UCONN
UNIVERSITY OF CONNECTICUT

UITS Data Center Access Policies and Procedures

Revision 5:

2/15/2017

Author:
Len Sousa, UConn/UITS

Contents

UNIVERSITY OF CONNECTICUT

1. Introduction

The UITS Data Center provides specific environmental, enhanced security access, fire alarms/suppression, Uninterrupted Power Supplies (UPS), health system backbone connectivity, and a number of other elements required by the mission-critical resources that it houses. The procedures described in this document have been developed to maintain a secure Data Center environment and must be followed by people working in the Data Center. It is important that any department/group contemplating the installation of their servers in the Data Center fully understand and agree to these procedures.

2. Primary Guidelines

The Data Center is a restricted area requiring a much greater level of control than normal non-public spaces. Only those individuals who are expressly authorized to do so by the data center manager may enter this area. Access privileges will only be granted to individuals who have a legitimate business need to be in the data center.

3. Requesting Access to the Data Center

Department/Groups that have computer equipment in the Data Center may request access to the Data Center. The individuals designated by the requesting department/Group will be granted access once the Data Center manager authorizes them. To initiate authorization for access, the manager of the department/Group requesting access should direct a request through the UITS Web site http://uits.uconn.edu/ and select services at the top of the page. From the Services Page, choose Enterprise Infrastructure/Data Center and scroll to the data center section.

After completing the UITS Data Center Grant Badge Access request Form, and upon approval, the Data Center manager will add the person to the Authorization Access List and register the person in the security system, if appropriate for the access level granted. Before granting access read the UITS Data Center Access Policies and Procedure document and the “UITS Data Center Access Agreement” then e-signed and submit the agreement from the UITS web site.

When a person who has access to the Data Center terminates employment or transfers out of the department, a person’s department manager must complete the UITS Data Center Terminate Badge Access request Form from the UITS web site so that the person’s access to the Data Center can be removed.

4. Levels of Access to the Data Center

There are two levels of Access to the Data Center

a. Escorted

Escorted Access is closely monitored access given to people who have a legitimate business need for infrequent access to the Data Center. “Infrequent access” is generally defined as access required for less than 25 days per year. Individuals with Escorted Access will *not* be granted card access.

A person given Escorted Access to the area must sign in and out under the direct supervision of a person with Full Access, must provide positive identification upon demand, and must leave the area when requested to do so.

b. Electronic Card Access (One Card or Similar)

Full Access is given to people who have free access authority into the Data Center. Full Access is granted to the UITS core server, storage, network and data center technical staff whose job responsibilities require that they have access to the area. These individuals also have the authority to grant temporary access to the Data Center and to enable others to enter and leave the Data Center. People with Full Access are responsible for the security of the area, and for any individual that they allow into the Data Center.

5. Data Center Doors

All doors to the Data Center must remain locked at all times and may only be temporarily opened for periods not to exceed that minimally necessary in order to:

- Allow officially approved and logged entrance and exit of authorized individuals.
- Permit the transfer of supplies/equipment as directly supervised by a person with Full Access to the area.
- Prop open the door to the Data Center only if it is necessary to increase airflow into the Data Center in the case of air conditioning failure. In this case, staff personnel with Full Access must be present and limit access to the Data Center.

6. Physical Security

Proxy card access is required for access to the data center doors. If doors are open for more than 2 minutes an alarm will sound and automatically dispatch the UConn police department. The police department will respond to the call as a security breach to the data center.

Security cameras are present throughout the data center, including every isle and entrance way. Cameras are monitored in real-time. Additionally, they continually record and are available for playback when necessary (30-day retention).

Tenants will have a key assigned to each individual owner for opening their specific cabinet. Each key must be signed out. If someone attempts to gain entry into a cabinet without a key the DC manager will call an existing key owner to verify that the individual is authorized for entry. All tenant cabinets must be locked when exiting the area.

7. Periodic Review of Access

Periodic (at least annual) reviews will be performed of those with card access to the Data Center. The Data Center manager will perform these reviews. If an individual no longer requires Data Center access, it will be revoked. (Appendix B)

The results of periodic reviews will be reported to the CIO. The report will include an updated list of those allowed access to the Data Center.

8. Access Control Log

Proxy card logs are imported and maintained in the UITS log collection system.

The Data Center Access Control Log must be properly maintained at all times. The Log is maintained by the Data Center technical staff. All individuals with Full Access to the Data Center are responsible for maintaining this log. The following procedures must be followed:

- Each time an individual with Escorted Access to the Data Center is admitted to the area, he must properly log in on the Access Control Log at the time of entrance. The person admitting the visitor must countersign and fill out the appropriate section of the form.
- Each time an individual with Escorted Access to the Data Center leaves the area, he must properly log out on the Access Control Log at the time he leaves (even if only for a short time). The person with Full Access to the area who allows the visitor to leave must fill out the "Log Out" section of the Access Control Log.

9. Exception Report

All infractions of the Data Center Access Policies and Procedures shall be reported to the CIO.

Individuals with Full Access to the area are to monitor the area and remove any individual who appears to be compromising either the security of the area or its activities, or who is disrupting operation. It is particularly important that individuals with Full Access show initiative in monitoring and maintaining the security of the Data Center.

10. Escalation

The Data Center manager has overall responsibility for the administration of these policies and procedures. Issues the DC manager is unable to resolve will be escalated to the CIO.

11. General Data Center Operations Policies for Departments/Groups

a. Hosting Policy for Data Center Capacity Planning

UITS Data Center staff must be consulted for any new equipment to be installed in the Data Center. It is advisable to consult with UITS DC staff as early as possible (preferable months before actual equipment is ordered), to confirm your equipment actually can be hosted.

b. Policy on Infrastructure Work in the Data Center

ITS Data Center staff must be notified of all work pertaining to infrastructure in the Data Center. This includes things such as equipment installation/removal, construction or any activity that adds/removes assets to/from the Data Center.

Asset/inventory control must be maintained.

c. Cleanliness Policy

The Data Center must be kept as clean as possible. All individuals in the Data Center are expected to clean up after themselves. Boxes and trash need to be disposed of properly. Tools must be returned to their rightful place.

Food and drink are not allowed in the Data Center.

d. Equipment Deliveries/Pick-Up

Any department that is planning to have equipment delivered to or picked up from the Data Center should submit a request through the UITS web site under Data Center and installation requests.