Information Technology Physical Access Procedure

Office: Information Technology

Procedure Contact: Chief Information Officer

Revision History

Revision Number:	Change:	Date:
1.0	Initial version	**02/06/2012**
1.1	Format changes	**03/24/2014**

A. Purpose

This procedure defines the physical security access practices for the Information Technology Department of Southern Oregon University. This procedure applies to the network closets, telephone switch room, and data center facilities located on the Ashland Campus and the Higher Education Center on the Medford Campus. Effective implementation of this policy will minimize unauthorized access to these locations and provide more effective auditing of physical access controls.

B. Definitions

Data center: The physical location of all centrally managed servers and core networking equipment. There are two data centers, one located on the Ashland and Medford campuses. The Ashland campus data center is located in Computing Services Room 114. The Medford campus data center is located on the first floor of the Higher Education Center.

Switchroom: The physical location of the campus telephone PBX, Computing Services Room 112

Network closet: A location for physical networking equipment. There are typically one or two network closets per building, but there may be more depending on the size of the building.

C. Procedure

1. Ownership and Responsibilities

The Department of Information Technology is responsible for the safety and security of data on its network and the equipment used to run the network infrastructure.

2. Physical Access

Physical access to all IT restricted facilities must be documented and managed.
All IT facilities must be physically protected in proportion to the criticality or importance of their function at Southern Oregon University
Access to IT facilities will be granted only to the Southern Oregon University support personnel and contractors whose job responsibilities require access to that facility.
The process for granting card and/or key access to IT facilities must include the approval of the Chief Information Officer or the Network Services Manager.
Access cards/fobs and/or keys must not be shared or loaned to others.
Access cards/fobs and/or keys that are no longer required must be returned to Facilities Management and Planning. Cards must not be reallocated to another individual bypassing the return process.
Lost or stolen access cards and/or keys must be reported to Facilities Management and Planning.
Card access records and keys logs for IT facilities must be kept for routine review based upon the criticality of the resources being protected.
The Facilities Management and Planning department will remove the card and/or key access rights of individuals that change roles within the college or are separated from their relationship with Southern Oregon University.
Visitors must be escorted in access controlled areas of IT facilities.

IT must review card/fob and/or key access rights for the facility on a periodic basis and remove access for individuals that no longer require access.
Any use of IT facilities must have approval of the Chief Information Officer or the Network Services Manager.
Authorized personnel must have 24 hour unobstructed access to critical IT facilities.

D. Authorized Personnel
Access to the IT data center and switchroom are restricted to the Chief Information Officer, Network Services staff, and Network Services Manager only. Access for other individuals, including other IT staff, Facilities Management and Planning personnel, and Campus Public Safety officers is restricted on an as-necessary basis. No other personnel are permitted unaccompanied access to those facilities. Access to other IT facilities, including network closets, are restricted to select IT staff and select Facilities Management and Planning personnel on an as-needed basis.

This procedure may be revised at any time without notice. All revisions supersede prior procedures and are effective immediately upon approval.