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

Insert organization logo by clicking on the outlined image.

Workstation Security 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 <organization name> workstations to minimize cybersecurity risks and protect it against internal and external threats at <organization name>.

These requirements are aligned with the Workstation Security Policy, mobile devices, personal devices, and NCA's cybersecurity requirements including but not limited to Essential Cybersecurity Controls (ECC - 1:2018), Critical Systems Cybersecurity Controls (CSCC - 1:2019), and other relevant legal and regulatory requirements.

Scope

This standard covers all workstations in the <organization name> and applies to all personnel (employees and contractors) in <organization name>.

Standards

1	Secure Access
Objective	To ensure the protection of workstations and their functionality against unauthorized access.
Risk Implication	Unauthorized access to workstations has severe implications that could lead to information theft and compromise where they can be used to carry out further harmful attacks against <organization name>'s personnel and infrastructure or against any other outside target.
Requirements	
1-1	Secure access and identity management for workstations must be implemented in accordance with the technical security controls mentioned in the Identity and Access Management standard applied in <organization name> in order to defend cybersecurity attacks.
1-2	Access to workstations must be limited to the accounts of the individual users of the workstations only.

1-3	In addition to a user/password combination, users must be required to use other authentication mechanisms or Multi-Factor Authentication (MFA), such as biometrics, hardware keys, one-time passwords, smart cards, certificates, etc., on workstations of highly protected environment, such as Security Operations Center (SOC).
1-4	BIOS bootloader passwords must be configured.
1-5	Restricting physical access to workstations to only authorized personnel.
1-6	Securing workstations (screen lock or logout) prior to leaving the workspace to prevent unauthorized access
1-7	Enabling a password-protected screen saver with a session timeout of <5 minutes> to ensure that workstations that were left unsecured will be protected.
1-8	Installing privacy screen filters or using other physical barriers to alleviate exposing data to authorized disclosure.
1-9	Exit running applications and close open documents when leaving the office.
1-10	Ensure access to wireless networks is secure by following the wireless security standard at <organization name>.
2	Secure Configuration and Hardening
Objective	To define critical workstation security requirements to ensure that the workstations are designed, configured and operated in a secure manner.
Risk Implication	Improper and weak configuration of workstations could create security vulnerabilities that could be exploited to jeopardize the confidentiality, integrity and availability of <organization name>'s data and business operation.

Requirements	
2-1	Secure configuration and hardening for workstations must be implemented in accordance with the technical security controls mentioned in the Secure Configuration and Hardening standard applied in <organization name> in order to defend cybersecurity attacks.
2-2	Unnecessary/unrequired applications and services, such as Telnet Protocol, touch keyboard, remote registry (if not needed), etc., must be removed/disabled on workstations.
2-3	Secure workstation images or templates must be created for all workstations based on the approved configuration standard controls and as per <organization name>'s Secure Configuration and Hardening Policy, and compromised workstations must be reimaged using one of the workstation image templates.
2-4	Workstation images must be stored in a secure environment on securely configured offline backups or storage environment, and they must be validated regularly using integrity monitoring tools.
2-5	Installing unauthorized software on workstations must be blocked.
2-6	Watermark feature must be used on workstations.
3	Endpoint Protection Software
Objective	To ensure the protection of workstations from viruses, malware, advanced persistent threats (APTs), zero-day attacks and any other type of malicious attacks.
Risk Implication	Successful malicious attacks on workstations could expose <organization name> to a breach, unauthorized access and disclosure of data if workstations are left unprotected.

Requirements	
3-1	Prevent creation/modification/deletion of operating system settings and peripheral security software. For example, changing system time manually, editing system files, creating/modifying/deleting files, etc., must be disabled.
3-2	Application whitelisting must be implemented on workstations to allow only specific applications and software to run based on need.
3-3	Application whitelisting must be implemented and two features of identifying the application must be used, including but not limited to cryptographic hash rules, publisher certificate rules or path rules to allow or restrict the use of applications.
3-4	Application whitelisting agents must be configured so that users cannot disable the agents with the exception of administrators when performing specific administrative tasks that require disabling application whitelisting temporarily.
3-5	For application whitelisting, a list of approved executable files (exe, com, pif, etc.), software libraries (dll, ocx, etc.), scripts (ps1, bat, vbs, etc.), and installers (msi, msp, etc.) must be defined to allow files from the approved list to be executed only.
3-6	Host-based Intrusion Prevention System (HIPS) must be implemented on all workstations.
3-7	Software host firewall must be implemented on all workstations.
3-8	Antivirus must be implemented on all workstations.
3-9	Antimalware must be implemented on all workstations.
3-10	Host Advanced Persistent Threat (APT) agents must be implemented on all workstations.

