CU Denver | Anschutz Medical Campus 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

Last Updated and Promoted: February 26, 2025

Introduction

The University of Colorado Denver | Anschutz Medical Center 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 ISS 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 ISS 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.
    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. Card Key Access logs and Physical Access Logs shall be reviewed on a quarterly basis
        i. Follow up on reviews or any security incidents discovered will be coordinated with the Anschutz ISS Office of Security and Compliance
    d. Key access shall be granted for emergency use to emergency personnel and facilities personnel.
    e. Lists of all personnel with access is maintained by the following departments, depending on location
        i. Anschutz Medical Campus Police Department, Electronic Security Division <https://www.cuanschutz.edu/police/divisons/electronic-security>
        ii. Auraria Higher Education Center, Access Control Division <https://www.ahec.edu/services-departments/facilities/access-control>
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.
        i. *To secure **Full Access** to the OIT Data Centers, individuals must take and pass the examination associated with "CU: Data Center Policy and Procedures" online training course.*
        ii. *The direct link to this training course is https://universityofcolorado.skillport.com/skillportfe/main.action#summary/CUSTOMER_DEFINED/CDE$210365:_cust_course:cu/_scorm12_cu_u00206_0001*
    b. **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
4. **Special Circumstances**

a. **Maintenance and Custodial Staff.** University maintenance and custodial staff must 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, who have not previously requested and secured full access must be escorted when provided access.

5. **Physical Access Logs**
   a. A physical log of all users without **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. 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.
6. **Access List Management**
   a. **Addition of Access:** CU Denver and CU Anschutz Medical Campus OIT requires a ticket to the OIT Service Desk (https://www1.ucdenver.edu/offices/office-of-information-technology/get-help) for additions to the Data Center Clearance Groups that enable ISS Data Center Access.
      i. ISS Risk and Compliance Department will work with Data Center Manager to validate the legitimacy of the business need for Data Center **Full Access**, as well as whether the individuals concerned have met the requirement for having taken the *"CU: Data Center Policy and Procedures" online training course.*
      ii. Upon validation by the Data Center Manager, the ISS Risk and Compliance Department will request that the Anschutz Medical Campus Police Department, Electronic Security Division will apply the appropriate Data Center Clearance Groups to the individual in question.
      iii. The Anschutz Medical Campus Police Department, Electronic Security Division will then apply the appropriate Data Center Clearance Groups to the individual in question.
   b. **Removal of Access:**
      i. Upon a staff members separation from the University, all badges will be de-activated by the Anschutz Medical Campus Police Department, Electronic Security Division effectively removing all access to the ISS Data Centers.
      ii. An individual department may request that the Data Center Clearance Groups be removed from one of their employees at any time. CU Denver and CU Anschutz Medical Campus OIT requires a ticket to the OIT Service Desk for removal of Data Center Clearance Groups that enable ISS Data Center Access.
         1. ISS Risk and Compliance Department will then request that Anschutz Medical Campus Police Department, Electronic Security Division remove the Data Center Clearance Groups from the individual.
         2. The Anschutz Medical Campus Police Department, Electronic Security Division will then remove the Data Center Clearance Groups from the individual.
      iii. On an annual basis, the Data Center Manager will review Levels of Access for individual employees with their department representatives to ensure such access is still warranted.
         1. If the access is no longer needed, the Data Center Manager will request that ISS Risk and Compliance Department remove Data Center Clearance Groups from the individual.
         2. ISS Risk and Compliance Department will then request that Anschutz Medical Campus Police Department, Electronic Security Division remove the Data Center Clearance Groups from the individual.
         3. The Anschutz Medical Campus Police Department, Electronic Security Division will then remove the Data Center Clearance Groups from the individual.
   c. CU Denver and CU Anschutz Medical Campus Data Center personnel are not responsible for providing physical access to individuals whose authorization has not been updated in the centrally maintained data Clearance Groups maintained by the Anschutz Medical Campus Police Department, Electronic Security Division.
   d. Data Center Customers (departmental representatives) remain responsible for the activities of all personnel for whom they requested **Full Access**, or provided **Escort Only Access**, whether they be Data Center customer employees, contractors or vendors.

Access Log

A physical log of access by anyone without **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 6 months.

- The review will include the Data Center Manager and the Director of Network and Hosting
- Others may be included at the discretion of the Director of Network and Hosting
- Anyone attending may propose changes to this policy
- All changes must be approved by the Director of Network and Hosting

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 Data Center Manager. This policy will remain in effect until replaced.

Electronic Security Clearance Groups that enable Data Center Access will be reviewed annually. Barring any other immediate need, those found not in compliance with Data Center Policy and Procedures or those that no longer need access will be removed from Clearance Groups at this time.