Data Center Access
Campus Policy 835.0
Information Technology

I. Purpose and Scope

The procedures described in this document have been developed to maintain a secure Data Center (server room, data storage systems, et cetera) environment and must be followed by people working in the data center. Security for the data center is the responsibility of the Information Services department. The Director of Information Services is responsible for the administration of this policy. The following are the general requirements, policies, and practices that govern access to this sensitive area. It is important that all employees and vendors follow these policies and practices. Failure to comply with this policy is grounds for personnel action.

II. Definitions

Data Center: Commonly referred to as the "server room". The data center is a climate-controlled and physically secured room that contains many servers and networking resources that are critical for UACCB campus operations.

III. Policy

The Data Center is a restricted area that requires a much greater level of control than non-normal public spaces. Only those individuals who are 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 Director of Information Services.

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.

The Information Services team will verify compliance to this policy through regular audits of the log sheet and video surveillance.

a. Levels of Access to the Data Center

There are 3 "Levels of Access" to the Data Center:

1. General Access
2. Limited access
3. Escorted Access

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 Services staff whose job responsibilities require that they have access to the area. Individuals who are granted general access may access the Information Services data center and disaster recovery areas via key access. Key access is granted by the Director of Information Services.

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 that the protocol is followed.

2. 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 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. 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.

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.

b. Data Center Door
The door to the Data Center is under continuous video surveillance and must remain locked at all times and may only be temporarily opened for periods not to exceed the minimal time 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, authorized staff with General Access must be present and limit access to the Data Center.

c. Exception Reporting
All infractions of the Data Center Access Procedures shall be reported. If warranted (e.g.: emergency, imminent danger, etc.) the safety officers 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 Services Team. If this occurs during the evening hours, Senior Management should be contacted. They will determine if the safety department or police department should be contacted.
The unauthorized individual should be escorted from the Data Center and a full written report should be immediately submitted to the Director of Information Services.
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.

IV. Enforcement

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

V. Related Information

Continuous improvement. The content of this document is subject to regular review based on input from UACCB Information Services staff and the campus community. Suggestions for improvement should be directed to the Director of Information Services.

VI. Revision History

Effective Date:
Revised Date:
Reviewed Date: