

## **Physical Access Policy**

### **I. Purpose**

The purpose of this policy is to establish standards for securing data center, network closet, and Information Technology facilities. Effective implementation of this policy will minimize unauthorized access to these locations and provide more effective auditing of physical access controls.

### **II. Scope**

The policy applies to all closets and locations containing Department of Information Technology owned or operated equipment. This policy is specifically for the datacenter located in the Lindell Library and PBX Switchroom in Mortenson Hall, building distribution facilities, local distribution facilities, and wire closets.

### **III. Policy**

#### **A. 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.

#### **B. Physical Access**

- All physical security systems must comply with all applicable regulations such as, but not limited to, building codes and fire prevention codes.
- 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 Augsburg College
- Access to IT facilities will be granted only to the Augsburg College 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 Director of Information Technology Systems.
- Access cards and/or keys must not be shared or loaned to others.
- Access cards and/or keys that are no longer required must be returned to the Department of Public Safety. 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 Department of Public Safety.
- 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 Department of Public Safety will remove the card and/or key access rights of individuals that change roles within the college or are separated from their relationship with Augsburg College.
- Visitors must be escorted in access controlled areas of IT facilities.
- IT must review card and/or key access rights for the facility on a periodic basis and remove access for individuals that no longer require access.
- Signage for restricted access rooms and locations must be practical, yet minimal discernible evidence of the importance of the location should be displayed.
- Any use of IT facilities must have approval of the Director of Information Technology Systems.
- Authorized personnel must have 24 hour unobstructed access to critical IT facilities.

### **C. Authorized Personnel**

Access to the IT data center and switchroom are restricted to the IT System Administrators and Director of IT Systems only. Access for other individuals, including other IT staff, Facilities personnel, Spectrum Solutions staff, and Public Safety officers is restricted on an as-necessary basis and requires checkout of a key at the Department of Public Safety Dispatch Office. 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 personnel on an as-needed basis. With the exception of IT System Administrators and the Student Services Liaison, other staff requiring access to those facilities must check out a key at the Department of Public Safety Dispatch Office.

### **IV. Enforcement**

Anyone found to have violated this policy may be subject to appropriate disciplinary action.