

4.4.1 Patch Management Policy

Contents

1. Definitions	2
2. Purpose	2
3. Scope	2
4. Policy	2
5. Non-compliance	4
6. References	4

Version	Adjustment Date	Approved By	Approval Date
2.1	18/12/2025	Saud Alsulami	2/1/2025



1. Definitions

For purposes of this "Patch Management Policy" the following definitions apply:

- **IT Asset:** is any valuable component within the information technology infrastructure of an organization. This can include hardware devices, software applications, data, networks, and other elements that contribute to the management, processing, and storage of information.
- **Asset Inventory:** a comprehensive and up-to-date listing of all organizational assets, including IT assets. It involves the systematic documentation of hardware, software, data, personnel, and other resources, along with relevant details such as ownership, classification, and location.
- **Risk assessment:** the process of identifying, analyzing, and evaluating potential risks and vulnerabilities in a system, organization, or process.

2. Purpose

This Patch Management Policy outlines the requirements and procedures for managing software and system patches in Taqnyat Al-Jawal. It aims to protect our information technology assets by ensuring the timely and effective application of security patches.

3. Scope

The scope of patch management covers all information assets within the Taqnyat, including but not limited to systems, applications, and network devices.

4. Policy

- 4.1. The IT asset inventory must be maintained and update as per Asset Management policies for all software, systems, and devices requiring patch management.
- 4.2. The classification of the patch is determined based on the classification of the asset, taking into consideration the patch's classification grade as determined by the manufacturer.
- 4.3. Patch deployment must be prioritized based on the risk assessment derived from these sources.
- 4.4. Utilize standard patch management tools must be used to automate and streamline patch deployment.



- 4.5. These patch management tools receive updates from the parent companies, then it sends notification to the IT operations team.
- 4.6. The cybersecurity officer and the IT operation team must monitor vendors notifications, security bulletins, and threat intelligence feeds to identify new patches and vulnerabilities.
- 4.7. The patch is tested on a testing environment if available for assets with low and medium classifications. If not available, the patch is applied directly to the production environment, ensuring it does not cause any harm to the Taqnyat's external services.
- 4.8. All patches for the assets with high classification must be tested in the test server or environment to evaluate patches before deploying them in the production environment.
- 4.9. Perform compatibility and functionality testing to ensure that patches do not adversely affect system operations.
- 4.10. Implement a regular patching schedule that includes the application of security patches at least monthly according to the following:
 - High-classification asset patches are applied after testing them on the staging environment to ensure no issues arise from their application. They are then applied to the production environment after approval from both the programming and NOC departments.
 - Low and medium classification asset patches are applied on the testing environment if available. They are then applied to the production environment directly by the cybersecurity officer.
 - If the update for high-classification assets involves directly upgrading an application related to services, such as upgrading the database application version to a newer one, it must be done according to the approved change management policy.
- 4.11. Critical patches should be deployed as soon as possible, and non-critical patches should follow a defined schedule on patch management process.
- 4.12. Installed patches must be successful and must not disrupt the normal operation of systems and software.
- 4.13. The effectiveness of the patches applied in remediating detected vulnerabilities must be verified.

5. Non-compliance

All personnel must adhere to this Patch Management Policy.

Non-compliance with this policy may result in disciplinary action, up to and including termination of employment, and related civil or criminal penalties.

6. References

- SANS
- National Cybersecurity Authority's (NCA) ECC standards

