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.

Privileged Access Workstations 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 for Privileged Access Workstations in <organization name>.

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, CSCC-1:2019 and CCC-1:2020, in addition to other related cybersecurity legal and regulatory requirements.

Scope

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

Standards

1	Workstation Security Controls
Objective	Ensure the successful deployment of secure workstations
Risk Implication	If workstation protection is not properly implemented, this may lead to severe implications that encompasses information theft, unauthorized access and information disclosure.
Requirements	
1-1	Privileged Access Workstation (PAW) must be both logically and physically located in a dedicated, secured and trusted network segment.
1-2	PAWs must be covered by the Privileged Access Management (PAM) and have additional monitoring compared to regular workstations. In addition to regular workstation, all events with privileged access on PAWs must be monitored and logged.
1-3	<organization name> must implement endpoint management services for proper PAWs monitoring and controls.

1-4	PAWs must limit the use of any risky applications to absolute necessary functionalities to work in accordance with the project and should not be connected to the Internet.
1-5	PAWs must incorporate application whitelisting policy to use only verified and approved software applications or executable files to provide dedicated services.
1-6	PAWs must not connect to Wi-Fi networks.
1-7	PAWs' software security updates and patches must be applied as soon as available and according to <organization name>'s change management procedure. Update process must not interrupt any applications that are crucial for privilege access management.
1-8	Access to PAWs must be restricted to selected administrators by only allowing access using network Access Control Lists (ACL) to administrators' individual accounts, which must be separated from their normal accounts and used only for a specific purpose.
1-9	Default/non-interactive/unneeded accounts must be disabled or renamed.
1-10	Session timeout and session idle lockout must be configured in accordance with <organization name>'s cybersecurity policies.
1-11	BIOS bootloader passwords must be configured on all PAWs.
1-12	Host-based Intrusion Prevention System (HIPS) must be implemented on all PAWs to prevent known and unknown malicious attacks
1-13	Software host firewall must be implemented on all PAWs to control the specific network behavior of individual applications on a system

1-14	Antivirus and Endpoint Detection and Response (EDR) software must be implemented on all PAWs.
1-15	Data Loss Prevention (DLP) agents must be implemented on all PAWs.
2	Hardware root of trust
Objective	Ensure proper hardening process of workstations by creating a ‘root of trust’. Proper technology must be selected in order to fulfill this objective.
Risk Implication	Improper hardening process may result in creating hardware vulnerabilities and attack vectors this can have severe implications that could lead to information theft, unauthorized access and information disclosure.
Requirements	
2-1	PAWs must be built on trusted hardware provided by trusted and verified supplier/third party vendor. Hardware must be maintained by trusted supplier periodically.
2-2	Any PAWs changes (especially relating to the operating system) must be logged and monitored. Log solution must be configured to send only specific logs to the central log system e.g., using syslog protocol and CEF, LEEF or RFC 5425 specified log format.
2-3	PAWs must implement a secure boot procedure to ensure that workstations boot only using software that is trusted by the Original Equipment Manufacturer (OEM).
2-4	PAW hardware drivers and firmware must be updated in a secure manner, using cybersecurity best practices (e.g., hash comparison).
2-5	PAWs must support Hypervisor-Protected Code Integrity (HVCI) technology to isolate the Code Integrity (CI) decision-

	making function from the rest of the operating system (Windows only).
2-6	PAWs must implement kernel Direct Memory Access (DMA) protection to prevent memory access attacks by malicious external devices.
2-7	PAWs must implement software security measures to protect and maintain the integrity of the system.
2-8	On startup, PAWs must validate that system integrity has truly been maintained through local and remote attestation.
3	Other Standards
Objective	The goal is to implement all PAW applicable and mandatory standards and requirements to ensure the highest levels of protection.
Risk Implication	Failure to align with <organization name>'s security standards and requirements could lead to information theft, unauthorized access and information disclosure.
Requirements	
3-1	The following standards must be implemented in relevant to PAWs: 1. Virtualization security 2. Key Management 3. Certification Authority 4. Cryptography 5. Event and audit logging 6. Physical security 7. Secure configuration and hardening

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 privileged 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.