Insert the organization logo by clicking on the image icon

Mobile Device Policy Template

Date:

**Document Control**

|  |  |
| --- | --- |
| **Document Title:** | Mobile Device Policy Template  |
| **Document ID:** |  | Version: | 0.1 |
| **Status:** | Draft |  |
| **Publish Date:** |  |

**Document Review**

|  |  |  |  |
| --- | --- | --- | --- |
| Version No. | Date | Reviewer(s) | Remarks |
|  |  |  |  |
|  |  |  |  |

Table of Contents

[1. Objective 4](#_Toc97458298)

[2. Scope 4](#_Toc97458299)

[3. Policy 4](#_Toc97458300)

[3.1 General Requirements 4](#_Toc97458301)

[3.2 Mobile Devices User Responsibilities 5](#_Toc97458304)

[3.3 Mobile Devices DST Responsibilities 5](#_Toc97458305)

[3.4 Mobile Devices Monitoring and Audit 6](#_Toc97458314)

[4. Policy Enforcement 6](#_Toc97458315)

# Objective

The objective of this policy is to minimize risks associated with using of the Mobile Device such as smartphones, tablets, laptops and other personal computing devices by the <entity name> employees to access internal information, data and services, However, the portability offered by these devices can also increase security exposure to unauthorized access, theft of information, theft of services, and malicious disruption of services.

# Scope

This policy applies to all employees who use the <entity name> mobile devices or personal devices to access information, data and services at the <entity name>.

# Policy

## General Requirements

1. All <entity name> mobile devices must be protected during the powered on with a secured complex password, passphrase or (biometric) and automatically locking for the mobile devices after several unsuccessful access attempt.
2. Stored information and data in mobile devices must be encrypted.
3. Connecting for mobile devices to Wireless access point in the <entity name> should be in accordance with Wireless Access Policy.
4. Mobile devices accessing <entity name> information or data should be in accordance with Access Control and physical Security Policy.
5. <entity name> mobile devices shall refrain from connecting to public or unsecured network.
6. Employees intend to use their Bring Your Own Device (BYOD) to access <entity name> information or data shall be after the management appropriate authorization.
7. <entity name> must conduct an assets inventory for all managed and unmanaged mobile devices connected to network.
8. Mobile devices shall be physically secured.
9. Unused <entity name> mobile devices must be stored in a security location.
10. Mobile devices accessing <entity name> network shall have active and up to date anti-malware, anti-virus and host firewall protection.
11. Designated Security Team (DST) must enable for a location service on all mobile devices and enable for a remote wiping.
12.
13.

## Mobile Devices User Responsibilities

* + 1. Employees shall report for any lost or theft immediately to DST.
		2. Unauthorized access to mobile devices or <entity name> data must be immediately reported to DST.
		3. Mobile devices shall not be rooted, jailbreak or installing for an unauthorized software or firmware.
		4. Employees shall not load illegal content or pirated softwares on the mobile devices used to access <entity name> information, data.
		5. Only approved softwares and applications by the DST are allowed to use.
		6. Keeping the mobile devices, softwares and applications up to date to most secured and stable version based on DST instructions.
		7. Ensuring the mobile devices operating system batches are installed based on the DST instructions.
		8. Mobile devices modification on the configuration must be authorized by DST.

## Mobile Devices DST Responsibilities

* 1.
	2.
	3.
1.
2. 1.
	2.
	3.
3. Managed and unmanaged mobile devices security standards and configuration must be identified and incorporate to all <entity name> employees.
4. Whitelist must be identified for approved softwares and applications.
5. Mobile devices must be authenticated by leveraging the AAA infrastructure established by the <entity name>.
6. Multi-Factor Authentication (MFA) must be implemented to all <entity name> users before accessing internal network (e.g. token, biometrics, trusted MFA application, etc).
7. Mobile devices must comply with <entity name> security policy before network access granted by implementing a Network Access Control (NAC).
8. Ensuring the mobile devices are protected with anti-virus, anti-malware and host firewall are enabled before accessing network and any mobile devices not meet the <entity name> protection level must be quarantined or network access terminated.
9. Security standards and configuration for mobile devices shall be enforced by DST using the Mobile Device Management (MDM) solution.
10. Utilizing MDM solution for asset inventory to identify manged and unmanaged mobile devices connected to organization /entity network.
11. Utilizing MDM solution for softwares scanning to identify running softwares and applications on the mobile devices.
12. DST shall use the MDM solution to enforce encryption and devices containerization to secure the stored information and data in the mobile devices.
13. DST shall use the MDM solution to wipe the mobile devices remotely if lost or theft.
14. Portable media connectivity to mobile devices should be in accordance with Removable Media Policy.
15. DST must review and update the security standards and configurations in regularly basis.

## Mobile Devices Monitoring and Audit

1. All mobile devices shall be routinely monitored, and security audits performed to verify the compliance with this policy, and to identify unauthorized mobile devices access.
2. Access logs and system audit trails shall be enabled and reviewed regularly.
3. Logs of the anti-malware, anti-virus and host firewall must be reviewed regularly.

# Policy Enforcement

1. Policy document sponsor and owner: <Head of Cyber Security Department>.
2. Policy implementation and enforcement: <Department Concerned with Information Technology>.
3. Any violation of this policy may subject the offender to disciplinary action as per the procedures followed in <entity name>.

-End of the Document-