ILLINOIS

UNIVERSITY OF ILLINOIS AT URBANA-CHAMPAIGN

Technology Services Data Center

Document Title: Technology Services Data Center Access Policies and Procedures

Intended Audience: General personnel Technology Services Data Center Access

Summary

Security for the Data Center is the Responsibility of the Technology Services Data Center. The TSDC Operations Manager is responsible for the administration of this policy. The following are the general requirements, policies and practices that govern access to this sensitive area, for which the TSDC Manager has responsibility. It is important that all University I.T. professionals and business associates follow these policies and practices.

General Data Center Safety Guideline

The data center is equipped with fire detection and fire suppression systems. The system was implemented to protect the equipment in the data center in the event of fire. If an alert is activated, it is imperative that everyone exit the data center and leave the building immediately. **Once the third level alert is activated, the system will release the water in 30 seconds at ACB. At DCL and HAB once the second level alert is activated, the system will release a chemical agent that is deadly to humans in 30 seconds.** The room will be filled with water or chemical agent which will extinguish any fire. The training for "**Fire Suppression System**" will be required for all personnel with TSDC access.

ILLINOIS

UNIVERSITY OF ILLINOIS AT URBANA-CHAMPAIGN

Technology Services Data Center

Data Center Access Policies and Procedures

1. **Introduction**

The procedures described in this document have been developed to maintain a secure Data Center environment, personnel safety is paramount, and safety procedures must be followed by everyone 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. **Data Center Physical Security Policy and Procedure.**

A. **Overview**

Security for the Data Center is the Responsibility of the Technology Services Data Center Team. The TSDC Operations Manager is responsible for the administration of this policy. The following are the general requirements, policies and practices that govern access to this sensitive area, for which the TSDC Manager has responsibility. It is important that all University I.T. professionals and business associates follow these policies and practices. Failure to do so is considered grounds for personnel action, including loss of access to the data center.

B. Primary Guidelines

The **"Data Center"** is a restricted area that requires a much greater level of access control than normal non-public foundation spaces. Only those individuals who are expressly authorized may enter this area. Access privileges will be granted to individuals with a legitimate business case upon completion of the "**Fire Suppression System**" training. Upon completion of training, the individual will receive access. Furthermore, this area may only be entered to conduct authorized business or work.

Any questions regarding policies and procedures should be

addressed to the TSDC Operations Manager.
The only exception allowed to the Data Center Security Policies and Practices is temporary suspension of these rules if it becomes necessary to provide emergency access to medical, fire and/or police officials, etc.

C. Levels of Access to the Data Center

There are two "Levels of Access" to the Data Center – General Access, and Escorted Access.

C1**. General Access** is given to the data center team and clients who have free access authority into the Data Center. If a person with General Access provides escorted access to an individual, the person granting access is solely responsible for escorting this individual and seeing to it the protocol is followed.

C2**. 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 15 days per year. Auditors and individuals with Escorted Access will not be issued ICARD access.

A person given Escorted Access to the area must sign in and out under the direct supervision of a person with General Access, must provide positive identification upon demand, and must leave the area when requested to do so.
The grantor is responsible for these individuals and must always escort them in the Data Center.
C4. **Data Center Tours** require approval by the Data Center manager scheduled one week prior to the tour. Visitors will be signed in and escorted by Data Center staff during the tour of the Data Center. Photographic and video recording devices are allowed in the Data Center during the tour.

D. **Data Center Door**

All doors to the Data Center must always remain locked and may only be temporarily opened for short periods 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 General Access to the area.

- Prop open a door to the Data Center **ONLY** if it is necessary to increase airflow into the Data Center in the event of air conditioning failure. In this case, staff personnel with General Access must be present and limit access to the Data Center.

E. Exception Reporting

All infractions of the Data Center Physical Security Policies and Procedures shall be reported to the TSDC Manager. If warranted (e.g.: emergency, imminent danger, etc.) the campus police should be notified as soon as is reasonably possible.

If an unauthorized individual is found in the Data Center it must be reported immediately to a member of, or Manager of, the TSDC Team. If this occurs during the evening hours or the weekend, the TSDC Manager should be contacted immediately. He or she will determine if the campus police should be contacted.

The unauthorized individual should be escorted from the Data Center and a full written report should be immediately submitted to the TDC Manager.

Individuals with General 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 operations. It is particularly important that personnel with General Access should uphold the Policies and Procedures to ensure the security of the TSDC.

F. **Requesting Access to the Data Center**

Departments/units that have computer equipment in the Data Center may request access to the Data Center. Individual members of Departments/units must request this access, via TDX ticketing system.

forms. General Access is valid until expiration of ICARD, leaving the Department/unit or Removal for cause of issuance upon approval by the TSDC Manager.

When a person who has access to the Data Center terminates his employment or transfer out of the department, a person's department manager must notify the TSDC Manager as soon as possible so that the person's access to the Data Center can be removed immediately. This is extremely important in cases where the employee was terminated for cause.

F. General Data Center Operations Policies for Departments/Projects

1. General Hosting Policy for the Data Center Capacity Planning

The TSDC Team must be consulted regarding equipment installation in the Data Center. It is advisable to consult with the TSDC Team as early as possible (preferably one or two months before the actual equipment is ordered), to confirm your equipment can be hosted.

2. General Policy on Infrastructure Work in The Data Center

The TSDC Team must be notified of all work pertaining to infrastructure in the Data Center. This includes equipment installation/removal, construction, or any activity that adds/removes assets to/from the Data Center.

3. Visitor Logs

Each Technology Services Data Center has its own visitor log sign in sheet. The TSDC Manager will collect the visitor log once a month. This log will be reviewed with the calendar of events and access log from continuum and then scanned into box.

4. **General Safety**

All individuals in the TSDC must conduct their work in observance with all applicable (i, e: bargaining unit, campus, state, federal) policies related to safety.

5. **General Cleanliness Policy**

The TSDC 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.

6. **Policies For Data Center Equipment Deliveries/Pick-Up**

Any department planning to have equipment delivered to or picked up from the TSDC should contact the Data Center Team and provide details in advance of delivery/pick-up using the TDX ticketing system:

For the delivery of equipment:

Expected day of delivery
PAS number for the equipment (if known)
Vendor name and description of the equipment.
Person to be contacted when the equipment arrives.

For the pick-up of equipment:

Expected day the equipment will be picked up.

Vendor name and the description and location of the equipment to be picked up.
Name of the person to be notified once equipment is picked up.