Division Of TECHNOLOGY & INNOVATION
California State University CHANNEL ISLANDS

Process Number:	BP-03-003.03	**Effective Date:**	04/24/2013
Approved By:	A. Michael Berman VP for Technology & Innovation		**Page 1 of 4**

Business Practice for Physical Access to T&I Facilities

PURPOSE:

To assure the confidentiality, integrity, and availability of CSU Channel Islands information assets by controlling physical access to T&I facilities

BACKGROUND:

The University is required by CSU system-wide policy to protect its information assets. Physical security to sensitive or critical information systems must be limited to authorized persons to prevent theft or espionage. Additionally, access to workstations should also be physically secured to prevent unauthorized use, or theft, of workstations.

The Integrated CSU Administrative Manual, Section 8080.0, Physical Security, requires campuses to identify physical areas that must be protected from unauthorized access, and review and document physical access rights annually. This Business Practice is enacted to comply with that policy.

BUSINESS PRACTICE:

Accountability:

Manager, T&I Infrastructure
Information Security Officer

Applicability:

All persons with access to T&I computing facilities, including workstations

Definitions:

Text:

General

In order to ensure the confidentiality, integrity, and availability of the University's information assets, T&I will implement the following procedures.

Business Practice for Physical Access to T&I Facilities

Security Sensitive Areas
The Ojai Hall Data Center and all data closets are designated as security sensitive areas. Access to these spaces is permitted only by authorization of the Manager, T&I Infrastructure, and is restricted to those employees who have a demonstrated business need for such access.

Workstations, Laptops and Other Systems not in Security Sensitive Areas
Each person assigned a workstation, laptop, or other information system or asset must take adequate measures to physically secure that asset. "Adequate measures" includes locking the workstation to prevent theft, and locking the screen or logging out of the system when it is unattended. If the workstation's screen cannot be locked, or the workstation cannot be secured in such a way as to prevent theft, physical access to the room or space the workstation is located in must be secured.

Each person assigned a mobile device must take reasonable precautions to prevent the loss or theft of that device.

Employee authorization to access security sensitive areas
Each T&I employee desiring to access security sensitive areas must—

(1) Demonstrate and document a business need for the access privileges to the Manager, T&I Infrastructure,
(2) Complete Data Center Operations Training, and
(3) Complete an OPC Key Request endorsed by the VP for Technology & Innovation at the conclusion of their training.

Employees outside of the Division of Academic and Information Technology requesting access to security sensitive areas must—

(1) Demonstrate and document a business need for the access privileges to their Division executive or designee,
(2) Obtain the approval of their Division executive and the Manager, T&I Infrastructure,
(3) Complete Data Center Operations Training, and
(4) Complete an OPC Key Request endorsed by the VP for Technology & Innovation at the conclusion of their training.

Guest, Visitor, Vendor and Contractor Access to Computing Facilities
All guests, visitors, vendors and contractors accessing a security sensitive area identified by this business practice must—

Business Practice for Physical Access to T&I Facilities

(1) Have a legitimate business need for this access,
(2) Present to an authorized employee of T&I, and display upon request while in the security sensitive area, government- or employer-issued photo identification,
(3) Sign into and out of the security sensitive areas in the T&I Visitors Log. This log entry must include—
    a. The guest's sign-in and sign-out times,
    b. The name of the guest, and the name of the guest's employer, or the name of the guest's division and department or program for CI employees or guests,
    c. The name of the employee escorting the guest, and
    d. The reason for the visit.
(4) Be accompanied by an employee of T&I that is permitted to access the security sensitive area at all times.

Business Practice Violations
Violations of this business practice will result in the violator's access to security sensitive areas being immediately revoked until appropriate remediation is completed.

Reviewing Effectiveness
T&I will review the list of persons accessed to authorize security sensitive areas annually, and make adjustments to this business practice as required to maintain physical security.

Business Practice for Physical Access to T&I Facilities

Assessment Requirements

Assessment requirements and history are listed in the grid below.

Description	Frequency	Role Assigned	Date Completed
Review access list	Annual	Mgr. T&I Infrastructure	99/99/9999

Revision History

BP Nbr:	BP-03-003	**Enacted Date:**	04/24/2013		
Revision Nbr:	002	**Revision Date:**	08/17/2014	**Revised By:**	Neal Fisch
	003		02/02/2017		NFisch