TELECOMMUTING & MOBILE COMPUTING POLICY

*Revision: r1.0*

*Effective Date: ddmmyyyy*

*Classification: INTERNAL*

**INTERNAL INFORMATION**

This is a proprietary document and is the property of XXXX.; it contains information that is proprietary, or otherwise restricted from disclosure. If you are not an authorised recipient, please return this document to the above-named owner(s). Dissemination, distribution, copying or use of this document in whole or in part by anyone other than the intended recipient is strictly prohibited without prior written permission of XXXX.

Table of Contents

1. Introduction 3

1.1 Document Definition 3

1.2 Objective 3

1.3 Scope 3

1.3.1 Applicability to Employees 3

1.3.1 Applicability to External Parties 3

1.3.2 Applicability to Assets 3

1.4 Related Documents / References 3

2. Policy Statements 5

2.1 Management Approval for Remote Access 5

2.2 Telecommuting Privileges Review 5

2.3 Alternative Worksite Review 5

2.4 Pre-Requisite Training 5

2.5 Device Security Procedures 5

2.6 Mobile Device Security Baseline 5

2.7 Acceptable Use 5

2.8 Reporting of Lost Devices 5

2.9 Device Lock-Out 6

2.10 Unattended Device Inactivity 6

2.11 Remote Wipe Capability 6

2.12 Malicious Mobile Code 6

2.13 Automatic Device Discovery 6

2.14 Privacy Law & Legislation 6

2.15 Physical Security Requirements 6

2.16 Bring Your Own Device (BYOD) 7

3. Policy Compliance & Enforcement 9

3.1 Compliance Measures 9

3.2 Enforcement 9

4. Exception Process / Glossary 10

4.1 Exception Process 10

4.2 Glossary / Acronyms 10

5. Document Management 11

5.1 Document Revision Log 11

5.2 Document Ownership 11

5.3 Document Coordinator 11

5.4 Document Approvers 11

5.5 Document Distribution 11

# Introduction

## Document Definition

This document is a Policy.

For a full description of document types, see XXXX-POL-ALL-001 *- Information Security Policy Framework*.

## Objective

The objective of this policy is to provide information security requirements to:

* Ensure the secure use of mobile devices;
* Protect XXXX. (XXXX) data stored on or transmitted using mobile devices, and;
* Access to XXXX’s networks and computing resources by authorised remote workers.
* This also covers homeworking by staff

The scope of this policy includes all mobile devices (both company provided, and personal (a.k.a. Bring Your Own Device (BYOD)) that connect to a XXXX network or contains XXXX data. Mobile devices include, but are not limited to, mobile phone, tablets, laptops etc. regardless of make / model / functionality.

## Scope

### Applicability to Employees

XXXX refers to XXXX. as well as its majority-owned subsidiaries and joint ventures (if applicable). This Policy applies to all Employees (including staff working from home), officers, members of Board of Directors, and all consultants, and contractors.

### Applicability to External Parties

Relevant Policy statements will apply to any external party and be included in contractual obligations on a case-by-case basis.

### Applicability to Assets

This Policy applies to all information assets globally owned by XXXX, or where XXXX has custodial responsibilities.

## Related Documents / References

* *XXXX-POL-ALL-001- Information Security Policy Framework*
* *XXXX-POL-ALL-002 - Acceptable Use Policy*
* *XXXX-POL-ALL-009 - Access Control Policy*
* *XXXX-POL-ALL-012 - Incident Response Policy*
* *XXXX-STD-ALL-013- - Authentication Standard*
* *XXXX-POL-ALL-016 - Encryption & Key Management Policy*

# Policy Statements

## Management Approval for Remote Access

Working from an alternative worksite must be approved by Employee’s direct line manager and processed by IT

## Telecommuting Privileges Review

Line managers of telecommuting Employees must re-evaluate the privileges on a quarterly basis and report findings / recommendations to IT

## Alternative Worksite Review

XXXX retains the right to inspect telecommuter worksites without notice and to examine the content of any computing device thought to contain XXXX data assets.

