CS&T Data Center
Hosted Shared Services
Policies & Work Rules

Personal Accountability
Failure to 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 the procedures most applicable to their activity.

It is important that you understand the potential for negative impact that 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 incidents. Failure to comply with any procedure may result in your immediate removal from the site and may result in the permanent loss of your access to the facility.

I have been given a copy of the CS&T Data Center Hosted Shared Services Policies & Work Rules and acknowledge their receipt. I have had an opportunity to review and ask questions about these policies and procedures. I agree to follow these policies and procedures to the best of my abilities.

Company, Department, or College _____

Name [print] _____

Signature _____ Date _____

Accepted by CS&T Data Center _____ Date _____

If at any time you have questions or require assistance use the following numbers:

CS&T Data Center Policies & Work Rules

The following policies regulate activities at the CS&T Data Centers (for convenience, referred to as "Data Center" in this document). These rules are intended to ensure the safety and security of individuals and equipment at the Data Center. Failure to adhere to these rules may result in the expulsion of individuals from the Data Center and could result in the declaration of default by Data Center for the Customer and the termination of the Customer contract. Appropriate response to violations of these rules shall be solely within the discretion of CS&T. CS&T reserves the right to update, modify or amend these rules, as necessary.

A. General Guidelines

1. All Customers and Customer vendors shall conduct themselves in a courteous professional manner while visiting the Data Center. Customers shall refrain from using any profanity or offensive language.
2. Customers may not tamper with, or in any manner adversely affect, security, infrastructure monitoring, and/or safety systems within the Data Center.
3. CS&T is not responsible for any loss, damage or theft of vehicle or the contents thereof, while located in campus parking areas.
4. Alcohol, controlled substances, firearms, and explosives are not permitted on CS&T property. Smoking, drinking, and eating are strictly prohibited within the Data Center raised floor space. Smoking is expressly prohibited in all CS&T buildings.
5. Persons under 18 years of age or requiring adult supervision are not permitted within the Data Center without the express written permission of CS&T.
6. All visitors to the Data Center should wear appropriate footwear and attire.
7. Unless otherwise expressly permitted by CS&T in writing, storage of combustible materials (e.g. wood, cardboard and corrugated paper, plastic or foam packing materials, flammable liquids or solvents) are prohibited within the Data Center. Customers are expected to be familiar with and adhere to all OSHA standards associated with work in a computer room environment.
8. Customers may use cell phones inside the Data Center. Two-way radios are not permitted in the Data Center. Cell phones with camera capabilities may not be used for picture or video capture.
9. Skateboards, skates, scooters, bicycles or other types of vehicles are prohibited in the Data Center.
10. Sharing CS&T Proprietary information, without the express written permission of CS&T, is strictly prohibited.
11. All hand-carry containers, boxes, bags, laptops, purses, backpacks, or equipment carried into or out of the Data Center are subject to inspection by Data Center staff and/or Security.
12. CS&T does not accept Mail/Post on behalf of Customers at the Data Center. All Mail/Post should be directed to the Customer's business address.

13. Customers must cooperate and obey all reasonable requests of CS&T staff while within the Data Center, including immediately addressing any violations of rules when brought to the Customer's attention.
14. Upon activation of a smoke detector or emergency alarm, all Customers (including their employees and vendors) must be prepared to evacuate the building and await further instructions from the CS&T staff.

B. Pictures or Video

15. Any use of cameras, video, and other photographic equipment along with but not limited to audio monitoring and audio capture devices are prohibited within the Data Center without the express written permission of CS&T. No person, other than CS&T staff, shall be permitted to take photo or videotape records within the Data Center.
16. Customers are not permitted to take pictures or videos of the Data Center. Customer site pictures or videos must be arranged in advance and according to CS&T Security regulations.
17. If pictures or video are required for insurance or marketing purposes, contact CS&T for assistance.
18. All types of cameras, unless otherwise provided in this Service Guide, are prohibited in the Data Center.

