulnerability remediation is to be completed as per the below guidelines.

|  |  |  |
| --- | --- | --- |
| Severity | Description | Target Remediation Time |
| Critical | Critical vulnerabilities have a CVSS score of 8.0 or higher. They can be readily compromised with publicly available malware or exploits. | **[Insert Target Remediation Time]** |
| High | High-severity vulnerabilities have a CVSS score of 8.0 or higher. There is no known public malware or exploit available. | **[Insert Target Remediation Time]** |
| Medium | Medium-severity vulnerabilities have a CVSS score of 6.0 to 8.0 and can be mitigated within an extended time frame. | **[Insert Target Remediation Time]** |
| Low | Low-severity vulnerabilities are defined with a CVSS score of 4.0 to 6.0. Not all low vulnerabilities can be mitigated easily due to applications and normal operating system operations. These should be documented and properly excluded if they can’t be remediated. | **[Insert Target Remediation Time]** |
| Informational | Information vulnerabilities have a CVSS score lower than 4.0. These are considered risks but are generally reference information for the state and configuration of an asset. | **[Insert Target Remediation Time]** |

# Responsibilities

**[List Who Is Responsible For Sponsoring, Setting Up And Maintaining The Program.]**

**Responsibilities For Senior Management**

* Establish a vulnerability and patch management program within the Office of the Chief Information Officer (OCIO) and ensure executive sponsorship and governance.
* Define policy, process, and procedures for vulnerability and patch management to include automated, repeatable processes to adequately protect IT information assets
* Ensure the maintenance of a continual **[Business Name]** wide IT assets.