UTSA Institutional Compliance
Office of Information Security

OIS 8 – Standard for Data Center Facility

I. STANDARD STATEMENT

The University Technology Solutions Data Center (UTSDC) requires that all customers, contractors, and vendors abide by the following guidelines, which are designed to promote safety and to protect the servers and infrastructure that support the University's operations.

II. RATIONALE

This standard supports HOP Policy 8-12 Information Resources Use and Security Policy

III. SCOPE

This standard applies to all UTSA faculty, staff, and students. Any UTSDC are those data centers maintained by UTS.

IV. CONTACTS

informationsecurity@utsa.edu

V. PROCEDURES

A. GENERAL

1. UTSDC requires that all customers, contractors and vendors abide by the the following general guidelines.

   a. Food, beverages, and smoking are not allowed in the Data Center.
   b. Doors are not to be propped, blocked, or taped open. All security doors are to be kept locked at all times.
   c. The FM200 (fire suppression room) is off-limits to unauthorized personnel.
   d. Umbrellas, rain coats, etc. must be left in the front area to prevent water damage to the equipment or floor.
   e. No cleaning supplies (including water) are allowed in the Data Center without prior approval.

f. Compressed air canisters are not allowed in the Data Center. If it is necessary to cleanse a system by blowing the dust out, it must be done outside the Data Center.
g. Only HEPA filter vacuum cleaners may be used in the Data Center, and only on approved isolated power circuits.
h. Employees may only access racks containing equipment for which they are responsible.
i. Only Data Center staff may install/relocate floor tiles or make adjustments to dampers on vented floors. Floor tiles are not to be removed without prior approval from UTSDC management.
j. No air handling equipment shall be deployed within the Data Center without prior approval from the UTSDC staff. Exception: If the Data Center cooling systems have failed, and it is necessary to safeguard equipment.
k. All racks located within the Data Center will have front and rear doors and must be locked at all times. UTSDC staff must be provided with keys for all racks and systems to be kept in a secure location and used only in emergency situations.

B. ACCESS TO THE FACILITY

1. Only authorized personnel are allowed to enter the Data Center unescorted. "Authorized personnel" is defined as someone who has been granted access to the room via the card access system.
2. Non-UTSA employees without a legitimate, work related reason shall not enter the Data Center. Children under the age of 18 are not allowed in the data center under any circumstances.
3. Vendors, contractors and other individuals with a need to enter the Data Center (but do not have card access) may be placed on the Approved Access list. All Data Center access is subject to review by the UTSDC management. To request inclusion on or removal from the Approved Access list, please email your request to techcafe@utsa.edu.
4. Any UTSA employee who does not have card access, but needs to enter the facility, must present proper identification, sign in and out, and provide a legitimate reason for being in the data center. If Data Center personnel determine that the reason is not legitimate, access will be denied to the Data Center.
5. Tours, photographs, videos, etc. are to be cleared in advance with UTSDC management.

C. EQUIPMENT

1. Network devices (switches, routers, etc.) must be rack mountable and must not have wireless and DHCP services enabled.
2. New equipment must be unboxed and unpacked before it enters the Data Center. The front area of the room is designed to be used as a staging area to facilitate this.

3. Rack "U" positions that are not used or filled with rear-facing equipment (i.e. network switches) must be covered with blanking plates to ensure proper routing and distribution of air to and through the equipment in the rack.
4. All departments and vendors utilizing the Data Center must keep their areas neat, orderly, and free of refuse (such as discarded equipment boxes, paper, water, packing materials, etc.).

D. SAFETY

1. Do not place anything on or near fire suppression equipment.
2. Do not place anything on or within three feet of any transformer or electric panel.
3. Do not place anything on top of an air handler.
4. Do not block access to or view of safety equipment and signs.
5. Do not block any doors in the Data Center.
6. During a fire alarm, everyone except authorized fire responders must immediately evacuate the Data Center.
7. UTSDC reserves the right to permanently revoke Data Center access and/or request any visitors or personnel leave the premises should they violate any of these policies.

Title: OIS 8 – Standard for Data Center Facility
Effective Date: January 1, 2014
Last Reviewed: August 5, 2020