[Secure Spaces Physical Access Policy]
[Policy Number]

[Information Technology Services]

Applies to: [Faculty, staff, student employees, students, vendors, visitors, and volunteers, etc.]

Purpose of the Policy

The California State University Information Security Policy (Published at http://www.calstate.edu/icsuam/sections/8000/) section 8080 titled “Physical Security” states:
Each campus must identify physical areas that must be protected from unauthorized physical access. This policy supersedes EM:P11-11 HSU Data Center and Telecommunications Physical Access Policy

Definitions

Secure Space: A campus physical space for which all access needs to be explicitly authorized, and therefore cannot be accessed with a campus master key. Typically this is due to a legal or policy requirement to restrict the space, such as: storage of information assets, regulated medication, or criminal evidence. Such areas would include data centers, the University Police Department, Academic Personnel Services/Human Resources, the Health Center, and the President and Provost’s suites. Campuses must protect these limited-access areas from unauthorized physical access while ensuring that authorized users have appropriate access.

Formatted: Font: (Default) Arial, 11 pt, Font color: Black

Secure Space Steward: A designated MPP in the department assigned responsibility for a given Secure Space or their delegee.

Secure Space Review Group: Convened annually by the Information Security Officer and the campus Risk Manager with membership made up by the Secure Space Stewards. The Secure Space Review Group will review and update the list of campus Secure Spaces and their associated Stewards.

Policy Details

Physical access to secure spaces will be restricted to individuals with operational need for access. All personnel must have proper authorization to obtain access to these spaces requested by their supervisor and approved by the Steward of that space.

The Information Security Officer (ISO) will maintain a combined set procedures related to physical security and access to secure spaces. Each Secure Space Steward must approve changes to physical controls such as locks and alarm codes in their areas.

Prior to being granted any unrestricted or unescorted physical access, individuals must:

- Have a signed confidentiality agreement on file
- Complete a background check
- Complete training as defined by the Information Security Officer (ISO)

Compliance:

Unauthorized access to locations defined in this policy must be reported to University Police and the Information Security Office.

Violators of this policy are subject to disciplinary action up to and including dismissal from employment, expulsion from the University, and civil or criminal prosecution, as appropriate. Disciplinary action shall be conducted in accordance with applicable collective bargaining agreements or other appropriate University policies.

History *(required)*

Drafted:	08/31/2016 By: Information Security Office
Review:	10/26/2016 By: University Space and Facilities Advisory Committee:
Revised:	MM/DD/YYYY
Edited:	MM/DD/YYYY
Reviewed:	MM/DD/YYYY