**IT DATA CENTER ACCESS POLICY & PROCEDURES**

**TABLE OF CONTENTS**

[**1. INTRODUCTION** 2](#_Toc123017520)

[**2. OVERVIEW** 3](#_Toc123017521)

[**3. PRIMARY GUIDELINES** 3](#_Toc123017522)

[3.1 Levels of Access to the Data Center 3](#_Toc123017523)

[3.2 Data Center Door 4](#_Toc123017524)

[**3.3 Exception Reporting** 5](#_Toc123017525)

[3.4 Requesting Access to the Data Center 5](#_Toc123017526)

[**4. DATA CENTER OPERATIONS POLICIES FOR DEPARTMENTS/PROJECTS** 5](#_Toc123017527)

[**4.1 General Hosting Policy for Data Center Capacity Planning** 5](#_Toc123017528)

[**4.2 General Policy On Infrastructure Work In The Data Center** 6](#_Toc123017529)

[**4.3 General Safety Policy** 6](#_Toc123017530)

[**4.3 General Cleanliness Policy** 6](#_Toc123017531)

[**5. POLICY COMPLIANCE** 6](#_Toc123017532)

[**5.1 Policy Compliance** 6](#_Toc123017533)

[**5.2 Exceptions** 6](#_Toc123017534)

[**5.3 Non-Compliance** 6](#_Toc123017535)

**1. INTRODUCTION**

The procedures described in this document have been developed to maintain a secure Data Center environment and must be followed by Data Center personnel. 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. OVERVIEW**

Security for the Data Center is the Responsibility of the Information Technology Department. The Security and Identity Management Engineer 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 Information Technology Department 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.

**3. PRIMARY GUIDELINES**

The “Data Center” is a restricted area which required a greater level of control than normal non-public 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 University business.

Any questions regarding policies and procedures should be addressed with the Security and Identity Management Engineer.

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.

3.1 Levels of Access to the Data Center

There are 3 “Levels of Access” to the Data Center:

* General Access
* Limited access
* Escorted Access

3.1.1.  General Access

General Access is given to people who have free access authority into the Data Center. General Access is granted to the Information Technology staff whose job responsibilities require that they have access to the area.

Individuals who are granted general access may access the Information Technology data center and disaster recovery areas via key access.  Key access is granted by property control after appropriate permission is granted by either the CIO or Security and Identity Management Engineer.

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 ensuring the protocol is followed.

3.1.2.  Escorted Access

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 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.

3.1.3.  Limited Access

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.

3.2 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 of an air conditioning failure. In this case, staff personnel with General Access must be present and limit access to the Data Center.

**3.3 Exception Reporting**

All infractions of the Data Center Physical Security Policies and Procedures shall be reported. 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 Information Technology Team. If this occurs during the evening hours, Senior Management 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 Information Technology Management.

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.

3.4 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 CIO or  Security and Identity Management engineer authorizes them.

Upon approval by the, the Information Technology staff will set up an appointment with the person requesting access in order to provide the person with a copy of the Information Technology 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 Security and Identity Management Engineer 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.

**4. DATA CENTER OPERATIONS POLICIES FOR DEPARTMENTS/PROJECTS**

**4.1 General Hosting Policy for Data Center Capacity Planning**

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

**4.2 General Policy On Infrastructure Work In The Data Center**

Information Technology 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.

**4.3 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.

**4.3 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 drinks are not allowed in the Data Center.

**5. POLICY COMPLIANCE**

**5.1 Policy Compliance**

The Information Technology team will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, video surveillance, and feedback to the policy owner.

**5.2 Exceptions**

Any exception to the policy must be approved by the Information Technology CIO and security team in advance.

**5.3 Non-Compliance**

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.   In addition to University discipline, users may be subject to criminal prosecution under federal, state or local laws; civil liability;  or both for unlawful use of any IT System.