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 MIS Department. The Foundation MIS Manager 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 MIS has responsibility. It is important that all University faculty, 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 individual who are expressly authorized to do so may enter this area. Access privileges will be grated 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 MIS 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 3 “Levels of Access” to the Data Center – General Access, Limited 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 MIS staff whose job responsibilities require that they have access to the area. Individuals with Limited access will be granted a different key combination for 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 escorting the individual granted access and seeing to it they 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 combination 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.
Individuals allowed Escorted Access will be placed on the ITS Operations.

C3. **Limited Access** is granted to a person who does not qualify for General Access but has a legitimate business reason for unsupervised access to the Data Center.

Unescorted Access personnel cannot authorize others to be granted unsupervised access to the Data Center. Unescorted access personnel can only grant escorted access to individuals where related to the grantor’s business in the Data Center.
The grantor is responsible for these individuals and must escort them in the Data Center at all times
Students who are given Limited Access may NOT escort anyone into the Data Center without approval from personnel with Foundation MIS.

D. Data Center Door

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 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 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 MIS. 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 MIS Team. If this occurs during the evening hours, a Senior Operator or the Operations Manager 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 MIS 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 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 MIS Manager authorizes them.

Upon approval by the Foundation MIS Manager, the MIS staff will set up an appointment with the person requesting access in order to provide the person with a copy of the Foundation MIS 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 MIS Manager 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

1. General Hosting Policy For Data Center Capacity Planning
ITS Operations must be consulted for any new equipment to be installed in the Data Center. It is advisable to consult with ITS Operations as early as possible (preferably months before actual equipment is ordered), to confirm your equipment actually can be hosted.

2. General Policy On Infrastructure Work In The Data Center
ITS Operations 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.

3. General Safety Policy
All individuals in the Data Center must conduct their work in observance with all applicable (ie: bargaining unit, campus, state, federal) policies related to safety.

4. 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.

5. 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 ITS Operations and provide details to ITS Operations in advance of delivery/pick-up. Please provide ITS Operations 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