Mobile Devices Policy

Objective and Scope

The objective of this policy is to describe the security measures to be adopted to manage the risks associated with the use of mobile devices, to ensure they do not compromise business and client information.

A mobile device is a broad definition considered to be any computing device small enough to hold and operate in the hand. Generally, devices connect to the internet and interconnect with other devices via Wi-Fi or Bluetooth. Integrated cameras, digital media players, mobile phones, and Global Positioning System (GPS) capabilities are all considered mobile devices.

Power is typically provided by a lithium battery. Mobile devices may run mobile operating systems that allow third-party applications to be installed and run.

The scope of this policy as it applies to mobile devices covers:

- maintaining a register of devices used for business purposes whether company or privately owned
- physical protection of devices
- restrictions of software installation to 'approved list' installations only
- control of software versions and applying patches
- access and encryption controls
- use of web services and web applications
- remote disabling, erasure or lockout
- backups

Roles, Responsibilities and Authorities

The Operations Director or competent IT Team delegate takes ownership of the Mobile Asset Register, issuance of company mobile assets, device setup and ensuring data security protocols are in place.

The Operations Director and the IT Team take ownership of mobile asset management in relation to assigning, tracking and return of remote assets including wiping of company data on privately owned assets on termination of employment.

Company devices are assigned owners for general use and compliance to this policy. Equipment and portable devices (regardless of ownership) are listed on the Asset Register against the assigned user.

Where an exception or deviation from an expectation or plan occurs, the senior assigned role shall make the determination in terms of what is an acceptable change. The change management process may need to be enacted.

Mobile Devices Policy

Legal and Regulatory

Title	Reference
The Telecommunications (Lawful Business practice)(Interception of Communications) Regulations 2000	www.hmso.gov.uk/si/si2000/20002699.htm
Computer Misuse Act1990	www.hmso.gov.uk/acts/acts1990/Ukpga_19900018_en_1.htm
The Privacy and Electronic Communications (EC Directive) Regulations 2003	www.hmso.gov.uk/si/si2003/20032426.htm
The Freedom of Information Act 2000	https://www.legislation.gov.uk/ukpga/2018/12/contents
Online Safety Act 2023	https://www.legislation.gov.uk/ukpga/2023/50/contents/enacted
National Assistance Act 1948	https://www.legislation.gov.uk/ukpga/Geo6/11-12/29/enacted
Criminal Law Act 1967	https://www.legislation.gov.uk/ukpga/1967/58/introduction
The Copyright, Designs and Patents Act 1988	https://copyrightservice.co.uk/

ISO 27001/2 REFERENCES	ISO 27001: 2013 Clause ID	ISO 27002: 2013 Annex A ID	**ISO 27001: 2022 Clause ID**	**ISO 27002: 2022 Control ID**
Mobile device policy Security of assets off premises	8.0	6.2.1		7.9
User endpoint devices				8.1

Related Information

- Remote and Teleworking Policy
- Physical (Equipment) Asset Management Policy
- Asset Register (Mobile Devices)
- Information Classification Policy

Definitions and acronyms

Data	A unit that contains raw materials which do not carry any specific meaning.
Information	Information is a group of data that collectively carries a logical meaning
Risk assess	A systematic process that involves identifying, analysing and controlling hazards and risks
Secure area	Area for handling sensitive information or shelter valuable IT equipment
Threats	A threat exploits a vulnerability and can damage or destroy an asset
Vulnerabilities	Vulnerability refers to a weakness in your hardware, software, or procedures.

Policy

Information stored on, processed by or accessible via user endpoint devices shall be protected regardless of its location. Endpoint device use is a business imperative however, standards are set in place to protect information from unauthorised access, misuse or intrusion software capabilities.

Mobile Devices Policy

Prevision Research accepts that privately owned mobile devices may be used remotely or for general company purposes only on approval by the Operations Director. All roles with high risk IT access shall be provided with company owned equipment and cannot use these devices for any other purpose. Refer Information Classification Policy.

Persons provided with company mobile devices may be required to complete and sign a declaration acknowledging duties and responsibilities in regard to the mobile device, or this may be included in an employment agreement.

Persons permitted to use their own mobile device for company business may be required to acknowledge their duties and responsibilities in regard to waiving ownership of business data and allowing the wiping of data by the Operations Director or representative in the case of theft, loss of the device or on employment termination.

Regardless of ownership, each device must meet the minimum company standards in terms of security and use.

Minimum company standards

1. Mobile devices shall be approved as fit for purpose and registered for business purposes, whether company or privately owned by the Operations Director or IT Team delegate.
2. Mobile devices shall be maintained with a protective cover, not left unattended by the owner and not shared with any other person.
3. The Operations Director shall determine the software applications to be installed on the mobile device from the 'approved list' of installations only and determine who takes responsibility for control of software version updates and applying patches.
4. Access controls shall be put in place including password protection and encryption controls as determined by the Operations Director.
5. For business provided mobile devices the use of web services and web applications is limited to those approved by the Operations Director.
6. The company reserves the right to remotely disable, erase or lockout a device that has been subject to unauthorised access, loss, theft or otherwise at risk of a secure data breach.
7. All devices are subject to the agreed backup via cloud arrangements as determined by the Operations Director.

Asset management – Operations Director, IT Team and Owner

Issuance of company mobile devices, once approved for use by the relevant manager, shall be subject to Operations Director set up with installation of the required business software applications, encryption controls and other control settings. Settings and controls will vary depending on the high risk level of data security required of the role.

The owner of a **company mobile device** will be provided with instructions including:

- the need to install a unique password subject to change control
- mobile device protection from misuse, loss, damage or data breach
- restrictions on use by designated owner only

Mobile Devices Policy

- the need to ensure the mobile device is kept updated with control of software version updates and patch application immediately on notification appearing on the device

When information is considered highly sensitive yet is necessary to store on an endpoint device, approval by the Operations Director is required and the device must be company owned.

The owner of a **privately owned mobile device** will be instructed to:

- install a unique password subject to periodic change control
- allow for the installation of protection software to prevent misuse, loss, damage or data breach
- protect the device and/or business content on the device by use from other users
- ensure the mobile device is kept updated with control of software version updates and patch application immediately on notification appearing on the device

No information considered highly sensitive can be stored on a privately owned endpoint device.

Device security

Mobile devices shall be virus/malware protected according to Operations Director instruction. When a version change or patch update is notified on the device, this shall be enabled immediately on notification.

Suspected unauthorised access of a mobile device

Report any lost, damaged mobile device, unauthorised access/use or suspected malware activity immediately to the Operations Director. Provide details regarding likely impact on data security and effects on company or client information.

Policy review

This policy shall be reviewed by the policy owner no less than annually or immediately after a process change or a policy breach is known to have occurred. Refer below for the most recent review.

History table

Date	Rev No	Changes	Reviewed By	Approved By	Training Y/N