CU Denver | Anschutz Medical Campus OIT Data Center Policies and Procedures

University of Colorado Anschutz Medical Campus (CU Anschutz) and University of Colorado Denver (CU Denver)

Purpose: The purpose of this document is to serve as a guiding set of procedures for customer activity within the Denver and Anschutz Medical Center environments.

Document Type: Process

Principal Author: Steve Stelzer

Access Type: Public

Last Updated and Promoted: February 14, 2020

Introduction:

The following policies regulate activities at the CU Denver | Anschutz Medical Campus Data Centers . These rules are intended to ensure the safety and security of individuals and equipment in the Data Centers. Failure to adhere to these policies may result in the expulsion of individuals from the Data Centers and could result in the termination of access. Customers shall be responsible for all repair charges associated with any damage caused by failure to adhere to these policies.

Appropriate response to violations of these policies shall be solely within the discretion of CU Denver and CU Anschutz Medical Campus Office of Information Technologies (OIT). OIT reserves the right to update, modify or amend these rules, as needed.

Failure to knowingly comply with the following procedures is grounds for immediate removal from the facility. All persons allowed access to critical areas must review these policies and work rules and demonstrate their understanding of these procedures most applicable to their activity.

General Rules:

- All Customers and Customer vendors shall conduct themselves in a courteous and professional manner while in the Data Centers. Customers shall refrain from using any profanity or offensive language.
- Customers may not tamper with, or in any manner affect, security, infrastructure monitoring, and/or safety systems within the Data Center.
- Customers must cooperate and obey all reasonable requests of Data Center Staff while within the Data Centers, including immediately addressing any violations of rules when brought to Customers' attention.
- Upon activation of a smoke detector or emergency alarm, all Customers (their employees and vendors) must be prepared to evacuate the Data Center and or building. Further instructions and re-entry will be coordinated with OIT Staff.
- No photographs shall be taken inside the data center without the explicit permission from CU Denver and CU Anschutz Medical Campus OIT and possibly CU Denver and CU Anschutz Legal department.

Physical Security:

- CU Denver and CU Anschutz Medical Campus Data Centers are secured facilities. Access to the Data Centers and other areas of the facility are restricted to those persons with authorization. Authorization levels are defined in CU Denver-Anschutz Medical OIT DC Access and Physical Security Policy Gold.
- Customers are restricted to authorized areas only, including common areas and customer racks within the Data Centers.
- Security controls include the following:
    - Sign-in procedures for all ingress and egress
    - Managed key and access card plans
    - Managed access permissions and access request methods.
- Closed-circuit television (CCTV) cameras are used to monitor all areas of the Data Centers.
    - All CCTV cameras are monitored and images are retained. Violations noted by camera will be addressed promptly.
    - Tampering with, or in any manner adversely affecting, security and/or safety systems within the Data Centers is strictly prohibited.
- Exterior Data Center doors may not be propped open. These access doors are monitored and alarmed.
- Data Center customer will not add security devices that would hinder Data Center Management access to any individual rack or space therein.

Data Center Ingress and Egress:

All persons entering the Data Centers must:

- Possess a valid CU Denver | Anschutz Medical Campus issued photo ID.
- Have authorization to access the facility as per CU Denver-Anschutz Medical OIT DC Access and Physical Security Policy Gold.
- Display their CU Denver | Anschutz Medical Campus photo ID at all times while in the facility.

Access List Management:

Access to University of Colorado data center spaces is highly regulated and controlled. Access is limited to those granted prior authorization by OIT or data center customers and is centrally recorded by OIT personnel.

- Customers are responsible for maintaining and updating their access list with OIT.
- CU Denver and CU Anschutz Medical Campus OIT requires an email submission for additions and deletions to the Customer's access list. Individuals identified on this list will be granted access to the Customer's Rack(s).
- CU Denver and CU Anschutz Medical Campus are not responsible for providing access to individuals whose authorization has not been updated in the centrally maintained data center access lists.
- Data center customers remain responsible for the activities of all personnel for whom they requested access whether they be data center customer employees, contractors or vendors.

Common Areas:

The common areas, and room areas within the Data Centers are for the common use by all CU Denver and CU Anschutz Medical Campus Customers. The Data Centers common areas are offered as a convenience for the preparation of new equipment and the removal of old equipment.

