CU Denver-Anschutz Medical OIT DC Access and Physical Security Policy

Purpose: The purpose of this document is to serve as a guiding set of policies and procedures for physical access to the the CU Denver | Anschutz Medical Center Data Center environments.

Document Type: Policy

Principal Author: Steve Stelzer

Access Type: Public

Effective: February 1st, 2017

Approved by: Sheard Goodwin, Director of Operations, OIT

Responsible Office: Office of Information Technology

Policy Contact: Sean Clark, Information Security Officer

Supersedes: 1/31/2017

Last Reviewed/Updated: November 10th ,2021

Applies to: University of Colorado Denver | Anschutz Medical Campus

Introduction

The University of Colorado Denver | Anschutz Medical Center (the University) strives to provide stable and secure environments for housing servers and related components which store and manage university data. This document establishes guidelines for access and physical security related to Office of Information Technology (OIT) university data centers, regardless of size or location.

Scope

This policy applies to all OIT data centers on both campuses.
This policy is intended to:

- Ensure access is controlled to protect both the physical resources and university data from unauthorized use, accidental or malicious damage, and theft
- Define appropriate levels of access (LOAs) based on demonstrated business need
- Improve stability and security of systems which store and manage university data
- Support the university's strategy to incorporate information technology as an integral part of decision-making, competitive positioning and delivery of services

Policy Statement

1. **Access** Access is controlled to protect both the physical resources and the university data. Access to OIT data centers shall only be granted when a legitimate business need is demonstrated. This access assessment requirement specifies the criteria for granting access to specific individuals or groups, and the different levels of access allowed.
2. **Physical Security** Entry to OIT data centers shall be controlled through physical security, card swipe or keyed entry. Access shall only be granted to named individuals, and cannot be shared or transferred. The only exception is for emergency personnel, for whom shared access can be granted provided the access credentials (swipe cards/keys) are secured when not in use.
    a. Card swipe access shall be requested by email to the OIT Security Team.
    b. Card access logs will be stored by OIT Security Team
    c. Access logs shall be reviewed on a quarterly basis
    d. Key access shall be granted for emergency use to emergency personnel and facilities personnel.
3. **Levels of Access (LOAs)**
    a. **Full Access, or unsupervised 24×7 access**, to OIT data centers shall only be granted to individuals with an approved and demonstrated business need to access the data centers on a regular basis as part of their primary job duties. These individuals can come and go as needed and are not required to log their entry/exit. Individuals who require access as part of their job duties should be granted Full Access.
    b. **Unescorted Access, or "knock then enter" access**, to OIT data centers shall be granted to individuals with an approved and demonstrated business need to access the data centers on an infrequent basis as part of their job duties. These individuals must gain

entry from someone with Full Access, and must log their entry and exit to the data center. These individuals do not require an escort while in the data center, and must not allow any other person to access the data center. All Unescorted Access individuals are required to provide identification on demand and to leave the facility when requested to do so.

c. **All other individuals are considered unauthorized and granted Escort Only access**. These individuals must be accompanied by an escort at all times, and they must log their entry and exit to the data center. Any individual with elevated security who fails to present proper identification should be restricted to Escort Only access. All Escort Only access individuals are required to provide identification on demand and to leave the facility when requested to do so

d. **Individuals with an LOA of Full Access may escort and supervise unauthorized individuals** provided all individuals are logged on entry and exit and they have a business need for access to the data center. An escort must remain in the data center the entire time their guest is in the data center.

4. **Special Circumstances**
    a. **Maintenance and Custodial Staff.** University maintenance and custodial staff should be escorted when provided access to a university data center. All maintenance and custodial staff must sign the access log upon entering and leaving the data center, and inform the data center staff of any maintenance work.
    b. **First Responders.** Campus first responders, including police, fire, medical and facilities, are granted unescorted access.
5. **Physical Access Logs**
    a. A physical log of all access must be kept. All such individuals entering a university data center must sign the log as they enter and exit the facility for audit and security purposes. These logs will be review on a quarterly basis and keep for one year.
    b. Physical Access logs will be review on a quarterly basis and kept for one year.
    c. Signage is placed at all entrances/exits to direct personnel to sign in and out using physical logs.

Access Log

A log of access by anyone without an LOA of Full Access must be kept. All such individuals entering a university data center must sign the log as they enter and exit the facility for audit and security purposes.

Review

This policy will be reviewed no less than once every two years. However, threat vectors in Information Technology and Physical Security can evolve at a rapid pace creating new and unanticipated risks. As risks shift, this policy may be reviewed at any time at the discretion of the campus Information Security Officer. This policy will remain in effect until replaced.