Table of Contents

[1. Introduction to Mobile Devices & Teleworking Policy 5](#_Toc79058819)

[2. Purpose 5](#_Toc79058820)

[3. Scope 5](#_Toc79058821)

[4. Policy Specifications 5](#_Toc79058822)

[**4.1 Authorization** 5](#_Toc79058823)

[**4.2 Registration of Devices** 5](#_Toc79058824)

[**4.3 User Responsibility** 6](#_Toc79058825)

[**4.4 Affected technology** 6](#_Toc79058826)

[**4.5 Incident Reporting procedure** 6](#_Toc79058827)

[**4.6 Disposal** 6](#_Toc79058828)

[5. Awareness 7](#_Toc79058829)

[6. Organization Protocol 7](#_Toc79058830)

[7. Policy Non-Compliance 7](#_Toc79058831)

[8. Exceptions 7](#_Toc79058832)

[9. Employee Declaration 7](#_Toc79058833)

**DOCUMENT REVISION CONTROL**

REVISION HISTORY

| **Date** | **Author** | **Version** | **Change Reference** |
| --- | --- | --- | --- |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

REVIEWERS

| **Name** | **Position** | **Date** |
| --- | --- | --- |
|  |  |  |
|  |  |  |
|  |  |  |

DISTRIBUTION

| **Date** | **Distributed to** | **Version** | **Distribution Format** |
| --- | --- | --- | --- |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

APPROVALS

| **Date** | **Version** | **Approved by** | **Designation** | **Signature** |
| --- | --- | --- | --- | --- |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

**LIST OF ABBREVIATIONS**

|  |  |  |
| --- | --- | --- |
| **Index** | **Abbreviation** | **Stands For** |
| I | IT | Information Technology |
| 2 | SLA | Service Level Agreement |
| 3 | IOT | Internet of things |
| 4 | IAS | International Accounting Standards |
| 5 | FDP | Finance Department |
| 6 | ITSM | Information Technology Service Management |
| 7 | NDA | Non-Disclosure Agreement |

DEVICE WORKFORCE SEGMENTATION

| **Date** | **Work style** | **Business requirements** | **Location** | **Target Device** |
| --- | --- | --- | --- | --- |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

TELECOMMUTING AUTHORIZATION

| **Employee name** | **Designation** | **Address** | **Mobile no** | **No of weekdays** | **Importance** |
| --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

TELECOMMUNICATING SCHEDULE

| **Timings** | **Monday** | **Tuesday** | **Wednesday** | **Thursday** | **Friday** | **Saturday** |
| --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |

1. **Introduction to Mobile Devices & Teleworking Policy**

This document defines how the process of Mobile Devices & Teleworking Policy is implemented within <Company Name>.

It set outs framework, principles and expectations that apply to Mobile Devices & Teleworking. Teleworking includes different work arrangements and shall include home-working and working from remote locations, and other working arrangement as authorized by <Company Name>, under [**XXXXXXXX**] direction.

This policy will help restrict employees to copy, save or write data on any other media, while working in an unprotected environment, like home, remote locations, and even in protected environments.

Teleworking arrangements shall expand the scope of information security policy while using Mobile Devices & Teleworking.

1. **Purpose**

The purpose of Mobile Devices & Teleworking Policy shall support security measures to be adopted while using mobile devices, such that information assets are not compromised and are protected using physical protection, access control, cryptographic techniques, backups and virus and other situations, in an unprotected and protected environment.

1. **Scope**

This policy applies to all the users in the Organization, including temporary users, visitors with temporary access to services with limited or unlimited access time.

Also Teleworking policy applies to the use of all devices, that can be used for Teleworking, namely laptops, tablets, USB memory sticks, Mobile Devices - Smartphones, anything on which data can be stolen, or copied.

1. **Policy Specifications**

## **4.1 Authorization**

The use of mobile device outside the normal organization business hours, will be subjected to Authorization. The Authorization for Teleworking will be provided by **[XXXXXX]** at **[XXXXXXX]**

## **4.2 Registration of Devices**

All devices used for Teleworking, should be registered on the organization asset register

1. It is responsibility of the user to ensure that their devices risk assessed and registered
2. In case it is not registered, it will be considered as violation of policy, it will deem a disciplinary action as per **[XXXXXXXX]** rules.

## **4.3 User Responsibility**

Mobile devices

1. shall be protected from theft and from being compromised, at or in unprotected environment.
2. shall never be left unattended, in easily accessible and unprotected areas. Special care will be taken in public places
3. shall be kept secure and under lock and key when not in use.
4. shall be password protected, as per password policy
5. shall follow backup, antivirus procedures
6. shall follow mail and internet security policies, and encryption policies, as advised by information security department
7. Shall use only authorized software, as specified and installed by Information security

Users are advised

1. not to download games, social sites, screen savers et cetera that can attract or can lead to compromise the mobile device
2. that they cannot share or leave Mobile Devices with anyone else other than themselves.

## **4.4 Affected technology**

Connectivity of all mobile devices will be centrally managed by [company name]’s IT department and will utilize authentication and strong encryption measures. Although IT is not able to directly manage external devices – such as home PCs – which may require connectivity to the corporate network, end users are expected to adhere to the same security protocols when connected to non-corporate equipment. Failure to do so will result in immediate suspension of all network access privileges so as to protect the company’s infrastructure.

## **4.5 Incident Reporting procedure**

In case of any incident, Incident management procedure [Ref: XXXXXXXX] needs to be initiated in accordance with <Company Name> IT department

It is user responsibility to report loss or information, including contacting IT service desk and information passed to Information Security Team

## **4.6 Disposal**

Information Asset, is approved and issued to user, as authorized by [XXXXXXX]

Disposal and destruction of Information asset will follow “Disposal and Destruction Policy”

1. **Awareness**

This policy shall provide users awareness of security issues while using Mobile Devices & Teleworking, and user shall take proper prior authorization, from deemed authorized representative within <Company Name>.

# Organization Protocol

IT can and will establish audit trails and these will be accessed, published, and used without notice. Such trails will be able to track the attachment of an external device to a PC, and the resulting reports may be used for investigation of possible breaches and/or misuse. The end user agrees to and accepts that his or her access and/or connection to [company name]’s networks may be monitored to record dates, times, duration of access, etc., to identify unusual usage patterns or other suspicious activity. This is done to identify accounts/computers that may have been compromised by external parties. In all cases, data protection remains [company name]’s highest priority.

# Policy Non-Compliance

Failure to comply with this policy may, at the full discretion of the organization, result in the suspension of any or all technology use and connectivity privileges, disciplinary action, and possibly termination of employment. The (i) Vice-President of Finance, (ii) Chief Operating Officer, and (iii) immediate Manager or Director will be advised of breaches of this policy and will be responsible for appropriate remedial action which may include disciplinary action, including suspension or termination of employment.

# Exceptions

In certain circumstances, exceptions to this policy may be allowed based on demonstrated business need. Exceptions to this policy must be formally documented and approved by the Chief Information Officer. Policy exceptions will be reviewed on a periodic basis for appropriateness.

# Employee Declaration

I [employee name], have read and understand the above Mobile Devices and Teleworking Policy, and consent to adhere to the rules outlined therein

Employee signature Date

Manager signature Date

IT administrator signature Date