Southern Illinois University Carbondale
Information Technology
Wham Data Center Policies and Procedures

1.0 Introduction

The security of the equipment and data in the Wham Data Center is of critical importance to the daily functioning of the University. The computer systems and data must be protected and remain reliable at all times. This document is to communicate the policies and procedures concerning: access to the Data Center, the computing resources housed in the Data Center, and the conduct of individuals while in the Data Center.

2.0 Data Center Access Procedures

2.1 Access Authorization Levels

The Wham Data Center is a consolidated server room intended to provide a 24x7x365 high availability, secure environment for systems that need a high level of security. All personnel must have proper authorization to obtain access to the Data Center. There are several levels of authorization based on the access required. All individuals must be logged when entering/exiting the Data Center regardless of their level of authorization.

2.1.1 Level III Authorization

Level III authorization provides for unassisted, unescorted access to the Wham Data Center 24x7x365. Entry to the Data Center will be granted to access cards assigned to those individuals who have received Level III authorization. Level III staff members are the only individuals authorized to make infrastructure changes (network, cooling, power, etc.), add and/or remove equipment, or perform fixed asset audits (inventory) within the Data Center space.

Level III authorization is granted to:

- Data Center Manager
- Data Center staff members
- Data Center Technical Team – internal IT staff who are appointed to oversee the distribution of electrical power, network connectivity, cooling, and layout of the Data Center.

2.1.2 Level II Authorization

Level II authorization provides for unassisted, unescorted access to the Wham Data Center 24x7x365. Entry to the Data Center will be granted to access cards assigned to those individuals who have received Level II authorization.

Level II authorization is granted to:

- Full time SIUC Information Technology (IT) employees who have primary responsibilities for the physical maintenance and repair of critical services equipment housed in the Data Center.
- Level II staff members are not authorized to make any changes, modifications, and/or decisions regarding the Data Center space without explicit approval of the Data Center Manager or other Level III staff members.

2.1.3 Level I Authorization

Level I authorization grants escorted assistance to the Data Center during normal weekday business hours (8:00am-4:00pm). Access during non-business hours will be granted on a case-by-case basis. In the event of an after-hours emergency that cannot wait until the next business day, emergency access to the Data Center can be arranged by contacting the Data Center Manager or appointed Data Center staff. Entry to the Data Center will not be granted to access cards assigned to those individuals who have received Level I authorization. Level I authorized personnel must be escorted at all times by Level II authorized or higher personnel, unless an exception has been granted by the Data Center Manager.

Level I authorization is granted to:

- Carbondale Campus employees who contract with Information Technology to provide a secure location for their equipment and need occasional direct access to perform physical maintenance and/or repair functions.
- Part time IT employees (students, GAs, etc.) who assist Level II/III staff with the physical maintenance and repair of critical service equipment housed in the Data Center.

If an emergency situation requiring physical access to equipment in the Data Center occurs on a Holiday or day of Administrative Closure, arrangements will be in place to provide Level I authorized individual's physical access to the Data Center. For security purposes these arrangements will not be published in this document. Level I authorized individuals will receive instructions for Holiday/Administrative Closure access from the Data Center Manager or other authorized Data Center staff member.

2.1.4 Authorized Internal Vendor

Authorized Internal Vendors are all University employees who, through a contractual arrangement and appropriate approvals, have access to the Data Center. These employees may or may not be granted security card access. Access level will be determined on a case-by-case basis.

- Authorized Internal Vendors may include, but are not limited to:
  - Telecommunications staff
  - Physical plant staff (electricians, plumbers, etc…)
  - Building services staff

2.1.5 Authorized External Vendor

Authorized External Vendors are all non-University individuals who, through a contractual arrangement with appropriate approval, have access to the Data Center. External Vendors must be escorted at all times by Level II or higher authorized staff.

2.1.6 Visitors

Visitors are individuals who do not have Level III/II/I or a Vendor Level authorization. This may include IT employees (part time and/or full time) who do not have direct responsibility for the maintenance and repair of equipment housed in the Data Center. All visitors to the Data Center must adhere to the following guidelines:

- Visitors must be logged in and out when entering and exiting the Data Center. The purpose of the visit must be documented.
- Visitors must be accompanied at all times by a Level II, or higher, authorized employee while in the Data Center. All exceptions must have Data Center Manager approval.
- All visits to the Data Center should be scheduled though the Data Center Manager at least 24 hours in advance.
- IT employees wishing to enter the Data Center must be accompanied by a Level II or higher authorized employee. No advance notice is required.
- Tour groups are considered visitors to the Data Center, and any visit must be arranged at least 24 hours in advance, and be approved by the Data Center Manager. Tour groups are limited to 20 or fewer individuals at one time.

