



CALIFORNIA STATE UNIVERSITY, LONG BEACH

Subject: Clean Desk and Clear Screen Standard	
Department: Information Security Management and Compliance	Reference No.:
Division: Administration and Finance	Issue Date: April 2008
References:	Revision Date: N/A
Web Links: • Information Security Management and Compliance	Expiration Date: N/A

I. PURPOSE

The purpose of this Standard is to set forth the requirements to ensure that all work areas are clear of university information, whether in electronic or paper form, classified as Level 1 – Confidential (Confidential) or Level 2 – Internal Use (Internal Use) when the work area is unattended.

II. SCOPE

This Standard applies to CSU Long Beach employees and CSU Auxiliary Organization employees who collect, generate, use or otherwise handle Confidential or Internal Use information.

III. DEFINITIONS

Level 1 – Confidential Information

Information that is exempt from disclosure under the provisions of the California Public Records Act or other applicable state or federal laws. Confidential information is information whose unauthorized use, access, disclosure acquisition, modification, loss, or deletion could result in severe damage to CSULB, its students, employees, or customers. Financial loss, damage to CSULB's reputation, and legal action could occur. Confidential information is intended solely for use within CSULB and limited to those with a "business need-to-know. Statutes, regulations, or other legal obligations or mandates protect much of this information. Disclosure of Confidential information to persons outside of the University is governed by specific standards and controls designed to protect the information. Examples of Confidential information are contained in the campus [Records Management Standard](#).

Level 2- Internal Use Information

Information which must be protected due to proprietary, ethical or privacy considerations. Although not specifically protected by statute, regulations, or other legal obligations or mandates, unauthorized use, access, disclosure, acquisition, modification, loss or deletion of information at this level could cause financial loss, damage to CSULB's reputation, violate an individual's privacy rights or legal action could occur. Examples of Internal Use information are contained in the campus [Records Management Standard](#).

IV. STANDARDS

- Users must "log off" their computers when their workspace is unattended.
- Users must "shut down" their computers at the end of the workday.
- All Confidential and Internal Use information must be removed from the desk and locked in a drawer or file cabinet when the workstation is unattended and at the end of the workday.
- All Confidential and Internal Use information must be stored in lockable drawers or cabinets.
- File cabinets containing Confidential or Internal Use information must be locked when not in use or when not attended.
- Keys used to access Confidential or Internal Use information must not be left at an unattended work area.
- Laptops must be either locked with a locking cable or locked away in a drawer or cabinet when the work area is unattended or at the end of the workday.
- Passwords must not be posted on or under a computer or in any other accessible location.

- Copies of documents containing Confidential or Internal Use information must be immediately removed from printers.
- Documents containing Confidential or Internal Use information must be immediately removed from facsimile machines.

FURTHER INFORMATION

Information Security Management and Compliance

iso@csulb.edu.

(562) 985-4862