## Pre-Requisite Training

Employees must complete some remote access training by IT prior to being granted remote access privileges.

## Device Security Procedures

XXXX must have procedures in place to provision, de-commission, and secure mobile computing devices that connect to a XXXX network.

## Mobile Device Security Baseline

A security baseline must be developed and applied to all XXXX mobile devices per the policy.

Security baselines must consider all applicable legislative, statutory, regulatory, and contractual requirements and configured accordingly. Further guidance is outlined in *XXXX-STD-ALL-020 - Vulnerability Management Standard.*

## Acceptable Use

Users of mobile devices must comply with all the requirements of the *XXXX-POL-ALL-002 – Acceptable Use Policy*.

## Reporting of Lost Devices

Any loss of a mobile device containing XXXX information must be immediately reported to IT.

Authentication mechanisms for mobile devices must be configurable, provide sufficient protection of the device and stored data, and comply with the *XXXX-POL-ALL-009 - Access Control Policy*.

## Device Lock-Out

User access to a mobile device must be locked after a pre-defined number of failed login attempts.

## Unattended Device Inactivity

Any mobile device left unattended for a pre-defined amount of time must automatically lock and clear the screen.

## Remote Wipe Capability

All XXXX owned mobile devices must have the ability to be remotely erased to protect against unauthorised access to XXXX data in the event of device loss or theft.

## Malicious Mobile Code

Any suspected or confirmed interaction with malicious mobile content must follow the *XXXX-POL-ALL-012 - Incident Response Policy*.

## Automatic Device Discovery

All mobile devices utilising wireless discovery connection protocols (e.g., Bluetooth) must not be automatically discoverable.

## Privacy Law & Legislation

At all times this policy must comply with privacy law and legislation in all regions it covers.

## Physical Security Requirements

When working remotely staff must ensure the following

* Ensure the security and safety of the equipment; such equipment shall be password protected where the feature exists.
* Keep sensitive hard copy records locked away as much as possible.
* Promptly shred any hard copy record that is no longer required
* Not working on public Wi-Fi
* Always keep XXXX equipment away from friends and family.
* Minimise as much as possible visitors’ access to the working area where equipment and records are located

## Bring Your Own Device (BYOD)

* All Users are expected to protect personal devices used for work-related purposes from loss, damage, or theft.
* Remove any XXXX information stored on your device once you have finished with it including deleting copies of attachments to emails, such as documents, spreadsheets and data sets, as soon as you have finished using them.
* Remove all XXXX information from your device and return it to the manufacturers’ settings before you sell, exchange, or dispose of your device
* The XXXX will not be responsible for loss or damage of personal applications or data resulting from the use of XXXX applications or the wiping of XXXX information
* Upon resignation or termination of employment, or at any time on request, the user may be asked to produce the personal device for inspection. All XXXX’s data on personal devices will be removed by IT upon termination of employment.

All users must take appropriate secure measures under the XXXX’s Acceptable Use Policy including but not limited to:

