©(ORGANISATION NAME)

HARDENING/BASELINE STANDARDS

Subject: Hardening/Baseline Standards		Author: MuVio Solutions Ltd
Document Type: Policy (Internal)	Page: 1 of 8	Authorised by:
Effective Date: June 2024	Version 1.0	Next Review:

Author	**Signature**	**Date**
Muvio Solutions Ltd (Consultant Designation)		

Revision History:

Version	Date	Change Number	Summary of Changes
1.0	April, 2024		

Distribution:

Name	Title

Approved By:

Name	Signature	Date
Name (Designation)		
Name (Designation)		
Name (Designation)		
Name (Designation)		

Document Ownership

Information Security

Document Control

The validity of this document is limited to the use of the policy as a guideline for Information Security Organisation-wide. In the event that the adopted policy framework changes, the document will have to be reviewed and the document owner must assess this document for relevancy at that point. This document will be reviewed at least annually and updated accordingly to reflect changes to business objectives or the risk environment.

Document Control

The Document Owner controls the distribution of this document. The distribution is as follows:

- Chief Information Security Officer
- Chief Information Officer
- Chief Risk Officer
- Chief Audit Executive
- Chief Compliance Officer
- Head, Human Resources

Notice and Warning

This document is the property of CcHUB. Circulation is restricted to the Organisation’s use. It must not be copied or used for any other purpose other than for which it is supplied, without the expressed written authority of CcHUB.

Except where provided for purposes of contractual requirements, CcHUB disclaims any responsibility or liability for any use or misuse of the document by any person and makes no warranty as to the accuracy or suitability of the information to any third party. Any misuse of the document is addressable by CcHUB.

CONTENTS

1.0 Introduction

Networks form the basic means of electronic communication within and outside the organisation. Therefore, the organisation should deploy appropriate measures to protect these assets. Furthermore, interaction with external networks such as the Internet and other third-party networks introduces the risk of potential compromise to the organisation's information asset.

Reference	Description of Risk
SAFETag	Organisation Device Usage
SAFETag	User Device Assessment

1.2 Objectives

The objective of the standard is to ensure that the organisation devices (and other personal devices used in accessing the organisation resources) are adequately configured prior to usage in the production environment and to continuously evaluate to ensure all devices used by the organisation meet the minimum security requirement.

2.0 Hardening Standards for Network Devices

2.1 Access to network resources shall be in accordance with global best practices i.e. all access should be authenticated, authorised, and password security enforced.

2.2 All generic/inbuilt user credentials on the network devices should be disabled (except when there is a business need, in this case, the password must be changed, and ownership must be assigned).

2.3 Unused services, protocols, and ports shall be disabled on all network devices.

2.4 The network devices should be running on non-vulnerable operating systems that are being supported by the OEM (Original Equipment Manufacturer).

2.5 Network devices shall be adequately patched with the current fix released by the OEM (Original Equipment Manufacturer).

2.6 Logs capturing all changes to the network devices must be enabled.

2.7 Network devices are configured to send logs to a centralised Security Information and Event Management Tool (SIEM) or any other dashboard for correlation.

2.8 Network devices shall be securely configured to synchronise their time with an NTP server.

2.9 Remote access the network devices shall be through authorised VPN connectivity. Also, on premise access to the network devices shall be through access-list with permitted/whitelisted IP addresses.

2.10 Secured SNMP shall be deployed on all network devices for the purpose of monitoring; the use of unsupported and insecure versions of SNMP is prohibited.

2.11 All traffic traversing the network shall be encrypted.

2.12 Create warning banners for standard login services.
Recommended Banner "This is a <<Organisation Name>> network resource and is intended to be used by authorised <<Organisation Name>> users only. If you are not an authorised user, please do not attempt to access.
All access attempts are monitored. Any unauthorised access will be prosecuted by Law and <<Organisation Name>> policy".

3.0 Hardening Standards for Software/Application

3.1 Access to software/applications shall be in accordance with global best practices i.e. all access should be authenticated, authorised, and password security enforced.

3.2 All generic/inbuilt user credentials on the Software/Application should be disabled (except when there is a business need, in this case, the password must be changed, and ownership must be assigned).

3.3 Where available, segregation of function through maker-checker (imputer-authorizer) should be enabled on all applications.

3.4 Software and application on production environment should be free from unsecured/vulnerable components and utilities.

3.5 Vulnerability assessment should be conducted on software/applications prior to going live. Also, routine vulnerability and penetration testing should be conducted on software/applications after they have gone live.

3.6 Where available, application whitelisting software that prevents all applications that have not been specifically whitelisted from running on the system should be deployed.

3.7 Support from Software/Application OEM (Original Equipment Manufacturer) should be readily available.

3.8 Software/Applications shall be adequately patched with the current fix released by the OEM (Original Equipment Manufacturer).

