[Company]

MOBILE AND TELEWORKING POLICY

Remote working and mobile devices

1 Document Version Control

	Last Modified	Last Modified By	Document Changes
0.1	[DATE]		Document first created

2 Document Contents Page

3 Mobile and Teleworking Policy

3.1 Purpose

To manage the risks introduced by using mobile devices and to protect information accessed, processed, and stored at teleworking sites.

3.2 Scope

All employees and third-party users.

All company mobile devices.

All personal devices used to access, process or store company information.

3.3 Principle

Mobile devices and remote sites are to have adequate protection of company information.

4 Mobile Policy

4.1 Mobile Device Registration

Mobile devices are recorded in the asset register.

Mobile devices are assigned to a named individual.

Assigned owners are provided with a copy of the Mobile and Teleworking Policy and informed of their responsibility for the device and the information contained on it.

Mobile devices have appropriate encryption, anti-virus and access control installed where available.

4.2 Mobile Device Assigned Owner Responsibilities

Assigned owners are personally responsible for the device.

To ensure operating system and application patching is up to date.

To ensure encryption and antivirus where installed is enabled.

To ensure the device is not left unattended and when not in use physically secured.

To only access company information required for role in line with the Access Control Policy.

To not install software or change the device that would be in breach of the company information security policy, regulations, or applicable legislation.

Personal and confidential data is not stored on the device unless authorised and recorded in the asset register.

To not allow others including family members to access or use the assigned device.

To return the mobile device when no longer required, when requested or when leaving the company employment.

4.3 Mobile Device Firewall

Any mobile device connecting to payment card cardholder data environment must have a personal firewall installed and configured.

The personal firewall software must be configured to specific documented configuration settings, actively running, and not alterable by users of mobile and/or employee-owned devices.

4.4 Mobile Remote Wipe

Mobile devices are enabled to have their contents remotely wiped in the event of loss or theft. This feature is enabled prior to the user being given access to the mobile device and mobile devices have their automatic lockout enabled.

4.5 Mobile Back Up

Mobile devices are not backed up by default to company back up solutions and is the responsibility of the assigned user.

5 Teleworking / Remote Working Policy

Teleworking and remote working refer to working from a location outside the company directly owned and operated office space and connecting via networks that are not owned and controlled by the company.

The company does not operate a traditional teleworking model. There are circumstances where employees may wish to connect from remote locations. Subject to applicable laws and regulations which take precedence employ responsibilities include

- To ensure an adequate health and safety work environment.
- To ensure applicable insurance cover is in place.
- To adhere to the mobile device policy.
- To not use public open networks when connecting to services and where necessary and applicable to utilise VPN technology.

Equipment and storage are not left unattended in public or unsecured areas.

Protection and steps are taken to prevent viewing of information on a device on public transport and / or where shoulder surfing could occur.

6 Bring Your Own Device Policy (BYOD)

It is not the company policy to allow ‘bring your own device’ or use of personal mobile devices by default. Authorisation is required from the information security management team, the management review team, or the information security manager.

Where a personal mobile device is allowed

- The mobile device is recorded in the asset register.
- The user receives training and signs an acknowledgement of responsibility.
- All company policies including access control and the information security policy apply.
- The same policy for mobile devices, the Mobile Device Policy, apply.
- No personal data or sensitive data as defined by the GDPR, or Data Protection Act 2018 are to be stored on the device.

7 Policy Compliance

7.1 Compliance Measurement

The information security management team will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

7.2 Exceptions

Any exception to the policy must be approved and recorded by the Information Security Manager in advance and reported to the Management Review Team.

7.3 Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

7.4 Continual Improvement

The policy is updated and reviewed as part of the continual improvement process.