




Patch Management process


Doc. Control Number	Version
SNL-44	0.2



Document Reference

Item	Description
Title	Patch Management process
Department	Cybersecurity department
Version No	0.2
Status	Draft
Type	DOCX
Publish-Date	28 May 2024
Revision-Date	28 May 2025

Authors		
Name	Department	Signature/Date
Muhaned Kamal Ali	Cybersecurity - I. S Specialist	5/28/2024 

Reviewed by		
Name	Department	Signature/Date
Yasir Awad	Head of Cyber Security Department	5/28/2024 

Approved by		
Name	Department	Signature/Date
Abdullah Al Shuhail	V.P	5/28/2024 

Control-Page

Document Amendment Record			
Version-No	Date	Prepared-by	Explanation
0.1	28 May 2023	Muhaned Ali	First Release
0.2	28 May 2024	Muhaned Ali	The document has been reviewed



Contents

1. Purpose.....	4
2. Scope	4
3. Patch Management process	4
3.1 Desktops, Laptops, and Servers	4
3.2 Network Hardware/Devices (FW, Routers, Switches, etc.)	4
3.3 Exceptions.....	4
3.4 Patch-Compliance Review Procedure.....	5

1. Purpose

This document provides the processes and guidelines necessary to maintain the integrity of network systems and SNLC data by applying the latest operating system and application security updates/patches in a timely manner, and to establish a baseline methodology and time frame for patching and confirming patch-management compliance.

2. Scope

The processes addressed in this document affect all managed SNLC systems, including desktops, laptops, servers, network devices.

3. Patch Management process

3.1 Desktops, Laptops, and Servers

1. Download patches from a reliable source; in SNLC, we use desktop central from ManageEngine.
2. Test patches to identify adverse effects.
3. Input a Change Management Request case and discuss at the weekly change management meetings. Follow the Emergency CMR process for critical security patches that require immediate attention.
4. Communicate with stakeholders.
5. Deploy patches:
 - Windows Workstations:
 - o Monthly patches: Deploy no later than during the second weekly maintenance window of each month.
 - o Out-of-band security patches: Deploy as soon as possible; no later than one week following release.
 - UNIX/Linux Workstations:
 - o Deploy as soon as possible; at least once per month.
 - Windows Servers:
 - o Monthly patches: Deploy no later than during the third weekly maintenance window of each month.
 - o Out-of-band security patches: Deploy as soon as possible; no later than one week following release.
 - UNIX/Linux Servers:
 - o At least once per month.
 - o Critical security patches that resolve a known vulnerability: Deploy as soon as possible following release and no later than one week following release.

3.2 Network Hardware/Devices (FW, Routers, Switches, etc.)

1. Download patches as available. Patch notifications originate from vendors (Cisco, Fortinet, Aruba, Unifi, etc.)
2. Test (where a test environment is available).
3. Adhere to the SNLC Change Management Review (CMR) process for release to production.
4. Creating necessary backups based on risk assessment.
5. Implement
6. Review device configurations to identify known and potential vulnerabilities. Retain documented evidence of the review for a period of at least one year.

3.3 Exceptions

1. Systems or applications that cannot be patched to resolve a known vulnerability will have the justification documented by the device/application owner and the necessary compensating control(s) implemented.
 - Justification

- No vendor patch available.
- Patch provided by vendor creates instability within the system; instability outweighs the risk.
- Compensating Controls
 - Network segmentation
 - Access Control Lists
 - Intrusion Prevention Systems
- 2. Systems that transmit or store protected data and cannot be patched to resolve a known vulnerability will be brought to the attention of the data owner and to the SNLC information security manager, and the necessary compensating control(s) will be implemented.

3.4 Patch-Compliance Review Procedure

1. Desktop and server administrators will generate and review patch management/compliance reports at least monthly from the SNLC patch servers.
2. In reviewing the patch reports, desktop and server administrators will identify un-patched machines that connect to the SNLC network and either patch or define an exception.
3. The Information Security department will conduct vulnerability scans of known critical systems at least annually. Critical systems with un-patched vulnerabilities will be brought to the attention of the system/application administrator(s) for mitigation.