Mobile Device Encryption Policy

Created by or for the SANS Institute. Feel free to modify or use for your organization. If you have a policy to contribute, please send e-mail to stephen@sans.edu

1.0 Purpose
This document describes Information Security's requirements for encrypting data at rest on <Company Name> mobile devices.

2.0 Scope
This policy applies to any mobile device issued by <Company Name> or used for <Company Name> business which contains stored data owned by <Company Name>.

3.0 Policy
All mobile devices containing stored data owned by <Company Name> 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 Name> data on devices that are not issued by <Company Name>, such as storing <Company Name> email on a personal cell phone or PDA.

3.1 Laptops
Laptops must employ full disk encryption with an approved software encryption package. No <Company Name> data may exist on a laptop in cleartext.

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

3.3 Keys
All keys used for encryption and decryption must meet complexity requirements described in <Company Name>'s Password Protection Policy.

3.4 Loss and Theft
The loss or theft of any mobile device containing <Company Name> data must be reported immediately.

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

5.0 Definitions

Term	Definition
Cleartext	Unencrypted data
Full disk encryption	Technique that encrypts an entire hard drive, including operating system and data
Key	Phrase used to encrypt or decrypt data
PDA	Personal Data Assistant.

Remote wipe	Software that remotely deletes data stored on a mobile device.

6.0 Revision History
1.0 initial policy version, 2/22/2008