C. Physical Security

19. CS&T Data Centers are secured facilities. Access to the Data Center and other areas of the facility are restricted to authorized persons.
20. Customer access is restricted to authorized areas only.
21. Security controls include 24 x 7 staff presence, sign-in procedures for all ingresses and egresses, managed key and access card plans, managed access permissions, and access request methods.
22. Security cameras are used to monitor some areas of the facility including lobbies, common areas, Data Center floor space, and admin areas. All cameras are monitored and images are retained. Violations noted by camera will be addressed promptly.
23. CS&T attempts to provide off street parking, where feasible, with adequate lighting. CS&T is not liable for damage, loss, or theft of vehicles and/or their contents.
24. Tampering with, or in any manner adversely affecting, security and/or safety systems within the Data Center is strictly prohibited.
25. Exterior Data Center doors may not be propped open. These access doors are monitored and alarmed.
26. CS&T reserves the right to access any part of the Data Center at any time for safety and security reasons.

D. Data Center Ingress and Egress

27. All Customers entering the Data Center must:
    a. Possess a valid government-issued photo ID.
    b. Have authorization to access the facility.
    c. Sign in and out as required by the facility.
    d. Display their CS&T temporary "T" security badge at all times while in the facility.
    e. Surrender their security badge and Data Center owned tools prior to exiting the facility.
28. Customers are expected to be familiar with and adhere to all OSHA standards associated with work in a computer room environment.

E. Access List Management

29. Customers are responsible for maintaining and updating their access list. CS&T requires a written submission for additions and deletions to the Customer's access permissions list. Individuals identified on this list will be granted access to the Customer's Cabinet. Customers may grant temporary access to their Cabinet for an employee, vendor or technician by submitting an e-mail to xxxxxxx@xxxxxxx (See Exhibit 1) .
30. CS&T shall not be responsible for the actions of persons who are still in the CS&T access list, but who are no longer authorized by the Customer to access the Data Center. The Customer remains responsible for the activities of these individuals as with any other authorized Customer employees, contractors, or vendors.

F. Common Areas

31. The common areas are lobbies and hallways.
32. Customers using the common areas must throw away their trash in the appropriate receptacles.
33. A staging area is not available for Customers.
34. CS&T reserves the right to deny access to those Customers who abuse the common areas and the rights of other Customers.

G. Cage/Cabinet and Cabling Requirements

35. The Customer cabinet shall, at all times, be clean, neat, and orderly. Customer space shall not pose any danger or hazard to customers or employees (including subcontractors) that may be requested or required to enter the cabinet to perform a service or to any other customers of the Data Center.
36. Customers must take all necessary precautions to ensure the physical security of property contained within their customer location(s). Cabinet doors must be secured at all times when a Customer is not physically present.
37. Customers must remove all refuse materials. These materials include, but are not limited to boxes, crates, corrugated paper, plastic, foam packing materials, and any other materials which are non-essential to the operation of the

Customers' equipment. Materials must be placed in designated disposal area at the loading dock.

38. The creation of "office space" within the Customer Area on the Data Center Floor is prohibited. The Customer Area is reserved strictly for Customer cabinet(s) and the contents thereof.
39. "Un-racked" equipment, i.e. operating equipment outside of cabinets or racks, is strictly prohibited.
40. No combustible material, e.g. cardboard, foam, or paper, shall be stored in Customer cabinet.
41. Customers may not hang or mount anything on the walls, cabinets, fire suppression equipment or network gear unless authorized by the Computer Operations staff.
42. The tops of cabinets or ladder racks may not be used for physical storage.
43. 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. Cabling and racking is solely done by CS&T.
44. Cable wrapping, wire management, zip ties and/or Velcro (done solely by CS&T), must be used to organize cabling in a rack or cabinet.
45. All racking and de-racking of equipment will be done solely by CS&T.
46. CS&T reserves the right to decline the implementation of a Change Order if CS&T determines the Customer cabinet or cabling is not in compliance. Customers in violation will be notified by CS&T in writing and Customers must remedy the situation immediately. SLAs do not apply until the cabinet or cabling complies with the requirements.
47. Customers who do not comply with cabinet and cabling requirements will be notified and requested to promptly remedy the situation. If the Customer fails to remedy the situation, CS&T will make the Customer cabinet or cabling compliant and charge the Customer the time and material fees this action has incurred.
48. Customers may not climb onto cabinet and or scale walls. Customers must request CS&T staff assistance if they need to access cabinet /rack tops.
49. Customers may not make physical alternations or modifications to the space, without prior written permission from CS&T.