- The Data Center common area is not to be used as an office work area.
- Equipment assembly and similar functions are restricted to the common areas.
- The use of this area will be limited to specific duties detailed above and may not be monopolized for more than 24 hours.
- CU Denver and CU Anschutz Medical Campus OIT are not liable for Customer assets left unattended in this area.
- Customers using the common areas must throw away their trash in the appropriate receptacles.

Customer Provided Equipment Standards:

- All equipment must be installed in the racks taking into consideration weight distribution with the heaviest starting in the bottom most location first and moving up.
  Departmental equipment must be installed in Racks designated for Departmental use.
- No OIT equipment will be placed in Racks designated for Departmental use.
- Placement of operating equipment outside of rack(s), is strictly prohibited.
- Equipment requirements for hosting within the North Classroom or Fitzsimons data center environment
  - All server and ancillary equipment residing in the data center must be rack mountable
  - Equipment must utilize front to back air flow for hot aisle containment
- Equipment will be labeled with the equipment name on the front, back, and any removable face plates.
  - All equipment in the data center shall have unique names.
  - Equipment shall not be labeled with external IP addresses visible from outside the host rack
- Equipment requirements for hosting with the AHSB Data Center must meet the minimum requirements as defined in AHSB Data Center, Minimum Requirements For Hosted Equipment.
- Unless otherwise agreed to in writing, Customers will remove all customer-owned hardware from the Data Center no later than the Effective Cancellation Date of Service.
- Non-OIT web cams and audio monitoring and audio capture devices are expressly prohibited in the Data Center.

Racks and Cabling Requirements:

- All low-voltage cabling installations will follow industry standards as defined here.
  - All jumpers will be labeled in accordance with CU Denver | Anschutz Medical Campus Data Center TIA 606 B Cable Labeling Standard
  - All cabling in the data center must be secured by those responsible for its installation.
  - Unsecured cabling across aisles or on the floor is strictly prohibited. .
  - Cable wrapping, wire management, or Velcro, must be used to organize cabling in a rack. For assistance with proper cable management, a customer may open a service ticket. Please contact the OIT Service Desk to open a service ticket.
  - Cabling must not obstruct airflow/ventilation/AC (perforated tiles) or access to power strips.
  - All cables must use Velcro ties to secure all cables together with in racks and on all outside runs.
  - All cables will need to be no longer than what is needed to reach the equipment and run to the next place of connection (i.e. cables will not be allowed to be coiled up inside or outside of the racks).
- Customer managed racks
  - Customer provided racks are prohibited in the Data Centers.
  - Racks shall, at all times, be clean, neat and orderly.
  - Customer racks shall not pose any danger or hazard to customer or employees (including subcontractors) that may be requested or required to enter the Data Centers to perform a service or to any other customers of the Data Centers.
  - Customers must take all necessary precautions to ensure the physical security of property contained within their Rack(s).
  - No combustible material, i.e. cardboard, foam, or paper may be stored in Customer rack(s).
  - To ensure maximum ventilation Blanking Panels must be utilized on all open rack spaces within and between all equipment in the racks at all time.
  - Customers may not make physical alternations or modifications to rack, without prior written permission from OIT.

- Customers must request Data Center Staff assistance when needing to access the space above the Hot Aisle containment system.
- Rack Doors and Door maintenance
    - Rack doors may be removed with OIT approval while Customer is working within the rack but must be replaced before Customer exits the Data Center.
    - All rack doors must be closed when the data center is unoccupied.
    - If there is an issue concerning door closure or functioning, Customers must contact the Data Center Management staff for assistance by initiating a service ticket via the OIT Service Desk.
    - Do not pry, bend, or force the doors open.

OIT reserves the right to decline implementation of a change if OIT determines the Customer rack or cabling is not in compliance. Customers in violation will be notified by OIT in writing and Customer must remedy the situation immediately

- *Customer failure to remedy the situation will result in assessment of time and material fees if CU Denver | Anschutz Medical Campus OIT takes action to make the Customer rack or cabling compliant.*
- *SLOs do not apply until the rack or cabling complies with the requirements.*

Environmental Devices:

- Customers are allowed to install their own environmental sensing devices within the racks where their equipment resides.
    - Readings from Customer installed environmental sensing devices in a rack will be considered secondary to the Data Centers environmental monitoring for purposes of determining proper response by OIT Data Center Management.
- Individual or free-standing electrical devices such as humidifier/dehumidifier, fans, air circulators, or air filters are not permitted in the Data Centers.
- Fans integrated into racked equipment (servers, routers, switches) are permitted.
- Environmental condition concerns may be addressed by Customers by opening a service ticket with the OIT Service Desk.

