ENTERPRISE DATA CENTER
TENANT HANDBOOK

REVISED
MARCH 26, 2019

Table of Contents

PREFACE

The following safety, physical security, and operational rules relate to activities at the Texas A&M Enterprise Data Centers (University SAP: 29.01.03.M0.05 Information Resources - Enterprise Data Centers) and associated secure areas. These rules are intended to ensure the safety and security of individuals and equipment at Enterprise Data Centers and other secure areas. Failure to adhere to these rules may compromise the security or operational integrity of the services. Appropriate response to violations of these rules shall be solely within the discretion of the Division of IT, which reserves the right to update, modify or amend these rules as necessary. Occupants must cooperate with and obey all reasonable requests of Data Center personnel while on the premises, including immediately addressing any rule violations when brought to the tenant's attention.

General Guidelines:

1) All keys to racks in the West Campus Data Center (WCDC) and the Main Campus Data Center (MCDC) (formerly known as Teague Data Center) must be stored in the key inventory system (KEYper) located at each site. The WCDC Operations Team, or Security Guards are available 24/7 to open racks at the WCDC. The Incident & Operation Center is available 24/7 to open racks in MCDC. The Incident & Operation Center is located in room CS03.

2) Prior to the installation, removal, or movement of any hardware in a Data Center, an email must be sent to tamu-it-wcdc-ops@tamu.edu . A Data Center employee must be present and required to document any new installations or removals. The Texas A&M University's Division of IT maintains an inventory of all hardware in Texas A&M University's Enterprise Data Centers.

3) The installation of new hardware in the Wehner site must be approved by the CTO. Exemption requests should be emailed to tamu-it-wcdc-ops@tamu.edu . Current Tenants are encouraged to move existing production and backup systems to either WCDC or MCDC. Future operations at the Wehner site will be limited to network operations and legacy systems.

4) The Data Centers are secure facilities. Access to the Data Centers and other secure areas are restricted to persons with authorization.

5) The Division of IT reserves the right to exclude anyone from the facility, with or without cause and with or without notice. Anyone requested to leave the premises must do so immediately and peacefully.

6) Active video surveillance is employed both inside and outside the Data Centers and other secure areas.

7) The parking lot at the West Campus Data Center (WCDC) data is classified as an 'Any Valid Permit' lot, which means any person/vehicle with a currently valid Texas A&M Parking Permit is able to park in the lot.

8) A visitor upon entering the WCDC will be greeted by a security officer. The visitor must present a government-issued or Texas A&M University photo ID to receive a visitor's badge.

9) Badges/ID Cards must always be worn (and visible) while in a Data Center. Persons found not to be wearing an authorized badge/ID card will be asked to leave.

10) Tenants and vendors are restricted to authorized areas only. Areas tenants and vendors may be authorized for are limited to the lobby, lounge, conference rooms, common areas and tenant spaces on a Data Center floor.

11) WCDC physical security controls include a 24x7 security officer, sign-in procedures for all ingress and egress, managed key and access card plans, security enclosure, managed access permissions and access request methods.

12) All tenants of a Data Center must individually badge in and out using the electronic key card readers. Tailgating (multiple people entering/leaving on one card swipe) is not allowed.

13) Tenants may not bring guests into a Data Center without consent of Data Center stff. ALL guests must be escorted by the Tenant while visiting the Data Center.

14) Tours must be preapproved one (1) week in advance. All tours must be conducted by Data Center staff and the tour may not contain more than 15 people. Note that some areas of the Data Center have special safety or security designations and are not included in tours.

15) Any visitor or temporary badges, access cards, keys, and/or tools issued by the Division of IT must be surrendered prior to exiting the facility.

16) Equipment should be in the assigned location unless currently undergoing repairs or removal.

17) Tools or diagnostic equipment should be stored away when not in use.

18) Aisles should be kept free of materials, including wiring, cables, and other related materials.

19) Cameras are not permitted without prior approval from Data Center staff.

