Mobile Device Policy

Title

Mobile Device Policy

Version Control

Owner	Version	Edited By	Date	Comments
IS Rep	0.1	Karl Lapage	19/01/16	First Draft

Distribution

Held By	Format	Location	Comments
	Digital / Physical		

Status

X	Status	Approved By	Date
	Working		
X	Draft		
	Provisional Approval		
	Publication		

Classification

	Please refer to ISMS 02 Information Handling & Classification Procedure
X	**Confidential**
	Restricted
	Unclassified

Relevance to Standard

Standard	Clause	Title
ISO 27001:2013	A6.2.1	Mobile Device Policy

Mobile Device Policy

1.0 Overview

The mobile device policy describes the organisation's approach to managing risks associated to the use of mobile devices which includes but is not limited to Mobile Telephones, Smartphones, Table Computers, Laptops, Handheld devices.

2.0 Policy

2.1 Registering Mobile Devices (and BYOD)

All mobile devices shall be registered with the **IT Support Company** before being used to access the organisation's information assets.

The **IT Support Company** will apply any such security controls that it deems necessary to protect the device taking in to consideration:

- the value/sensitivity of data being stored or processed on the device,
- the environment in which the device is being used,
- Potential threats of third parties and
- Any other threats to the confidentiality, integrity or availability of the asset.

Bring Your Own Device is prohibited by the organization for security reasons.

2.2 Securing the Device

All mobile devices will have a PIN Number or Password enforced that conscribes to the minimum complexity as defined in the password policy.

Where a biometric security option exists, this should be used in preference to mitigate against PIN Numbers or Passwords being over looked.

However, employees should ensure that the **IT Support Company** have the ability to access the device and decrypt any data on the device and this may require a PIN Number or Password to be disclosed to the **IT Support Company** if it is changed.

2.3 Physical Security

Mobile devices should be stored and carried securely at all times. Careful consideration should be given before leaving a mobile device in a car, on a table or in visible in another public place.

When using a mobile device, the user should always consider the environment they are working in and be aware of opportunities to be overlooked or over heard.

Mobile devices should not be left unattended at any time, and the loss or theft of devices will be reported to the **IT Support Company** immediately.

2.4 Software & App Installation

Only software and apps authorized by the **Managing Director,** on advice of the **IT Support Company** are permitted to be installed on mobile devices.

All requests for new software or application installs shall be raised to the **IT Support Company**.

All software and apps installed on a mobile device shall be kept up-to-date by the user to avoid any security vulnerabilities.

The underlying operating system of the device shall be kept up-to-date by the user to avoid any security vulnerabilities.

2.5 Network Connections

Users will exercise caution when connecting mobile devices to public WIFI hotspots, or other connections, and this should be avoided as far as possible.

For internet access, users should use the organisation's authorized network connection.

Remote access to the organisation's network is not permitted.

When using web based services to carry out transactions or transfer information, the user will ensure that a trusted SSL certificate is available for the website in use. This is usually denoted by a pad-lock symbol located somewhere in the browser window.

Security alerts and warnings should never be ignored, and where one occurs the user should cease their activity immediately and report it to the **IT Support Company.**

2.6 Malware Protection & Security Controls

The applied Malware protection and any other security software should not be disabled or removed from the device.

If the user believes that the software is not functioning correctly, it should be reported to the **IT Support Company** at the earliest opportunity.

2.7 Remote Administration

The user understands that mobile devices may be remotely controlled, disabled, locked-out, tracked or erased by the **IT Support Company** to prevent unauthorized access to data on the device.

It is for this reason that it is recommended that personal data, including photographs, messages and music are not stored on the device.

The user will not attempt to by-pass or disable this remote functionality.

2.8 BackUp

Data and/or the mobile device settings will be backed up subject to the data backup policy.

2.9

2.10

3.0 Related Policies

Authorised Software List (see IT Handbook and/or standard PC build)
Password Policy.
Data Backup Policy. (see IT Handbook)