Mobile Employee Endpoint Responsibility Policy

Last updated: November 2023

1. Overview

See Purpose.

2. Purpose

This document describes Information Security's requirements for employees of Cloudoko that work outside of an office setting.

3. Scope

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

4. Policy

All employees shall assist in protecting devices issued by Cloudoko or storing Cloudoko data. Mobile devices are defined to include desktop systems in a telework environment, 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.

5. Policy Compliance

Compliance Measurement

The Infosec team will verify compliance to this policy through various methods, including but not limited to, periodic walk-throughs, video monitoring, 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

None.

7. Definitions and Terms

None.

8. Revision History

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

CLOUDOKO

www.cloudoko.com