This is a guidance box. Remove all guidance boxes after filling out the template. Items highlighted in turquoise should be edited appropriately. Items highlighted in green are examples and should be removed. After all edits have been made, all highlights should be cleared.

Insert organization logo by clicking on the placeholder to the left.

# Patch Management Standard Template

Choose Classification

| | |
|---|---|
| DATE | Click here to add date |
| VERSION | Click here to add text |
| REF | Click here to add text |

Replace <organization name> with the name of the organization for the entire document. To do so, perform the following:

- Press “Ctrl” + “H” keys simultaneously.
- Enter “<organization name>” in the Find text box.
- Enter your organization’s full name in the “Replace” text box.
- Click “More”, and make sure “Match case” is ticked.
- Click “Replace All”.
- Close the dialog box.

# Disclaimer

This template has been developed by the National Cybersecurity Authority (NCA) as an illustrative example that can be used by organizations as a reference and guide. This template must be customized and aligned with the <organization name>'s business and relevant legislative and regulatory requirements. This template must be approved by the head of the organization (Authorizing official) or his/her delegate. The NCA is not responsible for any use of this template as is, and it affirms that this template is solely an illustrative example.

# Document Approval

| Role | Job Title | Name | Date | Signature |
|---|---|---|---|---|
| Choose Role | <Insert job title> | <Insert individual's full personnel name> | Click here to add date | <Insert signature> |
| | | | | |

# Version Control

| Version | Date | Updated By | Version Details |
|---|---|---|---|
| <Insert version number> | Click here to add date | <Insert individual's full personnel name> | <Insert description of the version> |
| | | | |

# Review Table

| Periodical Review Rate | Last Review Date | Upcoming Review Date |
|---|---|---|
| <Once a year> | Click here to add date | Click here to add date |
| | | |

# Table of Contents

# Purpose

This standard aims to define the cybersecurity requirements related to the patch management for <organization name>'s technology solutions and assets. The ability of <organization name> to manage patches in accordance with this standard will assist in reducing the cybersecurity risks, in ensuring protection from related internal and external threats, and in preservation of the availability, integrity and confidentiality of <organization name>'s assets and information.

The requirements in this standard are aligned with the cybersecurity requirements issued by the National Cybersecurity Authority (NCA), including but not limited to ECC-1:2018, DCC-1:2022, CSCC-1:2019 and CCC-1:2020, in addition to other related cybersecurity legal and regulatory requirements.

# Scope

This standard covers all <organization name>'s information and technology assets and applies to all personnel (employees and contractors) in <organization name>.

# Standards

| 1 | Plan risk response |
|---|---|
| Objective | The objective of this section is to ensure that the organization is managing the patching in accordance with the assessment of the incoming cybersecurity risks and vulnerabilities. |
| Risk Implication | Without patching is being done in consequence of the <organization name>'s overall risk and vulnerability management processes (e.g., only being done as an operational duty), the chance of letting potential vulnerabilities unthreated is higher. |
| Requirements | |

| | |
|---|---|
| 1-1 | <organization name> must consider every new software vulnerability affecting <organization name>'s assets, including applications, operating systems, and firmware. |
| 1-2 | <organization name> must avoid the cybersecurity risk of unavailable or not introduced patches, ensuring that the likelihood of risk is reduced by eliminating the attack surface:<br>● uninstalling the vulnerable software;<br>● disconnecting vulnerable asset from network;<br>● decommissioning devices with the vulnerabilities;<br>● disabling computing capabilities in devices that can function without them. |
| 1-3 | <organization name> must mitigate cybersecurity risks by performing patches to eliminate the vulnerabilities, e.g.:<br>● patching the vulnerable software;<br>● disabling a vulnerable feature; or<br>● upgrading to a newer software version without the vulnerabilities. |
| 1-4 | <organization name> must deploy additional security controls to reduce vulnerability exploitation, e.g.:<br>● using firewalls and network segmentation to isolate vulnerable devices, thus reducing the attack surface. |
| 1-5 | <organization name> must define at least the following software vulnerability risk response scenarios they need to be prepared to handle:<br>● Routine patching (standard procedure for patches that are on a regular release cycle)<br>● Emergency patching (to address patching emergencies in a crisis situation) |

