san diego county office of
EDUCATION
FUTURE WITHOUT BOUNDARIES™

Mobile Device Encryption Procedure

1. Purpose

This document describes Information Security's requirements for encrypting data at rest on San Diego County Office of Education (SDCOE) mobile devices.

2. Scope

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

3. Procedure

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

3.1 Laptops

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

3.2 PDAs and Cell phones

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

3.3 Encryption Keys

All keys used for encryption and decryption must meet complexity requirements described in SDCOE's Password Protection Policy.

3.4 Loss and Theft

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

4. Enforcement

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

5. 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. Revision History

Date of Change	Responsible	Summary of Change