Information Technology Security Plan
Physical Access Policy (10.12)

Responsible executive: CIO
Responsible office: ITS

Approval date: 7/01/2016
Effective date: 7/01/2016

Related policies: IT Security Plan

1.0 Policy Statement

Physical access security provides physical access controls and environmental safeguards to network infrastructure facilities. Physical access must be granted, managed and monitored to protect information technology resources from unauthorized access and environmental threats.

2.0 Reason for Policy

The purpose of this policy is to establish standards for granting, managing and monitoring physical access to university facilities containing network infrastructure to protect them from unauthorized access and environmental factors.

3.0 Applicability

This policy applies to all university facilities containing network infrastructure, including but not limited to the data center, network and telecommunication closets and fiber distribution facilities.

4.0 Policy

4.1 Physical Security

Physical access privileges to all university network facilities must be documented and managed by Information Technology Services (ITS).

All facilities that house network infrastructure must be physically protected in proportion to the importance of their function.

Access to restricted network facilities will be granted only to university staff and affiliates whose job responsibilities require access to that facility.

The process for granting card or key access to network facilities must include approval from ITS.

Secured access devices (e.g. access cards, keys, combinations, etc.) must not be shared with or loaned to others by authorized users.

Lost or stolen access cards or keys must be reported to Public Safety immediately.

Access rights to network facilities must remove when the access is no longer required.

University visitors and contractors must be escorted and monitored while in restricted network facilities.

A system of monitoring and auditing physical access must be implemented to review or investigate any unusual access on a periodic basis.

All facilities housing network infrastructure must be kept locked when not occupied by an authorized staff person.

All network and computing equipment, which resides in a public access area, must be secured with a theft-inhibiting device.

4.2 Environmental Controls

All physical access controls systems must comply with all regulations, including, but not limited to, building and fire prevention codes.

Fire detection, power irregularity protection, air conditioning, humidity control and other environmental protection systems must be installed, operative and maintained.

Adequate air conditioning must be operational network facility to prevent long-term heat damage and equipment failure.

All network equipment and systems in network facilities must be connected to an uninterrupted power supply in order to prevent power spikes, brownouts, and subsequent damage to data and Hardware.