* Ensuring that their BYOD device is password protected using the features of the device and that a “strong password,” as defined in the Authentication Standard, is required to access the XXXX’s network and information
* Ensuring that their BYOD device locks itself with a password or PIN if the device is idle for one minute for phone and tablets, and not more than 10 minutes for laptops, computer systems and other devices
* Not using rooted (Android) or jailbroken (iOS) devices to access the XXXX’s information and network
* Not sharing their BYOD devices with friends, relatives, and family members
* Not using the BYOD devices on a public Wi-Fi
* Not storing or transmit illicit material or proprietary information belonging to another organisation
* Using their BYOD devices to access only the information authorized to access under the XXXX authentication and authorization procedures.
* Maintain the BYOD device themselves ensuring it is regularly patched and upgraded, including anti-virus
* Reporting lost, misplaced or stolen BYOD devices to the IT department within 24 hours
* Paying all costs associated with purchasing and their BYOD device.
* Report any security breach immediately to IT helpdesk
* Users are expected to exercise the same discretion in using their personal devices as is expected for the use of the XXXX’s devices. The XXXX’s policies pertaining to harassment, discrimination, retaliation, trade secrets, confidential information and ethics applies to the use of personal devices for work-related activities.
* The XXXX has the right, at any time, to monitor and preserve any communications that uses its networks in any way, including data, voice mail, telephone logs, Internet use and network traffic, to determine proper use.
* No user may knowingly disable any network software or system identified as a monitoring tool.
* The use of your own device MUST adhere to the XXXX’s Information Security Policy Framework
* From time to time, the XXXX may require that you install or update XXXX-approved device management software on your own device.
* It is your responsibility to familiarise yourself with the device sufficiently to keep data secure.

# Policy Compliance & Enforcement

## Compliance Measures

If applicable, compliance with the above Policy can be measured by the following criteria. Example evidence will vary depending on any supporting guidelines implemented to support this Policy. The following list is not exhaustive, and all example evidence types may not be required to validate compliance.

Evidence of compliance can be presented in hard copy or electronic format.

|  |  |
| --- | --- |
| **Criteria** | **Example Evidence** |
| For mobile device computing, evidence that a security baseline exists. | * A copy or screenshot of the mobile device security baseline |
| For a selection of lost devices, evidence that the device loss was reported to the appropriate personnel. | * Copies of communications related to the lost devices |
| For mobile devices, evidence that the device must be authenticated. | * Screenshots that the authentication system for mobile devices |
| For a selection of mobile devices, evidence that the device will lock after a certain number of failed login attempts. | * Observe a selection of devices * Screenshots of the configuration parameter for failed login lock including the number of attempts allowed |
| For a selection of mobile devices, evidence that the screen will lock and clear once the threshold is met. | * Observe a selection of devices * Screenshots of the configuration parameter for lock and clear including the timing threshold |
| For mobile devices, evidence that the device can be remotely erased. | * Screenshot of the remote erase command enabled * Observe remote erase on test device if possible |
| For a selection of mobile devices reportedly affected by malicious code, evidence that the reporting and handling of the device followed the Incident Response Policy. | * Copies of device issue reports and actions taken |
| For a selection of mobile devices with wireless discovery communication protocols, evidence that the device is not discoverable | * Screenshots of the selected devices discovery parameter |

## Enforcement

All staff of XXXX must comply with all Information Security Policies. Failure to comply with these policies may result in disciplinary action in accordance with the current XXXX Human Resources policy. Disciplinary actions may include, but are not limited to:

* verbal and/or written warnings;
* instant dismissal;
* and actions by judicial and regulatory authorities.

# Exception Process / Glossary

## Exception Process

Non-compliance with the Policy statements described in this document must be reviewed and approved in accordance with the Exception Process defined in *XXXX-POL-ALL-001 - Information Security Policy Framework*.

## Glossary / Acronyms

|  |  |
| --- | --- |
| BYOD | Bring Your Own Device |
| Malicious Code | Software designed to infiltrate or damage a computer system or mobile device without the owner's informed consent. |
| Security Baseline | Typically, a document or device configuration image that offers a "cookbook recipe" for a normal level of protection. |

# Document Management

## Document Revision Log

|  |  |  |  |
| --- | --- | --- | --- |
| **Date** | **Editor** | **Revision #** | **Description of Change** |
|  |  |  |  |
|  |  |  |  |

## Document Ownership

This Policy is owned by the YYYY

## Document Coordinator

This Policy is coordinated by the YYYY

## Document Approvers

|  |  |  |
| --- | --- | --- |
| **Approver Name** | **Signature** | **Date** |
|  |  |  |
|  |  |  |

## Document Distribution

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

* All Staff