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 Policy Template

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.

Choose Classification

DATE: Click here to add date
VERSION: Click here to add text
REF: Click here to add text

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 policy aims to define the cybersecurity requirements related to Patch Management of <organization name>'s systems, applications, databases, network devices, and information processing facilities to minimize cybersecurity risks resulting from internal and external threats at <organization name>. The requirements in this policy are aligned with the cybersecurity requirements issued by the National Cybersecurity Authority (NCA) including but not limited to ECC-1:2018 and CSCC-1:2019, in addition to other related cybersecurity legal and regulatory requirements.

Scope

This policy covers all technology assets of <organization name>, including all technology components of CTS, Critical Systems, OT, Telework Systems as well as technology assets of Social Media accounts and applies to the <cybersecurity function> and <information technology function> at <organization name>.

Policy Statements

1 General Requirements

1-1 Patch Management must ensure the protection of <organization name> systems, applications, databases, network devices, and information processing facilities, including all technology components of CTS, Critical Systems, OT, Telework Systems as well as technology assets of Social Media accounts.

1-2 Patches must be downloaded from an authorized and trusted sources according to <organization name>'s applicable procedures.

1-3 Secure and reliable methods and tools must be used for periodic scans to detect vulnerabilities and install patches and follow up their implementation.

1-4 Patches must be tested in the test environment before installation to systems, applications, and information processing facilities in

production environment to ensure their compatibility with systems and applications.

1-5 Rollback Plan must be set and implemented in case the patches adversely affected performance of systems, applications or services.

1-6 Patches that remediate security vulnerabilities must be prioritized taking into consideration the associated risk level.

1-7 Patches must be scheduled in alignment with vendor release cycles.

1-8 Patches should be installed on technology assets at least as follows:

Asset Type	Systems					
	All systems	Critical systems connected to the internet	Internal critical systems	Telework systems	Social media accounts systems	Cloud Computing Service Systems
	Frequency of patches application					
Operating Systems	Monthly	Monthly	Monthly	Monthly	Monthly	Monthly
Databases	3 months	Monthly	3 months	Monthly	Monthly	3 months
Network Devices	3 months	Monthly	3 months	Monthly	Monthly	3 months
Applications	3 months	Monthly	3 months	Monthly	Monthly	3 months

1-9 Users must be prevented from negatively affecting or disrupting patch technologies.

1-10 The patch management process must follow the approved requirements of change management process at <organization name>.

1-11 Emergency change management process must be developed and approved, and emergency patches must be implemented

according to the emergency change management process in case of high-risk security vulnerabilities.

1-12 Patches must be downloaded to a Centralized Patch Management Server before installation to systems, applications, databases, network devices, and information processing facilities, except when automated patching tools are not supported.

1-13 After patches are installed, independent and trusted tools must be used to ensure that vulnerabilities are effectively fixed.

1-14 Patch management procedures and standards must be developed based on business need.

1-15 KPI must be used to ensure continuous improvement for Patch Management requirements.

Roles and Responsibilities

1- **Policy Owner:** <head of the cybersecurity function>

2- **Policy Review and Update:** <cybersecurity function>

3- **Policy Implementation and Execution:** <information technology function>

4- **Policy Compliance Measurement:** <cybersecurity function>

Update and Review

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

Compliance

1- <head of cybersecurity function> will ensure the compliance of <organization name> with this policy on a regular basis.

2- The <cybersecurity function> and the <information technology function> of <organization name> must comply with this policy.

3- Any violation of this policy may be subject to disciplinary action according to <organization name>'s procedures.