Mobile Device Encryption Policy

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 <Company Name> mobile devices.

3. Scope

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

4. Policy

All mobile devices containing stored data owned by Company_A 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 Company_A data on devices that are not issued by Company_A such as storing Company_A email on a personal cell phone or PDA.

4.1 Laptops

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

4.2 PDAs and Cell phones

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

4.3 Keys

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

4.4 Loss and Theft

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

5. Policy Compliance

5.1 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.

5.2 Exceptions

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

5.3 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

7 Definitions and Terms

The following definition and terms can be found in the SANS Glossary located at: https://www.sans.org/security-resources/glossary-of-terms/

- Plaintext
- Full Disk Encryption
- Remote Wipe

8 Revision History

Date of Change	Responsible	Summary of Change
Dec 2013	SANS Policy Team	Converted format and retired.