



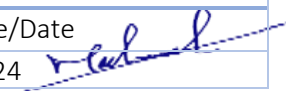
Patch Management Policy

Doc. Control Number	Version
SNL-16	0.3



Document Reference

Item	Description
Title	Patch Management Policy
Department	Cybersecurity department
Version No	0.3
Status	Draft
Type	DOCX
Publish-Date	13 March 2024
Revision-Date	13 March 2025

Authors		
Name	Department	Signature/Date
Muhaned Kamal Ali	Cybersecurity - I. S Specialist	13/3/2024 

Reviewed by		
Name	Department	Signature/Date
Yasir Awad	Head of Cyber Security Department	13/3/2024 

Approved by		
Name	Department	Signature/Date
Abdullah Al Shuhail	V.P	13/3/2024 

Control-Page

Document Amendment Record			
Version-No	Date	Prepared-by	Explanation
0.1	22 June 2022	Muhaned Ali	First Release
0.2	23 May 2023	Muhaned Ali	The Policy has been reviewed
0.3	13 March 2024	Muhaned Ali	The Policy has been reviewed



Contents

1. Purpose	4
2. Scope	4
3. Policy	4
4. Roles and Responsibilities	5
5. Policy Compliance	6

1. Purpose

The purpose of this policy is to define cybersecurity requirements based on best practices and standards related to the management of update and fix packages for systems, applications, databases, network devices, and information processing devices for SNLC to reduce cyber risks and protect them from internal and external threats by focusing on the basic objectives of protection, namely: Confidentiality, integrity, and availability of information.

2. Scope

This policy covers all systems, applications, databases, network devices, information processing devices, industrial control devices, and systems for SNLC, and applies to all employees of SNLC.

3. Policy

3.1 Tools and Techniques

- a) Automated patch management tools shall be utilized to streamline the patch deployment process and ensure timely application of patches across all relevant systems.
- b) SNLC utilizes ManageEngine for patch deployment management.

3.2 Patch Management Triggers

- a) Patch management triggers shall include:
 - Release of security patches by software vendors.
 - Identification of vulnerabilities through vulnerability scanning, penetration testing, or security incident response.
 - Changes in the organization's infrastructure, such as software upgrades or system migrations.
 - Compliance requirements and industry best practices mandating the application of specific patches.

3.3 Patch Testing Environment

- a) A dedicated patch testing environment shall be established to evaluate the compatibility, stability, and security impact of patches before deployment to production systems.
- b) The patch testing environment shall replicate the production environment as closely as possible to ensure accurate assessment of patch performance under real-world conditions.
- c) Testing procedures shall include functional testing, regression testing, and security testing to verify that patches do not introduce new vulnerabilities or unintended consequences.

3.4 Frequency

- a) Patching shall be performed on a regular basis to maintain the security and integrity of the organization's systems and applications.
- b) The frequency of patching shall be determined based on the criticality of systems, severity of vulnerabilities, and risk tolerance of the company.
- c) General requirements for patching frequency shall include:
 - Critical systems: Patches addressing critical vulnerabilities shall be deployed as soon as feasible following their release, with priority given to high-severity vulnerabilities.
 - Non-critical systems: Regular patching shall occur on a scheduled basis, with a minimum frequency of monthly updates.
 - Emergency patches: Critical security patches addressing zero-day vulnerabilities or actively exploited vulnerabilities shall be deployed immediately upon release, bypassing regular patching schedules.

3.5 Patch Management packages must be managed in a way that ensures the protection of systems, applications, databases, network devices, and information processing devices.

- 3.6 If the OS is Windows, the patch management tools should be set in a way that automatically downloads the latest Microsoft security patches. The patches will be reviewed and applied as appropriate.
- 3.7 Periodical reviews on the supplier’s website who provides servers, PC’s, switches, routers, FWs, and other peripherals check firmware patches.
- 3.8 It is the user’s responsibility to check all the patches update periodically as trained and take ownership of all automatic updates starting from operating systems, software, antivirus, workstations, patches, drivers of devices.
- 3.9 Department of Information Technology must test update and patch packages in the test environment before installing them on systems, applications, and information processing devices in the Production Environment, to ensure that the update and patch packages are compatible with the systems and applications.
- 3.10 A rollback plan must be developed and implemented if the update and repair packages negatively affect the performance of systems, applications, or services.
- 3.11 Updates and fixes should be installed at least once a month for sensitive systems connected to the Internet, and once every three months for internal sensitive systems.
- 3.12 Updates and fixes for technical assets should be installed as follows:

Frequency duration for installing updates		
Asset Type	Information and technical assets	Information and technical assets for sensitive systems
Operating systems	Per month	Per month
Databases	Three months	Per month
Network devices	Three months	Per month
Application	Three months	Per month

- 3.13 The process of managing updates and fixes should follow the requirements of the change management process.
- 3.14 Updates and fixes must be downloaded to a centralized server (Centralized Patch Management Server) before they are installed on systems, applications, databases, network devices, and information processing devices, except for update and fix packages for which there are no supported automated tools.
- 3.15 After installing update and patch packages, independent and reliable tools should be used to ensure that vulnerabilities are effectively addressed.
- 3.16 The Key Performance Indicator “KPI” should be used to ensure the continuous development of the management of update packages and fixes.
- 3.17 The policy and procedures for managing updates and fixes packages should be reviewed annually, and changes should be documented and approved.

4. Roles and Responsibilities

- 4.1 The sponsor and owner of the policy document: Head of Cyber Security Department.
- 4.2 Policy reviews and update: Cyber Security Department.

4.3 Policy implementation: IT Department

5. Policy Compliance

5.1 Compliance Measurement

The Infosec team will verify compliance with this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

5.2 Exceptions

Any exception to the policy must be approved by the Infosec team in advance.

5.3 Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.