2.2 Access Authorization Request

2.2.1 Employee Access

The process for IT and other Carbondale campus employees to obtain Data Center authorization is detailed below.

- The Authorized Access Request form must be completed by each employee requesting access to the Wham Data Center.
- The completed form is forwarded to the employee's director or department head for approval.
- The approved form is forwarded to the Data Center Manager for processing. The Facility Manager reserves the right to reject or downgrade any access level request.
- The employee's name is added to the authorization list.
- The employee will be authorized to enter the Data Center under the guidelines set for the authorization level assigned to that employee.
- The purpose of each visit must be documented. The employee must be logged in and out when entering and exiting the Data Center.

2.2.2 Vendor Access

The process for Internal and External Vendors to obtain Data Center authorization will be dealt with on a case-by-case basis by the Data Center Manager.

2.3 Audit Procedures

- 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.
- The Directors will review and update the list of authorized employees and return it to the Data Center Manager within two weeks.
- Failure to return access audits will result in the revocation of access privileges for previously authorized staff/vendors until such time as the audit is returned.

3.0 Data Center Policy

The following information is pertinent to the placement of equipment in the Data Center and the conduct of those who enter the Data Center.

In an effort to maximize security, minimize disruption, and provide a secure and stable environment for all of the equipment in the Data Center, the following policies apply to all of the equipment housed in the Data Center.

3.1 Equipment in the Data Center

The Data Center is intended as a limited physical access location for computer systems. Individuals who administer equipment that is housed in the Data Center should plan to have physical access to their systems to perform hardware modification, repair, or replacement only. With this in mind, all servers should be configured with secure access administrative tools to allow for as much remote administration as possible. Only if such tools are not available or feasible, will physical access to the Data Center be allowed.

3.1.1 Equipment Installation

- The Equipment Installation Form must be completed for all equipment to be placed in the Data Center. Data Center staff will deny entry to authorized staff or vendors who intend to install or change equipment without a properly completed form.
- Equipment housed in the Data Center must meet certain system specifications. These include:
    - All new equipment must be rack mountable unless prior arrangements have been made to allow a particular non rack-mountable piece of equipment into the room.
    - Equipment that has a business need to be in the room and is currently not rack mountable should be replaced with rack mountable units. If this is not possible, the functions the equipment provides should be relocated to hardware more appropriate for the Data Center.
    - All equipment should contain dual power supplies (redundant), unless an exception is made by the Data Center Manager.
    - All rack mounted power distribution units must be connected to the Data Center UPS backed power grid, and must provide remote monitoring capability to the Data Center Manager and monitoring systems.
    - No stand-alone or rack mount UPS units will be allowed.
- Placement of new systems and hardware in the Data Center must be coordinated with the Data Center Manager and/or Data Center Technical Team.
- As the number of systems housed in the Data Center grows, the infrastructure that supports the Data Center must be expanded. This may mean a delay in the deployment of hardware into the Data Center until the appropriate infrastructure (including console, network, power and rack space) is in place.

3.1.2 Equipment Removal

- The Equipment Removal Form must be completed for all equipment to be removed from the Data Center. Data Center staff will deny entry to authorized staff or vendors who intend to remove equipment without a properly completed form.

3.2 Conduct in the Data Center

In order to ensure that the systems housed within the Data Center are kept secure, the following policies apply to all personnel requiring access:

- All personnel who access the Data Center must have proper authorization. Individuals without proper authorization will be considered a visitor and may be denied access at any time for any reason.
- All authorized personnel must be logged in and out when visiting the Data Center to document the time and purpose of their visit.
- Authorized personnel shall only access equipment for which they are responsible. If any person accesses equipment for which they are not responsible, their Data Center access privileges may be downgraded or revoked.
- Only members of the Data Center Technical Team shall access the sub-floor or remove a floor tile.
- All authorized personnel must enter through the Data Center main entrance. The back entrance/exit may only be used by Data Center staff whose work assignment is in the Data Center.
- Visitors to the Data Center must adhere to the visitor guidelines (see section 2.1.6)
- All authorized personnel and visitors must carry a valid University ID, vendor identification badge, or State-issued ID at all times. You may be asked to produce this ID at any time.
- Food and drink are not allowed in the Data Center. For Data Center staff whose work assignment is in the Data Center, food and drink are confined to designated break areas.
- No hazardous materials are allowed within the Data Center.
- No cleaning supplies or any other liquid are allowed within the Data Center without prior approval.
- No cutting of any material (pipes, floor tiles, etc…) shall be performed inside the Data Center unless special arrangements are made.
- All packing material must be removed from computer equipment/components in the designated staging areas before being moved into the server area.
- Communicate all problems to the Data Center staff, Data Center Manager, or to the Data Center Technical Team.
- In the event of an emergency contact the Data Center staff immediately.