Compliance and Safety:

1) Safety and physical security

   a) Adherence to the following University SAPS is required:

      i) 24.01.01.M7 Fire and Life Safety Compliance

      ii) 24.01.01.M0.02 Visitors in Hazardous Areas

   b) Fire routes and locations of exits will be reviewed with all tenants and visitors. All fire alarms must be obeyed and everyone must evacuate the facility when alerted. Upon activation of a smoke detector or emergency alarm, all occupants must be prepared to evacuate the building to receive further instructions from Data Center staff.

   c) No one may tamper with — or in any manner adversely affect — physical security, infrastructure monitoring, and/or safety systems within the Data Center.

   d) Data Center doors must never be propped open. Emergency egress doors are monitored and will alarm on breach. Emergency egress doors should only be used during an emergency. No re-entry is allowed.

e) Tenants and visitors are solely responsible for personal belongings and property while on the premises. The Division of IT is not responsible for any missing, lost or stolen property of any tenant, vendor or visitor, or loss, damage or theft of vehicle or the contents thereof while located in a Data Center parking area.

f) Storage or use of combustible materials is not permitted inside a Data Center. Combustible materials must be unpacked on the loading dock or storage areas. Combustible materials include but not limited to: wood, cardboard and corrugated paper, plastic or foam packing materials, flammable liquids or solvents.

g) Cardboard and other shipping materials are not permitted in the data halls.

h) Persons under 18 years of age are not permitted within the Data Centers without the supervision of Data Center staff.

2) Cyber Security and Monitoring

a) All systems residing inside of a Texas A&M University Enterprise Data Center and on a Texas A&M University network will be monitored by Texas A&M University Security Operations.

b) Periodic vulnerability scans will be run on all systems residing inside of a Texas A&M University Enterprise Data Center that are on a Texas A&M University network. It is the responsibility of the tenant or system owner or system administrator to patch any vulnerabilities they are made aware of. Failure to patch critical and high vulnerabilities after three requests could result in the system(s) being blocked on the network until patched.

c) Texas A&M University Incident Response team reserves the right to take immediate action on any system inside of a Texas A&M University Enterprise Data Center that is also on a Texas A&M University network, in case of cyber-attacks. Any such action will happen with the consultation and involvement of the system owner. However, in rare cases where the system owner cannot be located in time and a larger threat exists the Incident Response team will take action to respond to the cyber incident without the initial consultation of the system owner.

3) Prohibited items

a) Food and beverages are strictly prohibited beyond the security enclosures and within the Data Center raised floor space. All food and beverages must be served and consumed in designated areas of the break room within the office annex only.

b) Uninterrupted power supply (UPS) equipment, other than what is provided by the Division of IT, is prohibited.

c) Smoking and tobacco products are expressly prohibited in all TAMU buildings pursuant to University SAP 34.05.99.M1 (http://rules-saps.tamu.edu/PDFs/34.05.99.M1.pdf).

d) Alcohol is prohibited within the buildings pursuant to University SAP 34.03.01.M1 (http://rules-saps.tamu.edu/PDFs/34.03.01.M1.pdf)

e) Skateboards, skates, scooters, bicycles or other types of vehicles are prohibited in the Data

Center.

4) Conduct and attire

   a) All tenants and visitors to the Data Center should wear business appropriate attire.

   b) Closed-toe shoes must be worn at all times.

   c) All tenants and visitors shall conduct themselves in a courteous and professional manner while visiting the Data Center. Out of respect for others in the facility, please refrain from using profanity or offensive language.

Access Request to Enterprise Data Centers

Electronic badge access will only be granted to Data Center tenants with responsibility for supporting equipment housed within the facility. All requests for badge access must be submitted through the Division of IT BARS system (https://bars.tamu.edu). The requestor must be approved in BARS by their organizational approver and then by the Division of IT. Final authority for granting access remains with the Division of IT. The Organizational Approver must provide timely notification to the Division of IT when access is no longer approved by the organizational approver.

Tenants who are granted electronic badge access must still adhere to all check-in and operational procedures, and all rules of the Data Centers.

Renewal Procedures

Full-time TAMU employees: Access authorization is annually reviewed during the announced renewal period.

Vendors: Access authorization is annually reviewed during the announced renewal period.

Data Center Use

1) The Division of IT reserves the right to access any part of the Data Center at any time for safety, physical security or operational reasons.

   a) The Division of IT's Information Technology Infrastructure Operation (ITIO) group may access racks for the express purpose of creating an inventory of what is in each rack for the following reasons;

      - to leverage Rack PDU management features that include power monitoring and power cycling,
      - to assist organization level property managers during their annual inventories,
      - and to report Data Center utilization information to senior management.

   b) The Division of IT has a mandate from the Texas A&M System to support the movement of significant IT Equipment into the West Campus and Main Campus Data Centers (MCDC) (formerly known as Teague Data Center). Policies that relate to this mandate are http://policies.tamus.edu/29-01-03.pdf and

http://rules.tamu.edu/PDFs/29.01.03.M0.05.pdf .