| | |
|---|---|
| | • Emergency workaround (to temporarily mitigate vulnerabilities before a patch is available)<br>• Unpatchable assets (isolation or other methods to mitigate the risk of systems that cannot be easily patched) |
| 1-6 | <organization name> must define maintenance groups and develop maintenance plan for each maintenance group for each applicable risk response scenario, e.g.:<br>• <Maintenance Plans for Scenario 1, Routine Patching><br>  ○ <organization name> must adopt phased deployments for routine patching in which a small subset of the assets to be patched receive the patch first.<br>• <Maintenance Plans for Scenario 2, Emergency Patching><br>  ○ <organization name> must use the same general approach for emergency patching as for routine patching, except with a highly accelerated schedule.<br>• <Maintenance Plans for Scenario 3, Emergency Workarounds><br>  ○ <organization name> must plan for the quick implementation of multiple types of emergency workarounds to protect vulnerable assets.<br>• <Maintenance Plans for Scenario 4, Un-patchable Assets><br>  ○ <organization name> must plan to implement multiple types of long-term risk mitigation methods besides patching to protect vulnerable assets. |

| 2 | Execute risk response |
|---|---|
| Objective | The objective of this section is to ensure that patching is being done by following logically structured risk response execution. |
| Risk Implication | Without a well-designed and structured risk response execution, the assessment of risks can fail on several occasions, leaving vulnerabilities unpatched, or untreated. |
| Requirements | |
| 2-1 | The execution of risk response must be composed of the following steps:<br>● Prepare risk response<br>● Implement risk response<br>● Verify risk response<br>● Continuously monitor risk response |
| 2-2 | Preparing risk response must cover the following activities:<br>● Acquiring patches<br>● Validating patches<br>● Testing patches |
| 2-3 | Implementing risk response must cover the following activities:<br>● Applying change management processes<br>● Determine method of installing<br>● Prioritize and schedule installing patches |
| 2-4 | Verifying risk response must cover the following activities:<br>● Confirmation of installed patch<br>● Checking the effectiveness of patching<br>○ Vulnerability scan |

| | |
|---|---|
| | ○ Using metrics (KPI) |
| 2-5 | Continuous monitoring of risk response must cover the following activities:<br>● Making sure no one uninstalls patches<br>● Making sure, that an older version of the patched software has not been restored<br>● Periodic vulnerability assessment for installed patches |
| 3 | Prepare risk response |
| Objective | The objective of this section is acquiring, validating, and testing patches for the vulnerable software or deploying additional security controls to safeguard the vulnerable software. |
| Risk Implication | Validation: The patch could have been acquired from a rogue source or tampered with in transit or after acquisition.<br>Testing: Operational risk by identifying problems with a patch before placing it into production. |
| Requirements | |
| 3-1 | Patches must be acquired only from legitimate sources. This includes acquiring it though secure sites provided by the vendor/manufacturer or developing it internally. |
| 3-2 | Available patches must be monitored by the asset owner and be installed if it is technically feasible, in accordance with the patched asset's criticality level, and after the patch has been tested. |
| 3-3 | File integrity must be confirmed before the patch is being tested or installed, using hashing algorithms if it is technically feasible (e.g., network device firmware). |

| | |
|---|---|
| 3-4 | Virus scan must always be performed on the downloaded patches, to avoid the possibility of a malware being installed. |
| 3-5 | Patches must be tested prior deployment or live implementation. |
| 3-6 | In case of software patches, a separate test environment must be used in order to avoid virus infection and software compatibility issues. |
| 3-7 | Upcoming issues must be documented and resolved in the testing phase before live implementation of the patches. |
| 3-8 | Processes with an option of rollback must be implemented in case there is an unforeseen incompatibility, so systems can be restored to their pre-patched state. |
| 3-9 | Backup and restore functions must be implemented in case there is an unforeseen incompatibility, so system availability can be ensured in such cases. |
| 4 | Implement risk response |
| Objective | The objective of this section is to ensure the safety and continuity of the information system through distributing and installing patches and changing asset configurations and state. |
| Risk Implication | Change management: Applying patches without the proper change management process can lead to the halt of business processes, or even data loss.<br><br>Prioritize and schedule: Without the prioritization of patches there is a chance that some of the critical or high severity patches are not being installed on an important asset. |
| Requirements | |

