

The security of the equipment and data in the University of Utah/UUHSC Data Center is of critical importance to the daily functioning of the University and the Hospital. The computer systems and data must be protected and remain reliable at all times.

This document is to communicate the policies and procedures by which access will be obtained and how individuals will conduct themselves within the Data Center.

1.0 Data Center Policies

1.1 Access to the Data Center

- All persons requesting access to the Data Center must have proper authorization.
- A Data Center authorization form must be on file for each person who is authorized to enter. This file will be maintained by Data Center staff.
- All persons must sign in when entering the Data Center to document the time and purpose of their visit. They must also sign out when leaving.
- All visitors to the Data Center will be accompanied at all times by authorized personnel.
- Visitors to the Data Center are to adhere to the visitors' guidelines as outlined in section 3.2 Visitor Guidelines below.
-

Note: The term "visitor" is defined as:

1. An employee who does not work in the Data Center;
2. An employee who does not possess Level I authorization to the Data Center;
3. An employee who does not possess Level II authorization to the Data Center.

2.0 Equipment in the Data Center

In order to enhance security and reduce the chance for disruptions, the following policies apply to all equipment housed in the Data Center.

- An equipment form must be completed for all equipment installations and removals. Equipment forms can be obtained online or by contacting the Data Center Manager.
- Data Center employees will deny access to anyone who intends to install, or remove equipment without an installation form on file.

2.1 Hardware/Software Maintenance & Upgrades of Production Equipment

- Level II authorized personnel may perform maintenance and or repairs of equipment on an as-needed basis between the hours of 7:00PM and 7:00 AM as approved by ITS Leadership Team.

3.0 Procedures

3.1 Access Authorization

The UUHSC Data Center is a consolidated server room intended to provide a 24x7 high availability, redundant, and secure environment for systems which need a high level of security. Intended uses include meeting HIPAA security requirements for servers, as well as other servers that need high availability and increased security. The Data Center design is intended to enable systems administrators of the servers housed in the Data Center to be able to effectively manage their machines remotely and securely. All personnel must have proper authorization to obtain access to the Data Center. There are two levels of authorization based on the type of access required. The first is Level I. Level I individuals will have assisted access to the data center 24 hours a day. They will not be assigned access cards. In order to enter the Data Center a Level I person will need to call and make arrangements to enter by contacting Data Center staff (most persons requesting access authorization will receive Level I access). Data Center staff is any person that reports directly to the Data Center Manager. The second is Level II. Level II individuals will have unassisted access to the Data Center 24 hours a day. They will not need to make arrangements to enter as they will have access cards assigned to them that will allow them to enter when needed.

The process to acquire authorization for each level is detailed below.

3.1.1 Level I Authorization

1. An authorization form must be completed by each employee requesting Level I access to the Data Center.
2. The director of the employee must sign the authorization form.
3. After director approval, the Data Center manager will then sign and file the authorization form.
4. The employee's name will then be added to the authorization list.
5. The employee will be authorized to enter the Data Center, but will not have bio scanner access. Data Center staff will validate employee authorization before allowing the employee to enter the Data Center.
6. The purpose of each visit must be documented. The employee must log in and out when entering and exiting the Data Center.

3.1.2 Level II Authorization

1. An employee requiring Level II access to the Data Center must complete authorization form.
2. The director of the employee must sign the authorization form.
3. After director approval, the Data Center manager will then sign and file the authorization form.
4. The employee's name will then be added to the authorization list.
5. The employee must present their current University id to obtain a bio scanner identification tag from the Data Center manager.
6. The employee will be given card reader access to the Data Center.
7. The purpose of each visit must be documented. The employee must log in and out when entering and exiting the Data Center.

3.2 Visitor Guidelines

Anyone who does not have Level I/Level II authorization is considered a visitor. All visitors to the Data Center must adhere to the following guidelines:

1. Visitors must log in and out when entering and exiting the Data Center. The purpose of the visit must be documented.
2. Visitors must be accompanied at all times by a Level II authorized employee while in the Data Center. All exceptions must have Data Center Manager approval.
3. To schedule visits call 801-587-6243. All visits to the Data Center should be scheduled through the Data Center Manager at least 24 hours in advance.

3.3 Audit Procedures

1. The Data Center Manager will send a list of authorized employees to each director on a quarterly basis (January, April, July and October) for review and verification.
2. The Directors will review and update the list of authorized employees and return it to the Data Center Manager within two weeks.

3.4 Equipment Installation

The Data Center is intended as a limited physical access location for servers. Systems administrators of machines which are housed in the Data Center should plan their servers as if they will only get physical access to them when it is necessary to perform hardware modifications or replacements. With this in mind, it is highly recommended that all servers be configured with secure access administrative tools to allow for remote maintenance. All machines in the Data Center must be rack mountable, unless prior arrangements have been made to allow particular non-rack-mountable hardware into the Data Center. Certain machines which have a business need to be in the Data Center and currently are not rack mountable should be replaced within a reasonably short time period of time with more appropriate hardware, or the machines' functions need to be relocated to other servers which are more appropriate for the Data Center.

Any employee intending to install equipment in the Data Center must submit an installation form. Installation forms are available from the Data Center manager or *online at future Data Center website*.

All new systems to the data center will need to undergo a security scan or audit prior to install. Also, while the Data Center provides increased network security, it is still necessary to take care of host-based security policies. Hosts in the Data Center will be regularly scanned for vulnerabilities and those reports provided to the appropriate personnel.

All new systems and hardware to the Data Center will need to be coordinated and scheduled with Data Center staff. As the number of machines in the Data Center grows, the infrastructure that supports the entire Data Center must incrementally expand. Sometimes this may mean a small delay in the deployment of hardware into the Data Center until we have the appropriate infrastructure (including console, network, power, and rack space) for the hardware to be deployed.

3.5 Equipment Removal

Any employee intending to remove equipment from the Data Center must submit a removal form. Removal forms are available from the Data Center manager or *online at future Data Center website*

4.0 Rules while in the Data Center

1. No food or drink is allowed within the Data Center
2. No Hazardous materials are allowed within the Data Center
3. All packing material must be removed from computer equipment/components in the specified staging areas before being moved into the Data Center. This includes cardboard, paper wrap, peanuts, plastic, wood and other such material
4. No cleaning supply is allowed within the Data Center without prior approval. This includes water
5. Only HEPA filter vacuums may be used inside the Data Center
6. No cutting of any material (pipes, floor tiles etc...) shall be performed inside the Data Center unless special arrangements are made
7. Boxes, tapes, CD's and other material shall not be stored inside the Data Center
8. ITS and OIT employees shall only access racks that contain equipment for which they are personally responsible
9. Only Data Center staff shall access the sub-floor or remove floor tile
10. ID must be worn above the waist and visible at all times
11. Communicate all problems to the Data Center staff
12. In the event of an emergency notify Data Center staff immediately