29.01.03 Information Security

Each member shall consolidate all of its significant IT equipment into a centralized member Data Center(s) or approved commercial Data Center as soon as practically possible but no later than September 1, 2019. "Significant IT equipment" includes, but is not limited to, mass storage, large/complex computational environments, most virtualized or physical-based servers, and any other internet exposed services. A member may request exceptions for certain equipment, such as specialized lab or research equipment. Each centralized member Data Center shall provide colocation services and fully managed services for member departments and units. At a minimum, each Data Center must have: redundant power delivery, redundant networks, redundant cooling, and physical and cybersecurity, and may also provide operating system setup and administration (including virtualized), backup and recovery, storage management, configuration and patch management, and other managed services. All requests for exceptions to the requirements of this section, including requests to extend the deadline, must be approved in advance by the chancellor and reported on an annual basis to the SCISO.

29.01.03.M0.05 Information Resources – Enterprise Data Centers

3.1 All high or moderate impact information resources must:

3.1.1 Reside in a Texas A&M Enterprise Data Center;

3.1.2 Be documented and maintained in the designated Texas A&M risk management system, including disaster recovery and backup information; and 29.01.03.M0.05 Information Resources – Enterprise Data Center

3.1.3 Follow all applicable Texas A&M information security controls.

3.2 Terms and conditions for the use of a Texas A&M University Enterprise Data Center are determined by the Vice President for Information Technology and Chief Information Officer.

3.3 The Vice President for Information Technology and Chief Information Officer shall maintain an "Approved List of Cloud Computing Providers" which enumerates commercial service providers that are approved for the purposes of hosting moderate or high impact information resources. A copy of such list may be obtained directly from the office of the CIO or may be obtained electronically via the office website. to report back to the President and the Board of Regions on the status of the move.

2) Tenant cage or cabinet shall be kept clean, neat and orderly at all times. Tenant space shall not pose any danger, hazard or obstruction to other tenants or employees (including subcontractors) who may be requested or required to enter the data hall to perform a service.

3) Tenants and Vendors are prohibited from touching, inspecting, documenting or any form of tampering with equipment that they are not the authorized administrator for that equipment. Persons seen engaging in such activity will be reported to security and may be subject to expulsion from the facility and legal action.

4) Tenants must take all necessary precautions to ensure the physical security of property contained within their assigned location(s). Cage and cabinet doors must be secured at all times when a tenant is not physically present.

5) Tenants must remove all refuse materials (which include but are not limited to boxes, crates, corrugated paper, plastic, foam packing materials, and any other materials which are nonessential to the operation of tenants' equipment) from the loading dock and make ready areas within eight (8) hours. Materials must be placed in designated disposal receptacles outside of the building.

6) The creation of "office space" within the tenant area on the Data Center raised floor is prohibited.

7) All spare/surplus equipment shall be removed from the data hall. No cabinet storage spaces are provided or allowed in the data halls.

8) "Un-racked" equipment outside of cabinets or racks, is strictly prohibited.

9) Tenant may not hang or mount anything on the cage mesh walls or cabinets unless authorized by Data Center staff.

10) The tops or inside of the cabinets or ladder rack may not be used for physical storage.

11) The Division of IT furnishes blanking panels. To ensure maximum ventilation, blanking panels must be utilized on all open rack spaces within and between racks at all times.

12) Unsecured cabling across aisles or on the floor is strictly prohibited. All devices must be installed in racks or cabinets. Ladder racking must support all cabling between rows. Division of IT Networking must approve all outside cabinet cabling.

13) Cable wrapping, wire management, zip ties and/or Velcro, must be used to organize cabling in a rack or cabinet. Should tenant need assistance with cable management, the Data Center staff can be contacted or a ServiceNow ticket may be submitted.

14) Cabling must not obstruct airflow/ventilation/AC (perforated tiles) or access to power strips and must be enclosed within the cabinet.

15) Non-compliance with any of the cage, cabinet or cabling requirements will result in notification to tenant and a request that the tenant promptly take action to remedy the situation. Tenant failure to remedy the situation will result in assessment of time and material fees if the Division of IT takes action to make the tenant cage, cabinet or cabling compliant.

16) Tenants may not climb onto cabinet and/or scale cage walls. Tenant must request staff assistance to access cabinet/rack tops

17) Tenants may not make physical alterations or modifications to the space without prior written permission from the Division of IT.

18) Tenants are not to hang anything from the Gordon Grid ceiling under any circumstances.

19) Tenants may not modify or remove the containment doors. Containment doors must remain closed except when entering or exiting the aisle.

