Title:	Information Technology Facility Physical Access Procedure

Division:	Business and Finance	**Department:**	Information Technology
Procedure Contact:	Chief Information Officer		
Date Posted:	8/6/2018		
Related Policies or Procedures:			

History

Revision Number:	Change:	Date:
1.0	Initial version	6/22/2018

A. Purpose

This procedure defines the physical security access practices for Eastern Washington University Information Technology. This procedure applies to the network closets and data center facilities located on the Cheney and the Spokane campuses. 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 Cheney and Spokane campuses. The Cheney campus data center is located in Huston Hall. The Spokane campus data center is located in the Eastern Washington Center building .

Network closet - A location for physical networking equipment. There is 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 of 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. Visitors to the data center are required to sign in.

All IT facilities must be physically protected in proportion to the criticality or importance of their function at Eastern Washington University.

Access to IT facilities will be granted only to the EWU 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 Infrastructure Services Senior 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 the issuing office. Cards must not be reallocated to another individual, bypassing the return process.

Lost or stolen access cards and/or keys must be reported to the issuing office immediately.

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 issuing office will remove the card and/or key access rights of individuals that change roles within the college or are separated from their relationship with Eastern Washington 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 Infrastructure Services Senior Manager.

Authorized personnel must have 24 hour unobstructed access to critical IT facilities.

3. Authorized Personnel

Access to the IT data centers are restricted to the Chief Information Officer, Infrastructure Services Senior Manager, and authorized Infrastructure Services staff only. Access for other individuals, including other IT staff, Facilities and Planning staff, and Campus Police 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 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.

D. Other Information