Bring Your Own Device Policy (BYOD)

**Classification**: Internal

This document may only be shared internally without prior confirmation from the owner.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Version | Approved By | Owner | Date Last Updated | Review Frequency | Next Review | Comments |
|  |  |  |  |  |  |  |

Contents

[Purpose of This Document 1](#_Toc132710524)

[Scope 2](#_Toc132710525)

[Responsibilities 2](#_Toc132710526)

[Exceptions 2](#_Toc132710527)

[Device Security 2](#_Toc132710528)

[Device minimum requirement 2](#_Toc132710529)

[Data Storage 2](#_Toc132710530)

[Remote Device Management 3](#_Toc132710531)

[Incident Reporting 3](#_Toc132710532)

[Costs 3](#_Toc132710533)

[Termination of Employment 3](#_Toc132710534)

[Training Requirements 3](#_Toc132710535)

# Purpose of the Policy

TechSolution.inc recognises employees' desire to use personal devices. This policy defines the security standards for such devices and the user's responsibilities.

# Scope

This policy covers:

* Anyone who uses their personal device for TechSolution.inc business purposes.
* Devices handling TechSolution.inc data, such as;
* Mobile phones
* Computers (Laptops / Desktops, etc)
* Tablets / Electronic notepads
* USBs

# Responsibilities

Line Managers will;

* Oversee team compliance.

All employees must;

* Follow this policy & procedures.
* Inform their manager or IT of any policy violations.

IT Team will;

* Aid in the policy's execution.

# Exceptions

* Exceptions should be requested via the IT Help Desk.

# Device Security

* Users must protect their devices against unauthorised access. Secure measures include;
  + Passwords (see the password policy)
  + PIN codes
  + Biometrics (facial or fingerprint)

# Minimum Device Requirements

* + - Devices must run the latest operating system and have updated security patches. IT will enforce access via 'conditional access rules'. For clarification, contact the IT Help Desk.
    - Install antivirus and anti-malware software.
    - Set devices to update security patches automatically.
    - Encrypt devices. For assistance, consult the Helpdesk.

# Data Storage

* Avoid storing company data on personal clouds or unencrypted drives.
* Refrain from saving sensitive information about employees or TechSolution.inc contacts on personal devices.
* Never store signatory reports and evaluations on personal devices.

# Remote Device Management

* TechSolution.inc retains the right to oversee and control BYOD devices, especially for security and data/applications related to TechSolution.inc.

# Incident Reporting

* Report any security issues concerning BYOD devices to the IT team immediately.

# Costs

* Employees bear all device and operating costs.

# Termination of Employment

* On employment termination, staff must erase TechSolution.inc data and passwords from their devices. Relevant details should be passed to their manager.

# Training Requirements

* New employees receive this policy and must familiarise themselves with it.