

Information Security Policies  
**Physical and Environmental Security Policy**

Version: 1.0

Effective Date:

9-23-11

Approved by:

IT Advisory  
Committee

# **Physical and Environmental Security Policy**

## **1.0 Purpose**

The purpose of this policy is to enhance the physical and environmental security of Keuka College in order to create an environment that can withstand significant loss to infrastructure before suffering downtime on critical systems.

## **2.0 Scope**

This policy includes (but is not limited to) any buildings which contain a significant number of assets belonging to Information Technology Services (ITS) and any areas within buildings that contain a significant number of assets belonging to Information Technology Services (ITS).

### *Individuals affected:*

This policy applies to all Information Technology Services (ITS) staff, employees or contractors hereafter known as *Information Technology Services (ITS) Support Personnel*. ITS Support Personnel include, but are not limited to, all Information Technology Services (ITS) staff, contractors, auditors or others with administrative, environmental or physical access to Keuka College resources.

### *Resources covered:*

This policy applies to all college resources, whether individually controlled, shared, stand alone or networked. It applies to all computers and communications devices owned, leased, operated or provided by Keuka College. This includes, but is not limited to personal computers, wireless communication devices, networking devices, workstations, servers, and any peripheral devices and the associated software thereof. This policy also applies to all privately owned devices used to store, process or transmit college owned data. This policy applies to all physical locations where Keuka College resources are stored or used.

## **3.0 Policy**

### **Access Control/Monitoring**

#### *Video Surveillance*

Critical areas will have video surveillance monitoring all internal entrances and exits of the Server room and Network Operations Center (NOC).

### *Access control/ monitoring*

Access control methods should be implemented both the Server room and the Network Operations Center (NOC). Any area considered to be a critical area should have at a minimum one form of authentication and accounting such that it can be known at any time who entered what room at what time.

### *Automated notification*

Any unauthorized attempts at access to critical areas (using the authentication and accounting methodologies) should be immediately and automatically reported to the ITS Support Personnel responsible for that location by the authentication and accounting hardware or software.

## **Doors**

### *External Doors*

Any doors leading into a building where there are critical areas will implement at a minimum metal-based doors with industry standard high security locks.

### *Internal Doors*

All rooms leading into or out of critical areas shall implement at a minimum solid wood-core based doors with industry standard high security locks.

### *Windows*

Any critical areas where there are windows leading to the outside shall be closed and latched shut when nobody is in the room.

## **Wiring**

### *Exposed wiring*

Wiring not in a critical area shall be concealed in a manner appropriate to the venue. Permanent wiring exposed in hallways shall be concealed by drywall or other interior appropriate means.

### *Labeled wiring*

All permanent or semi-permanent wiring used in critical areas shall be labeled appropriately as to the purpose of the wire and/or where the wire should be plugged in.

### *Wire organization*

Wiring in critical areas shall be organized in a manner that is:

- Optimal for air flow of the connected systems
- Professionally appropriate in appearance
- Space efficient

## **Server Racks**

### *Loading of racks:*

All servers and other associated rack-mounted equipment shall be mounted starting from the top of the rack to the bottom of the rack. Furthermore, server racks shall be relatively equally loaded so that no one rack is full while others are almost empty.

This policy statement can be overridden at any time by any senior member Information Technology Services staff.

### *Locking:*

All server racks should have side panels (if available) attached and secured when not under repair or usual maintenance. All server racks will have their front and rear doors locked (if available) at all times except when equipment in said rack is under repair or usual maintenance.

Information Technology Services will not purchase any new server racks that do not comply with the above statement if the option for a rack with locks and side panels is reasonably available (to be defined by Senior Information Technology Services staff).

All keys for server racks and other equipment in the racks shall be stored in a secured lock box in the Information Services main office. The list of personnel who have access to this lock box will be specified by the Director of Information Technology Services (ITS).

## **Water**

### *Sensors:*

Water detection methods shall be implemented on both the ceiling and the floor of any location where there is infrastructure equipment owned, operated, or maintained by Keuka College. Furthermore, when said sensors detect an unacceptable amount of water as to present a hazard to the equipment in the room (said level to be determined by a subsequent standard); an automatic notification system will be activated which will alert the proper personnel to the situation (those persons also being defined in a subsequent standard).

### *Drainage:*

Water catch pans and other containment devices shall be use where ever there is a significant possibility for damage to equipment (as defined by a subsequent standard). At a minimum, water catch pans shall be placed on top of each server rack and be able to automatically drain to a no-maintenance repository (sump pump, plumbing drain, etc; i.e. not something that needs to be manually emptied).

## **4.0 Enforcement**

### *Compliance:*

At minimum these principles must be followed by individuals employed by Keuka College while attending to Keuka College resources. Individual departments or locations may apply stricter standards, provided they do not conflict with the standards and procedure outlined in this document.

## **5.0 - Definitions**

*Critical Areas* – Any room or space that is a wiring closet, has one or more server racks, contains significant (as designated by the Director of Information Technology Services (ITS)) resources, or is an office of ITS support personnel

*Information Services Support Personnel* – Any person who’s primary function is provide technical support to any realm of the infrastructure **OR** any person who has significant administrative access to any system or group of systems (“significant” is defined at the discretion of the Director of Information Technology Services)

*Access Control* – any method that physically secures an entry point into a room. Examples include (but are not limited to);

- door locks

- electronic locks using
  - biometrics
  - magnetic card swipe access
  - RFID based tokens
  - Number pad requiring a pin or access code

## **6.0 Revision History**

## **7.0 Policy Impact Statement**

This policy will require ITS Support Personnel to roll out some significant changes to the ITS infrastructure focusing on the areas of physical and environmental security. This will likely involve a multi-step process towards achieving compliance with this policy.