Mobile Device and Teleworking Policy

PHX030

Contents

Purpose of this Document

Phoenix has a responsibility to ensure that all data stored on its IT systems is relevant and is securely held, is available in a complete and accurate form when needed and complies with the requirements of the General Data Protection Regulations and recommendations of the Information Security Committee.

The use of mobile devices increases the risks associated with the secure storage of data. The purpose of this policy is to set out the criteria for the provision of mobile devices and the conditions relating to their use. This policy is a supplementary policy to Phoenix Information Security Policy.

Intended Audience

This policy is applicable to all staff, contractors and third parties working within Phoenix who utilise mobile devices.

This policy applies to all mobile devices owned by the company that have access to corporate networks, data, and systems. This includes, but is not limited to, laptops, smartphones, and tablet devices.

Responsibilities – All Staff

It is the responsibility of all staff, whether based within Blenheim House or working externally, to ensure the confidentiality, availability and integrity of data belonging to Phoenix and to comply with the requirements of the General Data Protection Regulations.

- each mobile device user - whether this is a Bring Your Own Device (BYOD) or provided by the company - must take personal responsibility for the security of the equipment, software, and data in their care
- unofficial, unauthorised, or unlicensed software must not be loaded on company mobile devices
- mobile devices in cars must be stored out of sight and transported safely
- mobile devices must be physically protected against theft; never being left in cars within sight or left overnight and protected on other forms of transport, hotel rooms, conference centres and meeting places
- when travelling, devices (and media) should not be left unattended in public places
- laptops should be carried as hand luggage when travelling by public transport
- devices, where applicable, must be configured with a secure password that complies with the Acceptable Use Policy. This applies to personal devices which access the company network
- users must report all lost or stolen devices to the Phoenix HR Department immediately

- if a user suspects that unauthorised access to company data has taken place via a mobile device the user must report the incident Phoenix HR Department immediately
- for remote working, access to Phoenix information, networks and applications can be attained via the secure Virtual Desktop Infrastructure (VDI) or through VPN.
- home PCs and mobile devices should not be used to access the Phoenix network unless by VDI utilising encrypted logons
- users conducting remote working should not allow or give permission for unauthorised users (including family and friends) to use their PC/mobile device
- when connecting a company device to home Wi-Fi, staff are responsible for ensuring the Wi-Fi connection is encrypted
- users should always be aware of the potential for other people (including family, friends, colleagues, and intruders) to overlook screens and keyboards and view personal, confidential information or passwords. Users should ensure this does not take place
- users should always be aware of the higher risk to data loss/leakage when working in a public environment e.g. a café, public transport, conference facilities

IT Department

It is the responsibility of the Service Desk Department to ensure the correct configuration of the mobile devices that are issued to employees:

- encryption must be applied to all laptops
- all support and maintenance must be carried out or arranged by the Service Desk Department
- all mobile phone devices accessing company data must have a 6-digit pin, have the ability to be wiped, be on the latest version of the OS and be encrypted
- all data stored and saved on a laptop must default to a location that is backed up

Bring Your Own Device

Employees who use a personal device (BYOD) to access Company data are required to create a secure pin to restrict email access on their device.

The company's device management server detects a device accessing data and if it is not protected with the correct security controls, it will not allow the device to access Company data.

If the user's device does not have a secure pin, the device is not encrypted or does not have an up-to-date OS, they will be prompted to remediate those items. If they choose not to do this access will be denied and Company data will be removed from the device after a period of time.

Working from Abroad

Employees do not have access to company data outside of the UK. In the event an employee wants to access emails while abroad, Managerial approval must be provided. Any data access beyond emails must have Board approval.

Operational System

Virus Protection

All mobile devices must have up-to-date anti-virus software (if available for the platform) installed at the time they are issued. The anti-virus system's database will be updated on a regular basis. Under no circumstances shall the user delete or disable the anti-virus software.

Backups

Mobile devices should not be the primary repository of data; they may be used to hold changes until reconnected to the network and synchronisation can take place with the network storage.

If the above cannot be adhered to, advice should be sought from the Service Desk Department as to the best means of backing up data.

Personal Use

A reasonable level of personal data is accepted on Phoenix mobile devices. Phoenix does not accept responsibility of loss of this data.

Right to Inspect Data

All data and software held on Phoenix's mobile devices may be inspected by authorised staff at any time and without warning. Users may be required to remove software or data which is deemed to be inappropriate.

Version Control

Author	Version	Date	Description
ISC	1.0	01/07/2015	Original Document
ISC	2.0	18/11/2015	PIN Security
ISC	3.0	25/09/2018	Annual Review
ISC	4.0	10/10/2019	Annual Review
ISC	5.0	10/08/2021	Removal of Mobile Device Request / P11 Information
ISC	6.0	02/08/2022	Updated terminology during annual review

Document Approval

Name	Version	Date	Position
Sam Mudd	1.0	01/07/2015	Managing Director
Sam Mudd	2.0	18/11/2015	Managing Director
Sam Mudd	3.0	25/09/2018	Managing Director
Sam Mudd	4.0	10/10/2019	Managing Director
Sam Mudd	5.0	10/08/2021	Managing Director
Clare Metcalfe	6.0	30/09/2022	Operations Director

Signed: Clare Metcalfe Clare Metcalfe, Operations Director

Dated: 30/09/2022