| | |
|---|---|
| 4-1 | Patch deployments must be scheduled as part of the <organization name>'s change management activity. |
| 4-2 | <organization name> must implement only those changes in the <organization name>'s live environment that has been approved through the <organization name>'s change management procedure. |
| 4-3 | The application procedure of a patch being installed must be documented in order to be traceable (e.g., approvement and testing is already done) |
| 4-4 | The following installation methods must be used to install patches:<br>● Distributing patches through a centralized solution<br>○ Using automatic installation<br>○ Scheduling the installation of patches<br>○ Installing it manually (forced installation)<br>● Installing patches as a single installation |
| 4-5 | Patches must be prioritized in order to install higher priority patches first, in accordance with the results of <organization name>'s risk assessment. |
| 4-6 | Patch prioritization must be based on asset criticality, in accordance with the vulnerability management policy and standard.<br><organization name> must introduce a Vulnerability Mitigation Time Summary Matrix (Table 1 appendix) and provide mitigation metrics based on<br>● relative importance of the assets (low, moderate, or high) according to the classification of <organization name> and the legislative and regulatory requirements issued; |

| | |
|---|---|
| | • vulnerabilities (low, medium, high, or critical), according to the classification of <organization name> and the legislative and regulatory requirements issued. |
| 5 | Verify and monitor risk response |
| Objective | The objective of this section is to ensure that the implementation has been completed successfully. For patching, this means confirming that the patch is installed and has taken effect. For deploying additional security controls, ensure they are functioning as intended. |
| Risk Implication | In case the installation of patches is not monitored or confirmed, there is a risk that an information asset will be still vulnerable and open for attack. |
| Requirements | |
| 5-1 | The effectiveness of the patching must be checked in order to verify its success. The following techniques must be used for verification:<br>• Performing vulnerability scan on the patched asset<br>• Using metrics (Key Performance Indicators) provided by the information systems being used to install patches (WSUS, HPSA, SCCM) |
| 5-2 | The risk response must be continuously monitored, taking into consideration the following:<br>• Patches must be installed only by appropriate personnel (IT operations). Any other means of installing patches must be disabled by the system administrator.<br>• <organization name> must ensure no one uninstalls the patch, deactivates the additional security controls, lets the cybersecurity insurance lapse, or restarts the decommissioned device. |

| 6 | Other Standards |
|---|---|
| Objective | Patch Management must be securely deployed and used appropriately when required. |
| Risk Implication | If <organization name> is not compliant with all of standards and requirements, it could be exposed to severe threat rise. |
| Requirements | |
| 6-1 | The following standards must be implemented in relevance to Patch management:<br>1- Vulnerability Management Policy<br>2- Vulnerability Management Standard<br>3- Cybersecurity Risk Management Policy |

# Table 1 – Vulnerability Mitigation Time Summary Matrix <with data example>

| Vulnerability importance | Asset importance | | |
|---|---|---|---|
| | Low | Moderate | High |
| Low | By deadline: 64.7 %<br>Average time: 80.4 days<br>Median time: 75.2 days | By deadline: 72.4 %<br>Average time: 34.7 days<br>Median time: 33.7 days | By deadline: 85.0 %<br>Average time: 14.6 days<br>Median time: 8.1 days |
| Medium | By deadline: 66.5 %<br>Average time: 75.1 days<br>Median time: 70.7 days | By deadline: 68.7 %<br>Average time: 33.2 days<br>Median time: 31.6 days | By deadline: 71.4 %<br>Average time: 12.9 days<br>Median time: 10.5 days |
| High | By deadline: 68.6 %<br>Average time: 62.1 days<br>Median time: 58.0 days | By deadline: 78.8 %<br>Average time: 26.8 days<br>Median time: 22.1 days | By deadline: 85.5 %<br>Average time: 8.8 days<br>Median time: 8.1 days |
| Critical | By deadline: 81.4 %<br>Average time: 44.4 days<br>Median time: 41.3 days | By deadline: 92.3 %<br>Average time: 21.2 days<br>Median time: 23.9 days | By deadline: 95.2 %<br>Average time: 5.2 days<br>Median time: 5.1 days |

The metrics in each cell reflect the percentage of assets that were patched by the corresponding maintenance plans' deadlines, as well as the average (mean) time and median time for patching.

# Roles and Responsibilities

1- **Standard Owner:** <head of the cybersecurity function>
2- **Standard Review and Update:** <cybersecurity function>
3- **Standard Implementation and Execution:** <information technology function>
4- **Standard Compliance Measurement:** <cybersecurity function>

# Update and Review

<cybersecurity function> must review the standard at least once a year or in case any changes happen to the policy or the regulatory procedures in <organization name> or the relevant regulatory requirements.

# Compliance

1- The <head of the cybersecurity function> will ensure compliance of <organization name> with this standard on a regular basis.
2- All personnel at <organization name> must comply with this standard.
3- Any violation of this standard may be subject to disciplinary action according to <organization name>'s procedures.