3.9 Logs capturing all changes to the Software/Applications must be enabled.

3.10 Software/Applications are configured to send logs to a centralised Security Information and Event Management Tool (SIEM) or any other dashboard for correlation.

4.0 Hardening Standards for Operating Systems

4.1 Access to operating systems shall be in accordance with global best practices i.e. all access should be authenticated, authorised, and password security enforced. These privileges should be extended to the applicable OS file level permissions.

4.2 All generic/inbuilt user credentials on the operating system should be disabled (except when there is a business need, in this case, the password must be changed, and ownership must be assigned).

4.3 Servers and Workstations should be running on non-vulnerable operating systems that are being supported by the OEM (Original Equipment Manufacturer).

4.4 Servers and Workstations shall be adequately patched with the current fix released by the operating system’s OEM (Original Equipment Manufacturer).

4.5 Servers and Workstations shall be securely configured to synchronise their time with an NTP server.

4.6 Where applicable/available, all Servers and Workstations should be adequately joined to the organisation’s domain controller.

4.7 Where applicable/available, Group Policies (GPO) should be defined on the domain controller and enforced on all Servers and Workstations for basic security. Where domain controllers are not available, local Group Policies (GPO) should be defined and enforced on individual Servers and Workstations.

4.8 All available/mandatory security and monitoring solutions (i.e. antivirus, DLP, etc.) available within the organisation must be installed on all Servers and Workstations.

4.9 Appropriate audit policies should be enabled on all Servers and Workstations for capturing of relevant logs. Specifically, all privileged activities consummated by the administrator or root accounts must be logged.

4.10 Servers and Workstations are configured to send logs to a centralised Security Information and Event Management Tool (SIEM) or any other dashboard for correlation.

4.11 Configure a screensaver to lock the console screen automatically if the host is left unattended. Require password to unlock.

4.12 Create warning banners for standard login services.
Recommended Banner "This is a <<Organisation Name>> computer resource and is intended to be used by authorised <<Organisation Name>> users only. If you are not an authorised user, please do not attempt to access.
All access attempts are monitored. Any unauthorised access will be prosecuted by Law and <<Organisation Name>> policy".

5.0 Hardening Standards for Databases

5.1 Access to Databases shall be in accordance with global best practices i.e. all access should be authenticated, authorised, and password security enforced. These privileges should be extended to the applicable Table-level, Column-level, and Row-level permissions. In addition, database services should be configured to run under a low privileged user account.

5.2 All generic/inbuilt user credentials on the Database should be disabled (except when there is a business need, in this case, the password must be changed, and ownership must be assigned). As much as possible, avoid using the built-in administrator privileges (root, sa or SYS accounts) for routine activities.

5.3 Databases should be running on non-vulnerable versions that are being supported by the OEM (Original Equipment Manufacturer).

5.4 Databases shall be adequately patched with the current fix released by the operating system's OEM (Original Equipment Manufacturer).

5.5 Appropriate audit policies should be enabled on all databases for capturing of relevant logs. Specifically, all privileged activities consummated by the administrator or root accounts must be logged.

5.6 Databases are configured to send logs to a centralised Security Information and Event Management Tool (SIEM) or any other dashboard for correlation.

5.7 Data dictionary for all databases/tables created on the database management system (DBMS) shall be maintained and adequately updated based on changes to the database/table schemas.

5.8 All sensitive/PII fields defined on the database/tables shall be adequately protected/encrypted in line with the applicable extant regulation.

5.9 Database traffic shall be encrypted in transit and at rest.

5.10 Network (TCP) access shall be disabled on all databases. All access required calls should be over a local socket file or named pipe.

5.11 Databases shall be configured to only bind on localhost.

5.12 Access to databases is restricted to the network port to specific hosts with firewall rules.

5.13 Database servers should be kept in a separate dedicated LAN segment which is different/isolated from the application server.

5.14 Databases and Applications should not be running/installed on the same/single server.

5.15 Where available, install a trusted digital certificate on the database server.

5.16 Configure a regular backup of the database. Ensure that the backups are protected with appropriate permissions, and ideally encrypted.

6.0 Hardening Standards for Mobile Devices

6.1 Ensure that all Applications are installed from Official Stores.

6.2 Update the device software and applications as soon as possible/available by the OEM.

6.3 Use strong lock-screen pins/passwords: a 6-digit PIN is sufficient if the device wipes itself after 10 incorrect password attempts. Set the device to lock automatically after 3 minutes.

6.4 Consider using Biometrics (e.g., fingerprint, face) authentication for convenience to protect data of minimal sensitivity.

6.5 Only use original charging cords or charging accessories purchased from a trusted manufacturer. DO NOT use public USB charging stations. Never connect personal devices to government computers, whether via physical connection, Wi-Fi, or Bluetooth.

6.5 If available, mobile devices that will be used to access organisation resources should be enrolled on Mobile Device Management (MDM) solutions.