

Company Name

Mobile Devices Security Policy

Month – 2022

Table of Contents

Overview.....	4
Purpose	4
Scope	4
Policy	4
Must Abide.....	5
Technical Support.....	6
Individual Responsibility.....	7
Accountability, Risk and Exemption	7
Compensation	8
Discipline.....	9
Definition	10
Encryption	10
Individuals	10

Document Control

Type of Information	Document Data
Title	ASSIGNED Policy
Version	<Document Number>
Issue Date	<Year>
Document Owner	<COMPANY>
Document Creator	<Name>

Revision History

Version	Date	Author	Summary of Changes
1.0	1 Mar 2022	<Name>, <Designation>	First document

Document Approver

Version	Approval Date	Approving Authority	Signature
1.0	1 April 2022	<Designation>	

Mobile Device Security Policy

Overview

The COMPANY intends to protect its data, equipment, and records from unauthorized access, use, disclosure, alter, deletion, damage, and removal.

Purpose

The Mobile Device Security Standard specifies the minimum-security policy for remotely accessing COMPANY systems, data, and networks using both COMPANY and personal devices. All approved devices that frequently access COMPANY data and systems must be adequately protected to prevent unauthorized access, loss or compromise of confidential data, virus spread, and other forms of abuse of the COMPANY computing and information infrastructure.

Scope

This policy applies to all staff, managers, stakeholders, third-party vendors, and individuals who connect their personal device to the COMPANY network for business operations, such as:

- Portable computing devices – For example, Laptop, Notebook, Netbook.
- Portable storage devices - For example, USB, Memory card, DVD, and Portable HDD.
- Mobile devices: For example, tablets, smart watches, and smartphones.

Policy

Staff, employees, stakeholders, and users who wish to participate in the BYOD must follow this policy when using their personal devices on the COMPANY network.