20) Tenant failure to remedy any violation of the Data Center policies will result in assessment of time and material fees if the Division of IT has to takes actions to make the tenant cabinet, cage or suite compliant with the rules.

21) Tenants must clear audible alarms within 72 hours of notification.

Cabinet Doors

1) If a tenant needs a cabinet door removed, approval and assistance must be given by the Data Center staff and the door must be replaced properly and shut before the tenant exits the Data Center.

2) All tenant cabinets are equipped with doors which must be closed upon completion of work.

3) Should locks or doors not function properly, the tenant should contact the onsite Data Center staff for assistance. Do not pry, bend, or force doors open. Tenant shall be responsible for any repair charges associated with damage to doors caused by tenant.

Floor Tiles

1) Tenants are prohibited from lifting, removing or moving floor tiles in any part of the facility, including the data halls. The sub-floor area is restricted and accessible by Data Center staff only. The perforated tiles are strategically placed for HVAC cooling patterns. If experiencing temperature problems, a tenant should notify Data Center staff to resolve the cooling issues.

2) No movement of equipment that damages or scars the flooring is permitted. Contact Data Center staff if you require permission or assistance in equipment movement.

Data Center Equipment

1) Data center equipment such as tools, dollies, carts, server lifts, monitors and keyboards made available to tenants must be returned in good working order. Any damaged equipment will be charged to the tenant.

2) Modifications to loaned equipment is not permitted without permission from Data Center Staff.

3) Equipment must be used only for purposes defined by the original equipment manufacturer. At no time should equipment be used to transport, lift or hold people unless specifically defined for that purpose.

Shipping and Receiving

1) Tenant may bring equipment which can be hand-carried into the Data Center through the lobby. Tenant may contact Data Center Staff for assistance with equipment movement. Large amounts of equipment, shipments or large devices must enter the Data Center through the shipping/receiving dock. Tenants must notify Data Center management of any such deliveries

that will require processing through the loading dock by submitting a delivery notification to the e-mail address below:

tamu-it-wcdc-ops@tamu.edu

2) The email should include
   a) Purchase Order Number
   b) Name of person responsible for the equipment Vendor and / or Manufacture
   c) Type of equipment (Number of servers, racks, and or packages that were ordered)
   d) Estimated Date of shipping/receiving if known
   e) Company delivering/shipping equipment
3) The shipping address for all hardware is;

   West Campus Data Center (WCDC)
   Att: Recipient's Name/Dept.
   474 Agronomy Rd
   CS, Texas 77843

   Computing Services Center (Main Campus Data Center)
   Att: Recipient's Name/Dept.
   Building 0516 Room CS12
   731 Lamar St, College Station, TX 77843-3363

4) All packages shipped to the Data Centers must have the tenant's name and tenant information on the shipping label. Unidentified packages are a security risk. Any unidentified packages delivered to the Data Center will be refused for security reasons. Packages and smaller shipments will be received and stored in the secured storage room. Tenants will need to coordinate pick-up of such items within a period of time no longer than two weeks. After two weeks, packages may be shipped back to the tenant's department or back to the supplier at tenant's expense.
5) Storage in the MCDC is limited. Packages received at the MCDC will be stored if space is available, longer term storage is available in the WCDC storage area.
6) Tenants must unpack all equipment before it is moved into the WCDC data halls and the MCDC. All packing materials must be disposed of properly in the waste receptacles located in the parking lot.
7) Tenant, in coordination with Data Center staff, must implement appropriate protection plans to prevent damage to Data Center infrastructure (plywood on raised floors, cage wall removal, overhead clearance, etc.). Observe posted signage in the shipping/receiving area that egress points to raised floor areas noting that tenant should contact Data Center staff before moving equipment.
8) The Data Center staff is not responsible for packing and shipping tenant-owned equipment. The tenant may authorize the Data Center staff to have temporary access for their shipping company

to enter their cage or cabinet, to de-rack a device and make it available to the tenant's shipping company. The tenant must be present when the shipping company has specific orders to pick up or ship to the tenant space or cabinet. Data Center staff must escort the shipping agent and will designate the appropriate egress route.

9) The tenant is responsible for ensuring their shipper provides all packing material and physically packs the devices for shipping. The Division of IT shall not be liable for improper packing and shipping of tenant-owned devices.

10) Tenants and vendors are not allowed in the storage and receiving/shipping areas unescorted. Only Data Center staff may operate the dock and elevator lifts.

11) Upon termination of Data Center use, tenant must leave the space in good condition and must remove any tenant equipment and other tenant property from the space.

