Data Center Hardening Standard

Purpose

This standard describes the physical security requirements and the authorization process by which personnel may obtain access to the IT@UC Data Center (Data Center) at the University of Cincinnati. Compliance with this standard is required for all departments that locate systems at the Data Center and for all personnel who visit the facility.

Scope

This standard applies to all Data Center facilities operated at the University of Cincinnati. Variations in the different buildings may result in slightly different operating procedures, depending on the building in question.

Audience

All students, faculty and staff with systems located at the Data Center as well as any visitors.

Physical Security Policy

Exterior Security
Only authorized personnel may access the facility via card-key (ID badge). Authorized personnel can access the center 24 hours per day, 7 days per week, 365 days per year.

Security Systems
Surveillance cameras must record all movements, 24 hours a day.

Server Cabinets
Server cabinets must be secured and may be shared by multiple departments. Access to server cabinets must be restricted to authorized personnel only. Actions within cabinets shared by multiple departments must be monitored by Data Center personnel to ensure that only the intended equipment is modified.
The physical structures that house IT equipment must be properly installed with no loose or moving components.

**Environmental Systems**
Automated software must closely monitor temperature and humidity as well as detect leaks of water flowing under a raised floor.

Fire detection and suppression must be achieved via Halon/dry pipe equipment.

Temporary power units must be in place to have extended time for shut down of servers in the event of a power outage.

**Electronic Access Control System and Alarms**
Access to all entry points into and within the Data Center must be controlled by electronic access control mechanisms that allow only authorized individuals to enter the facility.

**Deliveries**
Co-location customers must schedule/notify the facility manager of deliveries at least one business day in advance if possible, or as soon as they become aware of a pending delivery.

**Non-Disclosure**
As a condition of obtaining access to the facility, all UC faculty, staff, students and third-parties must agree by signature (electronic or otherwise) to not disclose information they may obtain about the facility except to those who are required to have the information to conduct legitimate university business.

**Cameras**
The Data Center must be under video recording and surveillance at all times.

**Food, drink, and tobacco products**
Food and drink are not allowed in the raised floor area or server build room. Tobacco products are prohibited in the facility.

**Photography/videography**
Taking of pictures and/or video, including by cell phones equipped with cameras, is prohibited.

**Authorized Access to UCIT Data Center**

**Provisioning process for authorized personnel**

University personnel who require access to the Data Center for the purpose of working on co-located systems must obtain authorization prior to accessing the facility. In order to be authorized, you must:
• Be a UC student, faculty or staff member.
• Must be a U.S. citizen or green card holder.
• Agree to abide by this security policy.

Requesters may also be required to review educational materials.

Data Center management must approve all access requests.

Physical access to the facility shall not be granted on an “emergency” basis to individuals who have not obtained authorization. In the event that an authorized staff member is not available, the manager from the requesting unit must provide written approval to the Data Center Manager prior to access being granted.

Access requests must be renewed annually to maintain approved access. Access permissions must be reviewed at least quarterly. Managers must notify the Data Center immediately when access is no longer required due to an employee’s termination or a change in job responsibilities.

Authorized personnel must be checked in when entering and checked out when exiting the Data Center.

Visitor Access to UCIT Data Center

All unauthorized personnel are considered visitors and must adhere to the Data Center Visitor Policy.

All visitors must be a U.S. citizen or green card holder.

All UC faculty, staff, students, and third-parties visiting the facility are required to present their UC ID cards or valid government-issued identification and will be checked into and out of the facility. Visitors to the Data Center must be admitted to the facility by Data Center staff and must be accompanied at all times. Visitors must be checked in when entering and checked out when exiting the Data Center.

Facilities Maintenance Personnel
Maintenance of equipment and the facility by UC staff and third parties is required. Maintenance may include but is not limited to general cleaning, raised floor space cleaning, and maintenance on electrical and mechanical systems. Maintenance visits by non-UCIT Data Center staff must be scheduled in advance and known by the facility Data Center Manager. Maintenance staff must be admitted to the facility by Data Center staff and must be accompanied at all times. Maintenance personnel must carry an approved identification credential and adhere to Data Center policies and procedures.
Vendors
Critical systems with 24-hour-a-day, 365-days-a-year support provided by a vendor must be identified in advance so Data Center personnel can provide necessary access to those vendor representatives. Data Center staff must be notified as soon as possible before a vendor support visit is planned. Vendor representatives must be admitted to the facility by Data Center staff and must be accompanied at all times.

Related links
Data Center Visitor Policy

Contact Information
IT@UC Office of Information Security  513-558-ISEC (4732) Email: infosec@uc.edu

History:
Issued: 12/15/2015
Revised: 3/21/2017