8080.S01 Physical and Environmental Security

Implements: CSU Policy #8080.0
Policy Reference: http://www.calstate.edu/icsuam/sections/8000/8080.0.shtml

1.0 Introduction

Physical and environmental security controls prevent unauthorized physical access, damage, and interruption to campus' information assets. Campus controls must be adequate to protect critical or protected data. Such controls must:

a. Manage control of physical access to information assets (including personal computer systems, computer terminals, and mobile devices) by campus staff and outsiders.

b. Prevent, detect, suppress fire, water damage, and loss or disruption of operational capabilities due to electrical power fluctuations or failure.

2.0 Security Zones

Campuses must assign an appropriate security zone designation to their physical areas. Appropriate physical controls must be implemented in shared and limited access security zones to manage access. Campuses must review these controls regularly.

Zone	Brief Description	Necessary Controls
Public	No information assets containing protected data or critical systems are located in the area. (Example: Student Union, Library open areas)	None. Access to this area can be unrestricted.
Shared Access	An area containing one or more protected information assets or critical systems. Persons in the area include those who do not have authorization to protected information assets or critical systems stored in the area. (Example: Administrative Offices)	Appropriate physical access controls and construction must be implemented to restrict access to protected information assets or critical systems that reside in the area.
Campus Limited Access Area	An area containing one or more protected information assets or critical systems. Persons in the area are authorized to access the	Appropriate physical access controls and construction must be implemented that limit access to the area to only persons having a need for specific access in order to accomplish a legitimate task. The controls must enforce the principles of need to know and least possible privilege.

Zone	Brief Description	Necessary Controls
	protected information assets or critical systems. (Example: Data Center)	All physical access to such areas must be controlled by mechanisms such as tracking and logging. Access records must retain information such as: • Records identifying persons with keys (credentials, etc) • Where possible, systems must provide o Date and time of access o User ID performing access

3.0 Work Area Security

Campuses must establish and communicate user guidelines for securing protected data in work areas. This includes data in electronic and non-electronic form. The guidelines must address:

a. Ensuring that protected data is not left unattended.

b. Limiting the viewing of protected data from unauthorized users.

4.0 Viewing Controls

Information systems accessing protected data must not be left unattended or unsecured. Activation of automatic locking software or log off from the systems must occur when information systems are unattended.

The display screens for all campus information systems that have access to protected data must be positioned such that data cannot be readily viewed by unauthorized persons (e.g., through a window, by persons walking in a hallway, or by persons waiting in reception or public areas). If it is not possible to move a display screen to meet the above requirement, a screen filter must be used.

REVISION CONTROL

Revision History

Revision Date	Revised By	Summary of Revisions	Section(s) Revised
3/11/2011	Lisa Moske	Document Revision: Draft Standards Template	Click here to enter Revision Date
3/17/2011	Washington	Reformatted document. Updated the “Security Zones” and “Data Center Access” sections.	
3/22/2011	Washington	Replaced bullets with letters. Deleted “Data Center Access” section.	

Review / Approval History

Review Date	Reviewed By	Action (Reviewed, Recommended or Approved)
9/28/11	Washington	Approved