|  |  |
| --- | --- |
| [Organization Name] | **No:**  [Policy Number] |
| **IT Standard**:  **Patch Management** | **Updated:** 10/29/2024 |
| **Issued By:**  [Policy Authority]  **Owner:**  [Policy Owner] |

# 1.0 Purpose and Benefits

The purpose of the Patch Management Standard is to establish a proactive approach for managing security patches to prevent exploitation of vulnerabilities in the organization’s IT systems. By systematically applying software and firmware updates, the standard aims to minimize potential security breaches, thereby reducing both time and costs associated with managing these vulnerabilities.

Implementing this standard enhances the organization’s cybersecurity by ensuring timely updates and effective management of IT vulnerabilities. This proactive stance not only safeguards sensitive information but also improves operational efficiency by reducing the risk of exploit-related disruptions. Ultimately, adherence to this standard fosters a more secure IT environment, protecting organizational assets and maintaining trust with stakeholders.

# 2.0 Authority

This policy is established under the authority of organizational management and is guided by best practices outlined in the National Institute of Standards and Technology (NIST) Cybersecurity Framework 2.0. While not mandated by law, the organization adopts this framework to enhance its cybersecurity posture and protect its information assets. The authority for enforcement and adherence to this policy is vested in the [Policy Authority], who is responsible for ensuring compliance across all departments.

# 3.0 Scope

This policy applies to all employees, contractors, third-party vendors, and any individuals or entities accessing, using, or managing the organization's information systems, networks, and physical infrastructure, regardless of the medium or format of the information. It covers all electronic, paper-based, and verbal communication, including, but not limited to, data processing systems, cloud services, email platforms, mobile devices, databases, and other digital storage mechanisms that store, transmit, or process sensitive organizational information.

The policy encompasses internal and external users, whether they access the organization's systems on-site or remotely, and includes all physical infrastructure such as data centers, workstations, and hardware that interact with or support the organization's information environment. Additionally, it extends to any devices, both personal and organizational, that connect to the corporate network or handle company data.

All users are responsible for protecting the confidentiality, integrity, and availability of information, complying with this policy and relevant laws, and familiarizing themselves with the organization's security policies and procedures to ensure the protection of organizational assets. Failure to comply with these requirements may result in disciplinary action, including termination of access rights or contractual agreements.

# 4.0 Information Statement

The Patch Management Standard applies to all employees, contractors, and third-party vendors involved in managing the organization’s information systems and infrastructure. It requires the assignment of responsible personnel for patch management, whether internally or through outsourced agreements, and mandates a comprehensive process for monitoring vulnerabilities, distributing patches, and verifying installations.

All installed IT assets must be included in the patch management inventory, with prioritization based on vulnerability severity according to the Common Vulnerability Scoring System (CVSS). Timely application of patches is critical, with specific timelines established for high, medium, and low severity vulnerabilities. Compliance with this standard is essential to ensure the integrity and security of organizational information, and failure to adhere may lead to disciplinary actions.

* 1. Responsibility

The [Owner] shall:

1. Assign an individual or group within operations to be responsible for patch management.
2. If patch management is outsourced, service level agreements must be in place that address the requirements of this standard and outline responsibilities for patching. If patching is the responsibility of the third party, entities must verify that the patches have been applied.
   1. Process
3. A process must be in place to manage patches. This process must include the following:
   1. Monitoring security sources ([Appendix A](#AppendixA)) for vulnerabilities, patch and non-patch remediation, and emerging threats;
   2. Overseeing patch distribution, including verifying that a change control procedure is being followed;
   3. Testing for stability and deploying patches; and
   4. Using an automated centralized patch management distribution tool, whenever technically feasible, which:
      1. Maintains a database of patches;
      2. Deploys patches to endpoints; and
      3. Verifies installation of patches.
4. Appropriate separation of duties must exist so that the individual(s) verifying patch distribution is not the same individual(s) who is distributing the patches.
   1. Scope

As per the Information Security Policy, all entities must maintain an inventory of hardware and software assets. Patch management must incorporate all installed IT assets.

* 1. Prioritization and Timeline

1. Patch management must be prioritized based on the severity of the vulnerability the patch addresses. In most cases, severity ratings are based on the Common Vulnerability Scoring System (CVSS). A CVSS score of 7-10 is considered a high impact vulnerability, a CVSS score of 4-6.9 is considered a moderate impact vulnerability and a CVSS of 0-3.9 is considered a low impact vulnerability.
2. To the extent possible, the patching process must follow the timeline contained in the table below:

|  |  |  |
| --- | --- | --- |
| **Impact/Severity** | **Patch Initiated** | **Patch Completed** |
| High | Within **24 hours** of patch release | Within **1 week** of patch release |
| Medium | Within **1 week** of patch release | Within **1 month** of patch release |
| Low | Within **1 month** of patch release | Within **2 months** of patch release, unless ISO determines this to be an insignificant risk to the environment |

1. If patching cannot be completed in the timeframe listed in the table above, compensating controls must be put in place within the timeframes above and the exception process must be followed.
2. If a patch requires a reboot for installation, the reboot must occur within the timeframes outlined above.

# 5.0 Compliance

This policy shall take effect upon publication. Compliance is expected with all enterprise policies and standards. Policies and standards may be amended at any time; compliance with amended policies and standards is expected.

If compliance with this standard is not feasible or technically possible, or if deviation from this policy is necessary to support a business function, entities shall request an exception through the following process.

# 6.0 Policy Exceptions

Requests for exceptions to this policy must be submitted to the [Authority] by the requesting department. Each request should include the scope and justification for the exception, potential risks, proposed mitigation measures, and a timeframe for achieving compliance. The [Authority] will review and discuss these requests with the department.

# 7.0 Definitions of Key Terms

|  |  |
| --- | --- |
| **Term** | **Definition** |
| Information Systems | Any combination of hardware, software, data, and personnel that processes, stores, or transmits information, including but not limited to computers, servers, networks, and applications. |
| Users | Individuals or entities, including employees, contractors, and third-party vendors, who access or interact with the organization’s information systems and data. |
|  |  |

# 8.0 Contact Information

Submit all inquiries and requests for future enhancements to the policy owner at:

[Policy Owner’s Contact Info]

[Organization Address]

# 9.0 Review and Revision

This policy should be reviewed at least annually to keep pace with evolving regulations, threat landscapes, and organizational changes. However, more frequent reviews may be necessary following regulatory updates, cybersecurity incidents, significant technology changes, organizational shifts, or compliance audits. This policy should be revised based on these reviews and those revisions noted below.

|  |  |  |
| --- | --- | --- |
| **Date** | **Description of Change** | **Reviewer** |
|  |  |  |

# 10.0 Related Documents

[National Institute of Standards and Technology, Special Publication 800-40 - Guide to Enterprise Patch Management Planning: Preventive Maintenance for Technology](https://csrc.nist.gov/pubs/sp/800/40/r4/final)