3-11	Endpoint Detection and Response must be implemented on all workstations.
3-12	Endpoint Device Control software must be implemented on all workstations to prevent the use of unauthorized peripheral devices.
3-13	Data Leakage Prevention (DLP) must be implemented where deemed necessary by <organization name>'s relevant policies and procedures.
4	Cryptography
Objective	To ensure the confidentiality of user data and verify its integrity and authenticity against unauthorized access and sensitive information disclosure.
Risk Implication	Lack of proper security technologies to ensure the encryption of workstations data may expose <organization name>'s data to high cyber risks as a result of unauthorized access.
Requirements	
4-1	Cryptography for workstations must be implemented in accordance with the technical security controls mentioned in the Cryptography standard applied in <organization name> in order to prevent attempts of unauthorized access.
4-2	Workstations storage media, including hard disks, must be encrypted where deemed necessary by <organization name>'s relevant policies and procedures.
4-3	Workstation management protocol that supports or configures encryption for workstation management protocols, such as LDAP over TLS, SNMPv3 with authentication and privacy, Kerberos with TLS, encrypted syslog, etc., must be used.

5	Central Management
Objective	To define security requirements for the management of workstations to ensure that workstations are centrally managed and operated in a secure manner and ensure all security requirements are implemented and enforced.
Risk Implication	Lack of secure management and enforcement of security requirements on workstations increase the attack surface and expose <organization name> environment to potential vulnerabilities and weaknesses that could be exploited in a malicious attack or breach to compromise <organization name>'s workstations and data.
Requirements	
5-1	The central management server or domain server must be configured to enforce <organization name>'s workstation security policy on all workstations.
5-2	System configuration management tools that automatically enforce and redeploy configuration settings to workstations at regularly scheduled intervals must be deployed. For more details, refer to the <organization name>'s Secure Configuration and Hardening Policy.
5-3	A Security Content Automation Protocol (SCAP) compliant configuration monitoring system must be implemented to verify all security configuration elements, catalog approved exceptions, and alert when unauthorized changes occur.
6	Privileged Access Workstations "PAW"
Objective	To define additional security requirements for the protection of privileged access workstations PAWs used to access critical systems and network zones.
Risk Implication	Successful malicious attacks on PAWs could expose <organization name> to serious breaches and compromise of its most critical assets leading to extremely harmful outcomes.

Requirements	
6-1	Use of multi-factor authentication must be required for accessing PAWs used by system administrators.
6-2	Access to PAWs must be restricted to only authorized administrators and operators.
6-3	PAWs must be placed in the network management zone.
6-4	All traffic transmitted to or out of PAWs, including administrative access and control traffic (such as Secure Shell “SSH” and Remote Desktop Protocol “RDP”), and data traffic using cryptographic mechanisms (such as Transport Layer Security “TLS”), must be encrypted as per <organization name>’s Cryptography Standard.
6-5	Internet access on PAWs must be disabled.
6-6	Services that are not necessary or required (such as sending and receiving emails) must be disabled on PAWs.
6-7	All levels of logging, as well as audit trail and security logs, must be enabled locally and to a centralized event logging system.
7	Other Standard controls
Objective	To implement all workstation security standard controls and requirements to ensure the highest protection levels.
Risk Implication	Failure to implement all security standard controls and requirements exposes <organization name> to increased workstations security risks.

Requirements	
7-1	The following standard must be implemented in relevance to workstations: 1. Cybersecurity Event Logs and Monitoring Management standard 2. Cybersecurity Backup management standard 3. Physical security standard

Roles and Responsibilities

1- **Standard Owner:** <head of cybersecurity function>.

2- **Standard Review and Update:** <cybersecurity function>.

3- **Standard Implementation and Execution:** <information technology function> and <cybersecurity function>.

4- **Standard Compliance Measurement**: <cybersecurity function>.

Update and Review

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

Compliance

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

2- All personnel at <organization function> must comply with this standard.

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