Environmental Devices

1) The Division of IT operates and monitors the facility's environmental controls. Readings from tenant-installed environmental sensing devices in a cage or cabinet will be considered secondary to Data Center environmental monitoring and must be approved by Data Center staff. Tenant-installed environmental sensing devices must not interfere or interrupt any Data Center monitoring systems.

2) Individual or free-standing electrical devices, such as humidifier/dehumidifiers, fans, air circulators or air filters, are not permitted in cage areas, cabinets or data hall floors. Fans integrated into racked equipment (servers, routers, switches) and tenant-provided racks must be reviewed and approved by Data Center staff. Should any tenant need assistance with environmental conditions, Data Center staff must be contacted.

Tenant-Provided Cabinets

1) The Division of IT will provide all industry standard server cabinets in the Data Centers. Requests for the use of any other cabinet or enclosure must be submitted for review and consideration by the Division of IT's Chief Technology Officer. The dimensions, height, weight and operational requirements (HVAC impact, power and network requirements) of any tenant-provided cabinet or enclosure must be submitted in writing for inclusion in site documentation. Data Center Staff will participate in and oversee the installation of the tenant-provided racks to ensure proper installation and compliance with all applicable ordinances, codes, site standards and to ensure no interference with a CCTV camera field-of-view.

WCDC Supplied Power Strips (PDUs)

1) Each standard Division of IT cabinet is equipped with two L6-30 power strips (PDUs) with a total of 24 outlets containing 20 locking IEC C13 and four locking IEC C19 outlets.

2) Tenants requesting power in a different configuration must get approval from Data Center staff. If the proposed PDU configuration is approved, the Division of IT will supply the requested PDU and bill the tenant for the cost.

3) ONLY Data Center staff may install, uninstall, plug in, and power up or power off any PDU or power outlet.

4) Access above cabinets is prohibited. Only Data Center staff may interface with this area.

5) Tenants are prohibited from plugging in or daisy chaining additional power strips in their cabinets. This is a violation of electrical and safety codes. Any violations noticed by Data Center Staff must be corrected by the tenant within one business day. Failure to correct this violation may result in the power being turned off to the strip or cabinet.

6) For PDUs installed in MCDC, the Division of IT is not be responsible for damages or outages due to non-standard or tenant-provided power strips, or from prohibited equipment malfunction.

WCDC Tenant Provided Additional Security Devices

Tenants are not allowed to add security devices that would hinder staff access to the cage or cabinet areas. To ensure the safety and security of all areas, the Division of IT must have access to all areas of the Data Center at all times.

Data Center Goal

It is the goal of the Texas A&M Division of IT to provide the highest level of services to our Data Center tenants and guests. These guidelines and rules have been carefully developed to clarify our quality expectations, to reduce the risk of mistakes and unintended events, and to ensure that every tenant has the confidence that the IT services they host in our facility will provide them with highly available, robust and resilient levels of service. It is vitally important that you understand this is a shared service facility and you exhibit the utmost respect for all of your co-tenants. Adherence to the Data Center and university policies, rules and procedures is essential to our ability to deliver the high quality services expected by our stakeholders.

It is critical you understand the potential for negative impact of your actions could have on this site as a result of working inappropriately, and our desire to avoid such instances. These procedures and guidelines have been developed to clarify our quality expectations and to reduce the chance of mistakes and unintended events. Failure to comply with any procedure may result in your immediate removal from the site and may result in permanent loss of your access to the facility.

If you have any questions or concerns, please contact the Division of IT Incident Operations Center (IOC) at 979.458.1152. If you have an immediate security concern contact the WCDC Security Guard Office at 979-458-7843

For any general questions about Data Center Operations email tamu-it-wcdc-ops@tamu.edu

Enterprise Data Center

Tenant Handbook Acknowledgement

I have been given a copy of the Texas A&M Enterprise Data Center Tenant Handbook and acknowledge its receipt. I have had an opportunity to review and ask questions about these procedures and policies. I agree to follow these procedures and policies. I further agree to report any violation of these rules and regulations or any other suspicious or improper activity to Data Center staff.

The latest version of the Texas A&M Enterprise Data Center Tenant Handbook can be found on the Division of IT Data Center and Hardware web page (https://it.tamu.edu/services/data-center-and-hardware/data-centers/campus-data-centers/). Periodically email notifications will be sent to you when changes to the Texas A&M Enterprise Data Center Tenant Handbook are made.

NAME: _____

ORGANIZATION: _____

SIGNATURE: _____

DATE: _____

REVISED
MARCH 26, 2019