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 outlined image.

Configuration and Hardening Policy 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 policy aims to define the cybersecurity requirements related to the protection, hardening, and configuration of <organization name>'s information and technology assets to achieve the main objective of this policy which is minimizing cybersecurity risks resulting from internal and external threats at <organization name> in order to preserve confidentiality, integrity and availability.

The requirements in this policy are aligned with the cybersecurity requirements issued by the National Cybersecurity Authority (NCA) in addition to other related cybersecurity legal and regulatory requirements.

Scope

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

Policy Statements

1 General Requirements

1-1 All information and technology assets and all approved applications and software used in <organization name> must be defined and documented.

1-2 <organization name>'s workstations, systems, applications, network devices, servers, and security devices must be configured and hardened according to the technical security standards approved by the vendors, and as per the relevant legal and regulatory requirements and international best practices to prevent cyberattacks.

1-3 Print screen or screen capture features must be disabled for devices that create or process information based on the information classification.

1-4 Key Performance Indicators (KPIs) must be used to ensure the continuous improvement and effective and efficient use of configuration and hardening security protection requirements.

2 Technical Security Standard Development

2-1 The vendors' security configuration guidance must be used according to <organization name>'s regulatory procedures and policies, the relevant legal and regulatory requirements, and international best practices.

2-2 Security configuration guidance must be used from trusted sources that are aligned with factory standards such as the Center for Internet Security (CIS), the SysAdmin, Audit, Network, Security (SANS) Institute, and the National Institute of Standards and Technology (NIST).

2-3 <organization name>'s technical security standards must be developed in line with the nature of business, the vendors' security configuration guidance, factory standards, and the relevant legal and regulatory requirements.

2-4 Technical security standards for all <organization name>'s authorized information and technology assets, applications, and programs must be developed, documented, approved, and reviewed in line with international practices, <organization name>'s approved regulatory procedures and policies, and the relevant legal and regulatory requirements.

3 Configuration and Hardening Review and Implementation:

3-1 Configuration and hardening of all information and technology assets and applications must be reviewed at least once a year or in case any changes happen, and their implementation must be ensured according to cybersecurity guidelines, best practices, and vendors' recommendations, and in line with <organization name>'s change management mechanisms.

3-2 Configuration and hardening must be reviewed before launching applications, technology projects, and changes related to information and technology assets.

3-3 Default configurations of all information and technology assets for remote work systems must be reviewed, and to ensure that fixed passwords and default backgrounds do not exist.

3-4 Enabling remote work features and services must be restricted on an as-needed basis, and potential cybersecurity risks must be assessed in case of a need to enable them, in line with the relevant legal and regulatory requirements.

3-5 An image of the <organization name>'s configuration and hardening for information and technology assets must be approved and stored in a secure place as per the approved technical security standards.

3-6 An approved image must be used to install or update information and technology assets.

3-7 The necessary technologies must be provided to centrally manage configuration and hardening and ensure automatic implementation or/and update of configuration and hardening for all information and technology assets at pre-determined times, after conducting the required testing.

3-8 A Security Content Automation Protocol (SCAP) compliant configuration monitoring system must be implemented to verify that the configurations are in line with the approved technical security standards and are fully implemented. Any unauthorized changes must be reported.

3-9 Clock synchronization must be implemented centrally from an accurate and reliable source (such as relevant sources provided by Saudi Standards, Metrology and Quality Organization (SASO)).

Roles and Responsibilities

1- **Policy Owner:** <head of 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 regulatory requirements.

Compliance

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

2- All personnel 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.