Mobile Device Policy

Reference: FPD0062-2022

Version: 1

Owner: James Pobgee

First Issued Date:

Revision Issued Date:

To outline the rules for the appropriate and secure use of mobile devices within FISCAL Technologies.

Prepared for:
All Employees, select Contractors,
Partners and Customers

Prepared by:
James Pobgee

FISCAL Technologies Ltd
448 Basingstoke Road,
Reading, RG2 0LP
Tel: 0845 680 1905

1 CONFIDENTIALITY

This document is the property of FISCAL Technologies. It may not be copied, distributed, or recorded on any electronic or other medium without the express written permission of the company.

All material contained in this document which is not readily available in the public domain is regarded as confidential to FISCAL Technologies and may not be divulged to any other parties without the express written permission of FISCAL Technologies.

Table of Contents

2 DOCUMENT CONTROL

Item	Description
Document Title:	Mobile Device Policy
Associated Controls:	B.5.10 B.5.11 B.5.15 B.5.18 B.5.2 B.6.4 B.6.5 B.6.7 B.7.13 B.7.14 B.7.9 B.8.1 B.8.10 B.8.12 B.8.19 B.8.3 B.8.9
Reference ID:	FPD0062-2022
Version:	1
Status:	Draft
Approver:	
Approval Date:	
First Issued Date:	15/08/2023
Revision Issued Date:	
Reference Documents:	Linked Policies: • Acceptable Use Policy • Information Security Governing Policy Linked Procedures: Linked Records:

2.1 DOCUMENT PUBLICATION HISTORY

(All revisions made to this document must be listed in chronological order, with the most recent revision at the bottom)

Version	Date	Author
1		James Pobgee

3 PURPOSE AND SCOPE

3.1 PURPOSE

The purpose of this policy is to establish rules or the appropriate and secure use of mobile devices within FISCAL Technologies. This policy sets forth standards for the selection, provisioning, management, and security of mobile devices, as well as the responsibilities of employees who use these devices for work purposes.

3.2 SCOPE

This Mobile Device Policy applies to all employees, select contractors, partners, and customers who use mobile devices to access, process, store, or transmit FISCAL Technologies data or systems, regardless of ownership or funding source. This policy covers all mobile devices used for work purposes, including but not limited to smartphones, tablets, laptops, and smartwatches. This policy applies to all locations where work is performed, including off-site locations, and to all mobile devices used to connect to the organisation's networks or systems.

4 MOBILE DEVICE POLICY

The security of FISCAL Technologies' data and systems are of utmost importance. Mobile devices are increasingly being used for work purposes, and we must ensure that the devices used within our organisation meet the necessary security standards.

4.1 MOBILE DEVICE PROVISIONING

To ensure that mobile devices are set up correctly and that employees have access to the necessary applications and data, FISCAL Technologies has established the following criteria for the provisioning of mobile devices:

For specific details on software and hardware requirements please refer to the Acceptable Use Policy.

4.1.1 Application provisioning

Employees must have access to the necessary applications to perform their work duties. This includes access to email, productivity applications, and any specialised applications required for their job role.

The following policies apply to application provisioning:

- All applications must be risk reviewed and approved by the IT Department prior to installation or use.
- Applications must be downloaded from the official app store for the device's operating system or the company MDM.
- The IT department will configure and deploy necessary applications to work devices.

4.1.2 Device ownership

Work devices are owned by FISCAL Technologies and should be used for work purposes only.

Personal devices may be used for work purposes if they meet the necessary security criteria and are approved by the IT department. In the case of personal devices, FISCAL will only provide access to work-related applications and data via the Mobile Device Management (MDM) solution.

4.2 MOBILE DEVICE MANAGEMENT

FISCAL Technologies uses a Mobile Device Management (MDM) system to manage and secure mobile devices used for work purposes. All mobile devices used for work, including company-owned and employee-owned devices, must be enrolled in FISCAL Technologies MDM system.

In the case of an employee using a personal mobile device/s, the employee is responsible for enrolling their mobile devices in FISCAL Technologies' MDM system and keeping them up to date with the latest security patches and software updates. Devices that are not enrolled in our MDM system will not be allowed to access work-related information or systems.

Our MDM system can:

- Remotely lock, wipe, or locate lost or stolen devices.
- Monitor device usage and enforce security policies (such as device encryption, biometric or passcode locks, automatic screen locking, and automatic application updates)
- Install and update approved applications on devices.
- Enforce passcode policies and encryption requirements.
- And configure Wi-Fi, VPN, and other network settings.

Employees should be aware that by enrolling their personal mobile device in our MDM system, they are allowing FISCAL Technologies the ability to remotely access and manage their device. However, FISCAL Technologies will only access or monitor these mobile devices, as needed for business purposes and in accordance with FISCAL Technologies' privacy policy.

Any attempts to circumvent or disable FISCAL Technologies' MDM system on a work device will be considered a violation of this policy and may result in disciplinary action, up to and including termination of employment.

4.3 MOBILE DEVICE SECURITY

4.3.1 Device compliance

To ensure the security of FISCAL Technologies' data and systems, all mobile devices used for work must comply with the organisation's requirements set out within its MDM system.

4.3.2 Compliance monitoring

FISCAL Technologies' MDM system will monitor devices for compliance with the above-mentioned requirements and alert FISCAL Technologies if a device is found to be non-compliant. Employees will be required to take immediate action to bring their assigned device into compliance, such as updating the OS or enabling the required security settings.

4.4 DEPROVISIONING MOBILE DEVICES

To protect FISCAL Technologies' data and information, all mobile devices must be fully deprovisioned and appropriately wiped of all sensitive/company information when they are no longer in use or when an employee leaves the organisation.

4.5 USER RESPONSIBILITIES

All employees, contractors, partners, and customers who are authorised to use mobile devices in the course of their work for FISCAL Technologies must ensure the following:

- Protection of mobiles devices.
- Ensure that mobile devices are not left unattended and are kept in a secure location.

- Minimize the amount of information stored on a mobile device to only that which is needed to fulfil the business activity which is being delivered when working outside the normal office environment.
- Use special care in public places, open offices, meeting places and other unprotected areas (e.g., avoid reading confidential information if people can read from the back, lock you screen when away from the device, etc).
- Do not share your passcodes/pins.
- Report lost or stolen devices to the IT department promptly.
- Do not use jailbroken or rooted devices.
- Store and transfer company data only using approved applications and kept to an absolute minimum required to complete your roles requirements.
- Report any suspicious or unauthorised activity related to data or devices to the IT department.
- Comply with all applicable laws, regulations, and policies.
- Follow the IT department's instructions for appropriate device use.
- Take care of the device to prevent damage, unauthorised access, or loss.
- Obtain IT departments approval for any modifications to the device and before using personal cloud storage or storing data locally on the device.

5 ENFORCEMENT AND VIOLATIONS

5.1 ENFORCEMENT

All divisions & employees of the organisation must comply with the requirements of this policy. Management is responsible for ensuring that the policy is implemented within its area of responsibility.

FISCAL Technologies expects all users to comply with the terms of this policy and all other policies, procedures, guidelines, and standards published in its support.

5.2 VIOLATIONS

Violations of this policy shall result in disciplinary action / legal ramifications by the organisation. Disciplinary action will be consistent with the severity of the incident as determined by an investigation and as deemed appropriate by Management and HR.

Compliance with this policy will be reviewed by the organisation's Internal Audit Team.