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

Insert organization logo by clicking on the outlined image.

Secure Configuration and Hardening 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 detailed cybersecurity requirements related to the secure configuration and hardening of <organization name>'s systems in order to minimize cybersecurity risks resulting from internal and external threats at <organization's name>.

The requirements in this standard 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 standard covers all <organization name>'s systems assets and applies to all <organization name> personnel (employees and contractors).

Standards

1	Security baseline standards definition
Objective	To define security baseline standards (including base configuration) for the systems infrastructure.
Risk implication	Lack of configuration standards may result in required settings and security configurations being omitted; it may lead to deployment of systems or infrastructure with active vulnerabilities and issues; and increased maintenance and upgrade overhead due to the number of versions deployed.
Requirements	
1-1	Security baseline standards and configuration parameters for systems infrastructure must be defined, documented and approved.
1-2	Security baseline standards for the following must be prepared:

	a) end user devices including tablets and mobile devices b) network devices including firewalls, routers and switches c) network operating systems d) servers e) operating systems f) business applications (including social media applications) g) remote access and telework infrastructure, including servers, VPN and end user devices h) other critical systems defined by management
1-3	Security baselines must reference: a) manufacturer published guidelines or instructions b) manufacturer issued upgrades, patches or settings c) <organization name> cybersecurity risk assessments d) vulnerability management scans and results e) results of security testing f) globally and nationally trusted sources of security best practice information g) <organization name> policies requiring particular requirements
1-4	<organization name> secure baseline and configuration standards must be defined and applied for incorporated cloud-based and hosted applications and services (including SaaS/PaaS/IaaS).
1-5	Default passwords for all accounts must be changed, and new passwords created, at first login. New passwords must be created in accordance with <organization name> identity and access management policy and standard.
1-6	Software must be configured to disable services and functionality not required for use by the <organization name>

	operations, where those services and functionality present risk to <organization name>.
1-7	A register of disabled services and functionality must be maintained by <organization name> for use in setting configurations and builds.
1-8	Secure baselines and configurations must include centralized clock synchronization with an accurate and trusted source – e.g., Saudi Standards, Metrology and Quality Organization (SASO).
1-9	Baselines and configurations must be deployed via standard builds, images and configuration files which have been created from a controlled, master (or Gold) reference build.
1-10	Secure baseline and configuration builds, images and files must be stored in a secure manner, with access limited to authorized personnel, using physical and logical access controls.
1-11	Secure baseline and configuration builds, images and files must be protected against unauthorized access, unauthorized change and unauthorized disclosure by logical and physical controls.
1-12	Access to security baseline standard and secure configuration documentation must be restricted to appropriate individuals within <organization name>.
2	Secure configuration implementation and deployment
Objective	To implement and deploy secure configurations across the organization.
Risk implication	Not implementing standard builds may leave the organization with a mix of configurations and security settings; active vulnerabilities and issues in the production environment; and an increased maintenance and upgrade overhead.

Requirements	
2-1	All new systems, devices and software must be built and configured to the approved secure baseline and configuration, using the relevant builds, images and files.
2-2	All new systems, devices and software must be successfully tested before implementation/roll-out to ensure they meet the approved secure baseline and configuration.
2-3	The implementation/roll-out of systems, devices or software that do not meet the approved secure baseline and configuration must be paused.
2-4	Cloud-based and hosted applications and services (including SaaS/PaaS/IaaS) must be deployed following <organization name> secure baseline and configuration standards for cloud-based and hosted applications.
2-5	Secure baseline configurations must be deployed to existing systems as soon as practical and during agreed maintenance periods.
2-6	Systems, devices or software that do not meet the approved secure baseline and configuration must be remediated by applying the approved secure baseline and configuration as soon as practical and during agreed maintenance periods.
3	Update secure configurations
Objective	To ensure that secure configurations are kept up to date, reviewed regularly and updated in a controlled manner.
Risk implication	Using out of date configurations may expose the organization to new or existing threats, degrade functionality, reduce performance and deploy systems or infrastructure with known and active vulnerabilities.
Requirements	

3-1	Security baseline standards and secure configurations must be reviewed at least once a year or after any significant change to <organization name> infrastructure, devices or software.
3-2	Deployed systems, devices and software must be reviewed at least once a year to ensure the approved secure baselines and configurations are deployed.
3-3	Change management procedures must be followed to update secure baselines and configurations.
3-4	Cloud-based and hosted applications and services must be assessed at least once a year to ensure the applications and services are deployed using the approved secure baselines and configurations.
3-5	Deployed secure baselines and configurations must be updated to the approved version as soon as practical and during agreed maintenance periods.
3-6	Evaluation of infrastructure and remote working systems and systems must be assessed at least once a year to ensure that remote access is provided using the approved secure baselines and configurations.
4	Anti-malware software configuration
Objective	To protect <organization name> used IT assets from malware.
Risk implications	Lack of anti-malware software may expose organization IT assets to infection and attack from malicious code, resulting in loss or damage to data and information, loss of productivity, error and unexpected shutdown.
Requirements	

4-1	<organization name> approved anti-malware (AM) software must be installed on all server and client (i.e., desktop, laptop, tablet, mobile) systems.
4-2	At a minimum, the AM software must be configured with the following capabilities: a) signature and/or non-signature-based malware detection b) alert generation for logging and monitoring.
4-3	At a minimum, the AM software must be configured to: a) connect to the network automatically b) run continuously and/or perform a regular scan for malware c) check and download updates automatically at the scheduled frequency d) log all activities undertaken by the software e) generate alerts to the responsible for the user and send alerts to a central monitoring system (e.g. the SOC) f) require privileged access for changes to operation.
4-4	Host-based Intrusion Prevention Systems (HIPS) and Host-based Intrusion Detection Systems (HIDS) must be installed on all <organization name> used servers, desktops, laptops, tablets (where the system is capable of running HIPS and HIDS).
4-5	At a minimum, the HIPS must be configured to: a) connect to the network automatically b) run continuously c) check and download updates automatically at the scheduled frequency d) log all alerts, blocked activities and traffic processed by the HIPS e) generate alerts for the user and send alerts to a central monitoring system (e.g. the SOC)

	f) require privileged access for changes to operation.
4-6	Assets provided under third party agreements must be configured to meet the requirements of this standard.
4-7	Third party’s assets that do not/cannot meet the requirements of this standard must be identified, logged and reviewed.
4-8	Email gateway systems must be configured to protect against malware as per the <organization name>’s email protection policy and standard.
5	Critical systems configuration
Objective	To deploy additional controls for secure configurations on critical systems.
Risk implications	Standard configurations, builds and adjustment operations may not provide the level of protection required by critical systems, as such systems may be subject to higher levels of threat, higher frequency of attacks and higher levels of business impact if system operation is interrupted.
Requirements	
5-1	Security baseline standards and secure configurations for critical systems must be reviewed at least every six months or after any significant change to <organization name> infrastructure, devices or software, as well as any changes to the relevant legal and regulatory requirements.
5-2	Deployed critical systems, devices and software must be reviewed at least every six months to ensure the approved secure baselines and configurations are deployed.
5-3	Deployed secure baselines and configurations must be updated to the approved version as soon as practical and during agreed maintenance periods.

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.