



CALIFORNIA STATE UNIVERSITY, LONG BEACH

Subject: Electronic Data Security – Portable Devices and Removable Media	
Department: Information Security Management and Compliance	Reference No.:
Division: Administration and Finance	Issue Date: February 2009
References:	Revision Date: April 2009
Web Links: • Information Security Management and Compliance http://daf.csulb.edu/offices/vp/information_security	Expiration Date: N/A

I. Purpose

The purpose of this Standard is to establish requirements to provide for the protection of information stored on portable electronic storage media and portable computing devices.

II. Background

Portable computing devices (including, but not limited to, laptops computers, PDAs, tablet PCs) and portable electronic storage media (including but not limited to, CDs and USB storage devices) are vulnerable to loss or theft. In the event of loss or theft, information stored on these devices or media may result in identity theft or unauthorized access to secure systems, networks, and resources.

The University **Records Management Standard** requires that Confidential (Level 1) information stored on portable computing devices and portable electronic storage media be encrypted or otherwise rendered unreadable and unusable by unauthorized persons.

III. Scope

This Standard applies to:

- All University faculty, staff, students, and volunteers (collectively referred to as “employees”), contractors and consultants,
- All University owned portable computing devices and/or portable electronic storage media,
- All CSULB Auxiliary owned portable computing devices and/or portable electronic storage media containing University confidential or internal use data/information,
- All Confidential (Level 1) and Internal Use (Level 2) data/information.

IV. Portable Computing Devices

The following requirements apply to all University owned portable computing devices containing confidential or internal use data/information or any CSULB Auxiliary owned portable computing device containing University confidential or internal use data/information:

- a. Confidential (Level 1) information should not be stored on portable computing devices unless absolutely necessary and removed when the business reason for storage is no longer required. **Level 1 or Level 2 information may not be stored on non-university/auxiliary owned portable computing devices.**
- b. Physically secured when not in use.
- c. Encryption software must be loaded and correctly configured.
- d. Strong password protection rules for all user profiles.
- e. Operating system software must be kept current and antivirus software must be kept current on devices capable of running such software.

V. Portable Electronic Storage Media

The following requirements apply to all University/Auxiliary owned portable electronic storage media containing confidential or internal use data/information or any CSULB auxiliary owned portable electronic storage media containing University confidential or internal use data/information:

- a. Confidential (Level 1) information should not be stored on portable electronic storage media unless absolutely necessary and removed when the business reason for storage is no longer required. Method for removal is outlined in the [Records Management Standard](#). **Level 1 or Level 2 information may not be stored on personally owned portable electronic storage media.**
- b. All files must be encrypted.

VI. Disposal Requirements

All confidential or internal use information stored on portable computing devices or portable electronic storage media must be sanitized prior to disposal in accordance with the University Records Management Standard.

VII. Reporting Loss or Theft

The loss or theft of a portable computing device or portable electronic storage media within the scope of this standard must be reported to the employee's appropriate administrator, University Police and the office of Information Security Management and Compliance. If lost or stolen off-campus, local law enforcement must be notified and a police report obtained.

FURTHER INFORMATION

Information Security Management and Compliance
iso@csulb.edu.
(562) 985-4862