

Data Center Access Policies and Procedures

1. Introduction

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/project 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 Foundation IT Department. The Foundation IT Director is responsible for the administration for this policy. The following are the general requirements, policies and practices that govern access to this sensitive area, for which the Foundation IT has responsibility. It is important that all Foundation staff, University staff, and business associates follow these policies and practices. Failure to do so is considered grounds for personnel action.

B. Primary Guidelines

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

Any questions regarding policies and procedures should be addressed with the Foundation IT Director.

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 2 “Levels of Access” to the Data Center – General Access and Escorted Access.

C1. **General Access** is given to people who have free access authority into the Data Center. General Access is granted to the Foundation IT staff whose job responsibilities require that they have access to the area. Individuals are issued key cards providing logged access through the data center door.

Individuals with General access to the area may allow properly authorized individuals escorted access to the data center.

If a person with General Access allows Escorted access to an individual the person granting access is responsible for logging and escorting the individual granted access and seeing to it that 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. Individuals with Escorted Access will *not* be issued a door key card to access the data center with.

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.

D. Data Center Door

The door 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 General 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 on an 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 Foundation IT. If warranted (e.g.: emergency, imminent danger, etc.) the campus police should be notified as soon as is reasonably possible. When an unauthorized individual is found in the Data Center it must be reported immediately to a member of the Foundation IT Team. If this occurs during the evening hours, the Foundation IT Director or an IS Analyst should be contacted. They 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 Foundation IT Director.

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 operation. It is particularly important that individuals with *General Access* show initiative in monitoring and maintaining the security of the Data Center.

F. Requesting Access to the Data Center

Departments/projects that have computer equipment in the Data Center may request access to the Data Center. The individuals designated by the requesting department/project will be granted access once the Foundation IT Director authorizes them.

Upon approval by the Foundation IT Director, the IT staff will set up an appointment with the person requesting access in order to provide the person with a copy of the Foundation IT Data Center Access Policies.

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

3. General Data Center Operations Policies For Departments/Projects

A. General Hosting Policy for Data Center Capacity Planning

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

B. General Policy on Infrastructure Work In the Data Center

Foundation IT 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.

C. General Safety Policy

All individuals in the Data Center must conduct their work in observance with all applicable (e.g.: campus, state, federal) policies related to safety.

D. General 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 replaced to their rightful place.

Food and drink are not allowed in the Data Center.

E. Policies for Data Center Equipment Deliveries/Pick-Up

Any department that is *planning* to have equipment delivered to or picked up from the Data Center should contact Foundation IT and provide details to the group in advance of delivery/pick-up. Please provide Foundation IT with the following information for the equipment log:

For the delivery of equipment:

- Expected day of delivery
- P.O. 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 person to be notified once equipment is picked up