Power Considerations:

- Customers are prohibited from plugging their own power strips into Data Center provided PDU (daisy-chaining). This is in violation of electrical and safety codes.
    - OIT reserves the right to demand their removal.
    - Any violations of this policy must be rectified within one business day.
    - Failure to correct this violation after one business day is a material breach of the terms of the customer's contract.
    - CU Denver | Anschutz Medical Campus OIT shall not be responsible for an outage caused by a Customer provided power strip.
- Customer requested power audits must be requested via a service ticket through the OIT Service Desk to the Data Center Management.
- OIT may conduct periodic power audits of Customer Space. Any violation of power limitations must be addressed immediately.
- All PDUs must not be loaded with more that 80% of base rating.
- Individual outlets in the PDUs will be turned off as a base setting for PDU deployment.
    - Each piece of equipment to be installed into all racks of the Data Centers must be verified by the Data Center Management to comply with the equipment, rack and cabling standards as set forth in this policy before requesting that power be initiated.
    - To request the initiation for power, submit a service request with the OIT Service Desk.
- Equipment brought into the Data Center may require Data Center Staff assistance with the installation to help calculate the additional power draw of any new equipment being added to a customer's rack. This assistance is to help ensure customer power SLOs are not jeopardized.

Data Center General Environment:

- Customers are prohibited from lifting or moving floor tiles. The sub-floor area is a restricted area, accessible by OIT Staff only.
    - If a Customer needs to move a floor tile they must notify Data Center Management and officially request this service by initiating a service ticket via the OIT Service Desk.
- The tops of the racks or ladder rack may not be used for physical storage.
- Customers, in coordination with the Data Center Staff, must implement appropriate protection plans to prevent damage to Data Center infrastructure from customer shipments (plywood on raised floors, walls, overhead clearance, etc.).
- The Data Center Space is reserved for the installation and long-term support of equipment.
    - Customers shall pack all equipment outside of the Data Center Computer Rooms. No cardboard, packaging, paper and taping is allowed inside the Data Center Computer Rooms.

Data Center Support Equipment:

- Data Center equipment such as tools, dollies, carts, monitor and keyboards will be available to Customers on a first-come, first-served basis.
- Customers are responsible for all loaned equipment while it is checked out and shall return the equipment immediately.
- Modification of equipment on loan from the Data Center is not permitted without prior written approval from Data Center Management.

Shipping and Receiving:

- Customers may contact Data Center Staff for assistance with large amounts of equipment, shipments or large devices.
    - Customers must notify Data Center Management of any such deliveries that will require processing through the loading dock by submitting a Delivery Notification service ticket via the OIT Service Desk to the Data Center.

- To receive equipment, contact Data Center Management 10 days prior to shipment delivery to alert the Data Center Staff of a delivery via a service ticket initiated through OIT Help Desk.
- All packages shipped to the Data Centers must have the Customer's name and customers phone number on the shipping label. Any unidentified packages delivered to the Data Center will be refused.
- Data Center Staff will not move, unpack or uncrate any Customer owned equipment. Customers are responsible for unpacking, uncrating, and movement of heavy equipment to the Data Center floor, including all associated costs.
- All equipment to be installed in the Data Centers shall be unpacked outside the Data Center Computer Room and only the actual equipment shall be allowed inside the Computer Rooms of the Data Centers. Common areas are provided for this purpose.
- Customers, in coordination with the Data Center Staff, must implement appropriate protection plans to prevent damage to Data Center infrastructure (plywood on raised floors, walls, overhead clearance, etc.).
- The Data Center Staff will not pack and ship any Customer owned equipment.
- Customers are responsible to ensure their shipper provides all packing material and physically packs the devices for shipping to them. OIT shall not be liable for improper packing and shipping of Customer owned devices.

Audits:

All Customer requests for audits shall be made in writing and submitted to Data Center Management via a service ticket submitted via the OIT Service Desk.

- All desired audit points must be defined in the request for review.
- Unauthorized audits are strictly prohibited.