H. Rack/Cabinet Doors

50. Customers are not allowed to remove or replace the doors of their assigned cabinets. Customers must submit a work request to CS&T and once approved, the appropriate Computer Operations staff will remove or replace the Customer's cabinet doors.
51. If Customer cabinets are equipped with doors, the doors must be closed when the Customer is finished working on devices.
52. Should the locks or doors not function properly, Customers should contact the on-site CS&T staff for assistance. Do not pry, bend, or force the doors open. CS&T shall not be responsible for any repair charges associated with Customer-incurred damage to doors at the Data Center.

I. Floor Tiles

53. Customers are prohibited from lifting or moving floor tiles. The sub-floor area is a restricted area, accessible by CS&T staff only. The perforated tiles are strategically placed for HVAC cooling patterns. If a Customer is experiencing temperature problems, the Customer should notify CS&T staff. Only CS&T staff is permitted to access the sub-floor.

J. Data Center Equipment

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

K. Receiving

56. Customers may bring small hand-carried equipment through the lobby. Customers may contact CS&T staff for assistance. Large amounts of equipment, shipments, or large devices must enter the Data Center through the shipping/receiving dock. Customers must notify CS&T of any such deliveries that will require processing through the loading dock by submitting an e-mail to xxxxxxxx@xxxxxxxx.
57. Hand-carried equipment brought into the Data Center that need to be installed may require CS&T technician assistance 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 SLAs are not jeopardized.
58. All equipment brought to the Data Center must have the Customer's name and College and Department with a phone number on it. Unidentified equipment is a security risk. Any unidentified equipment delivered to CS&T will be refused for security reasons.
59. CS&T staff will not move (from loading dock to CSB-107), unpack or uncrate any Customer owned equipment (cabinets, servers, etc). Customers are responsible for unpacking, uncrating, and movement of heavy equipment to the Data Center floor, including all associated costs. Assistance for equipment more than 100 pounds may be offered to the Customer at the discretion of CS&T.
60. Customers, in coordination with the CS&T staff, must implement appropriate protection plans to prevent damage to Data Center infrastructure.
61. CS&T will not pack and ship any Customer-owned equipment. Customers may open a ticket to authorize temporary access for CS&T to enter their cabinet, or to have the data center staff de-rack a device and make it available to the Customer.

L. Removal of Equipment at End of Term

62. Unless otherwise agreed to in writing, Customers will have all their hardware removed from the Data Center no later than the Effective Cancellation Date. Customer-owned hardware remaining in the Data Center after the Effective Cancellation Date becomes the property of CS&T.
63. Upon termination or expiration of Service, Customers must leave the space in as good condition, normal wear and tear accepted, as it was at the Commencement Date. CS&T will remove any of their equipment and property from the hosted space.
64. Customers shall refer to the Service Guide for Cancellation guidance.

M. Customer Provided Cabinets

65. Customers may provide Dell cabinets upon approval of CS&T. CS&T will mount Customer-provided cabinets to ensure proper grounding and compliance with all applicable ordinance codes.

N. Customer Provided Power Strips

66. Customers are prohibited from plugging their own power strips into Data Center. This is in violation of electrical and safety codes, and CS&T reserves the right to demand their removal from the Data Center. 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.

O. Customer Provided Additional Security Devices

67. Customers are not allowed to add security devices that would hinder CS&T from accessing their cabinet. This is for security and safety reasons. CS&T must have access to all areas of the Data Center at all times.

Exhibit I: An example of an "Access Ticket"

Subject: Customer College/Department Access Ticket for 12/20/09

Access Ticket:

Customer College/Department ; ABC Corporation

Name and vendor: **John Doe (Dell Technician)**

Task being performed: **Working on the Dell Storage Array.**

Start Date\Time: **12-20-2009 at 01:00 PM**

End Date\Time: **12-20-2009 at 05:00 PM**

Location of Task: **ABC Corporation's cage in Data Center**

Escorted or Not Escorted: **Will need to be escorted (not on access list)**

Bill Smith
Director IT
ABC Corporation

Any additional comments or info relevant to this person's access go here.