MOBILE DEVICE POLICY

Eco Sourcing Hub
REDUCE COSTS, EMISSIONS & RISKS

+44 300 131 1331 ✉
www.ecosourcinghub.co.uk 🌐

FM001

1 - Introduction

Mobile devices, such as smartphones and tablets, are important tools for our organisation. However, mobile devices also represent a significant security risk as, if the appropriate security applications and procedures are not applied, they can be a conduit for unauthorised access to the organisation's data and IT infrastructure. This can subsequently lead to data breaches and system infection.

Eco Sourcing Hub Ltd has a requirement to protect its information assets to safeguard its customers, intellectual property and reputation. This document outlines a set of practices and requirements for the safe and secure use of mobile devices.

2 - Roles & Responsibilities

The Company Director is responsible for maintaining this policy and ensuring that it is fully implemented.

3 - Policy Scope

All mobile devices, whether owned by Eco Sourcing Hub Ltd or owned by employees, that have access to company networks, data and systems, not including company IT-managed laptops. This includes smartphones and tablet computers.

1 - Policy

1.1 - Technical Requirements

1- Devices must use the following Operating Systems: Android 10 or later, IOS 12 or later.

2- Devices must have data encryption always enabled.

3- Devices must be configured with a secure PIN/password that complies with Eco Sourcing Hub Ltd ’s password policy. Where supported, devices should be secured using biometric security (e.g. Touch ID).

Except for those devices managed by IT, devices are not allowed to be connected directly to the internal company network.

1.2- User Requirements

1- Users must report all lost or stolen devices to Eco Sourcing Hub Ltd IT immediately.

2- If a user suspects that unauthorised access to company data has taken place via a mobile device they user must report the incident to The Company Director

3- Devices must not be “jailbroken”* or have any software/firmware installed which is designed to gain access to functionality not intended to be exposed to the user.

4- Users must not load pirated apps/software or illegal content onto their devices.

5- Applications must only be installed from official platform-owner approved app stores. Installation of code from un-trusted sources is forbidden. If you are unsure if an application is from an approved source, contact The Company Director.

6- Devices and all apps/software must be kept up to date with manufacturer-provided patches/updates.

7- Users should avoid the merging of personal and work email accounts on their devices. They must take particular care to ensure that company data is only sent through the company email system. If a user suspects that company data has been sent from a personal email account, either in the body of text or as an attachment, they must notify The Company Director immediately.

8- All new employees should read and acknowledge this policy.

Next Update 13/11/2024