Mobile Device Encryption Policy

Last updated: November 2023

1. Overview

Mobile devices such as smart phone and tablets offer great flexibility and improved productivity for employees. However, they can also create added risk and potential targets for data loss. As such, there use must be in alignment with appropriate standards and encryption technology should be used when possible.

2. Purpose

This document describes Information Security's requirements for encrypting data at rest on Cloudoko mobile devices.

3. Scope

This policy applies to any mobile device issued by Cloudoko or used for Cloudoko business which contains stored data owned by Cloudoko.

4. Policy

All mobile devices containing stored data owned by Cloudoko must use an approved method of encryption to protect data at rest. Mobile devices are defined to include laptops, PDAs, and cell phones.

Users are expressly forbidden from storing Cloudoko data on devices that are not issued by Cloudoko, such as storing Cloudoko email on a personal cell phone or PDA.

Laptops
Laptops must employ full disk encryption with an approved software encryption package. No Cloudoko data may exist on a laptop in plaintext.

T +44 (0)1904 500808 **| E** support@cloudoko.com **| www.cloudoko.com**

Cloudoko Ltd is registered in England & Wales under company number 09294405 **|** Registered office: 1 Derwent Business Centre, Clarke Street, Derby, DE1 2BU

PDAs and Cell Phones

Any Cloudoko data stored on a cell phone or PDA must be saved to an encrypted file system using Cloudoko-approved software. Cloudoko shall also employ remote wipe technology to remotely disable and delete any data stored on a Cloudoko PDA or cell phone which is reported lost or stolen.

Keys

All encryption keys and pass-phrases must meet complexity requirements described in Cloudoko's Password Protection Policy.

Loss and Theft

The loss or theft of any mobile device containing Cloudoko data must be reported immediately.

5. Policy Compliance

Compliance Measurement

The Infosec 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.

Exceptions

Any exception to the policy must be approved by the Infosec Team in advance.

Non-Compliance

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

6. Related Standards, Policies and Processes

- [Password Protection Policy](#)

T +44 (0)1904 500808 **| E** support@cloudoko.com **| www.cloudoko.com**

Cloudoko Ltd is registered in England & Wales under company number 09294405 **|** Registered office: 1 Derwent Business Centre, Clarke Street, Derby, DE1 2BU

7.   Definitions and Terms

The following definition and terms can be found in the Cloudoko Glossary.

- Plaintext
- Full Disk Encryption
- Remote Wipe

8.   Revision History

Date of Change	Responsible	Summary of Change
November 2023	Kevin Boldy	Initial Version

T +44 (0)1904 500808 **| E** support@cloudoko.com **| www.cloudoko.com**

Cloudoko Ltd is registered in England & Wales under company number 09294405 **|** Registered office: 1 Derwent Business Centre, Clarke Street, Derby, DE1 2BU

CLOUD OKO