# Data Centers and Mission Critical Facilities Operations Procedures

## Attachment A

(Referenced in UW Information Technology Data Centers
and Mission Critical Facilities Operations Policy)

Updated: 04/15/2010
Created: 05/30/2005
Planning & Facilities
Data Centers & Facilities Management
206.221.4500
uwtech-facilities@uw.edu

## 1.0    Purpose

1.0.1    In order to provide reliable, safe and secure data centers and mission critical facilities, certain practices must be instituted and enforced.  This document establishes standards and procedures for UW Information Technology (UW-IT) centrally managed data centers for the University of Washington (UW), both owned and leased, along with other mission critical support facilities. These procedures apply to all authorized UW employees as well as authorized business partners and affiliates of the UW, including contractors, vendors, UW co-location customers, and UW co-location contractors. These procedures address topics that include, but are not limited to, safety, security, packing material, salvaging of equipment, space requests, computer hardware installs and de-installs, power, cabling, overall cleanliness, and other miscellaneous items within the data centers.

## 2.0    Exceptions

2.0.1    UW unit heads may solicit the Executive Director of Planning & Facilities for exceptions to any of these procedures.

## 3.0    Procedures

## 3.1    Safety Requirements

3.1.1    No floor tiles may be removed without the permission of the Data Center & Facilities Management (DCFM) manager or data center planner.  If floor tiles must be removed, the open space must be cordoned off by cones and safety tape.  No more than two contiguous tiles may be open at the same time. No more than six tiles in total may be open at the same time.

3.1.2    All computer cabinets and doors must remain closed at all times, unless they are being serviced.

3.1.3    Authorized electricians must perform all modifications to electrical service. All such changes must be authorized and coordinated by the DCFM manager or data center planner. All electrical testing must be conducted during off-hours. All work must be compliant with the National Electrical Code (NEC) and follow the guidelines of TIA-942.

3.1.4    Activation of emergency power off (EPO) system shall be avoided at all times. Placing this system into by-pass or disabled is a requirement. Step by step instructions will be provided by a DCFM planner on how to bring this system in

and out of by-pass or disabled status. In all cases UW-IT Computer Operations must be notified before the system becomes inactive and when it is returned to service.

3.1.5    No work may be done below the raised floor area without the approval of the DCFM manager or data center planner.

## 3.2    Air Condition and Air Quality Requirements

3.2.1    Humidity levels in the UW data centers (excluding non-data center mission critical facilities) must be maintained at 40% – 50%.

3.2.2    Temperature levels in the UW data centers and other mission critical facilities must be maintained ideally at 70 degrees (F), and always within 65 – 75 degrees (F).

3.2.3    All computer room air conditioners (CRACs) and computer room air handlers (CRAHs) must be serviceable at all times. Preventive maintenance service will occur monthly or quarterly (site dependent).  Preventive and emergency maintenance services may not be restricted in any way.

3.2.4    Industrial cleaning liquids or fluids may not be left unattended in the data center.  No highly ammoniated or chlorinated products are allowed in the data centers.

3.2.5    All floor tile alterations must be approved and coordinated by the DCFM manager or data center planner.  If holes must be cut in the floor panels to accommodate new equipment, the panel shall be removed from the data center, the holes cut, and a KoldLok ™ floor grommet (or other approved floor grommet) installed.  If the floor tile cannot be removed from the data center, HEPA vacuums must be used both above and below the raised floor surface to capture the dust particles created by the sawing action.  A KoldLok™ floor grommet (or other approved floor grommet) must then be installed. A HEPA vacuum is available from DCFM.  The vacuum must not be removed from the data center.

3.2.6    Due to the adverse effect on sub-floor pressure, the number of floor tiles pulled must be kept to a minimum.  When working in a raised floor room, no more than two contiguous floor tiles may be open at the same time. No more

than six floor tiles in total may be open at the same time. All vented floor tiles must be returned to the positions from which they were removed and all air dams maintained in the position they were found.

3.2.7    If no work is being performed, no open holes of any kind may be left exposed in the data center raised floor, to avoid creating unbalanced airflow and an unsafe work condition. No additional vents, grills or perforated tiles may be added without coordination with the DCFM manager or data center planner.

3.2.8    Except in designated areas, no food or beverages are allowed in the data center.

3.2.9    No changes may be made to the data center heating, ventilation and air conditioning (HVAC) systems without the approval of the DCFM manager.

3.2.10    New equipment destined for a data center must be unpacked outside the data center.  If an exception is granted that allows equipment to be unpacked inside the data center, care must be taken to limit the introduction of contaminants into the airflow. HEPA vacuums must be used to clean up after the unpacking process.  No packing materials shall be left in the data center.

3.2.11    The contracted HVAC maintenance contractor will perform maintenance activities to the HVAC systems monthly or quarterly, based on site requirements.

## 3.3    Authorization and Access Requirements

3.3.1    Access to all UW-IT operated data centers and mission critical facilities must comply with both the "Data Centers and Mission Critical Facilities Access and Physical Security Policy" document and the "Data Centers and Mission Critical Facilities Access and Physical Security Procedures" document. Copies of these documents will be sent to all current UW-IT data centers and mission critical facilities users and provided to all new users. Copies may also be found at UW-IT's Service Catalog; http://depts.washington.edu/uwtscat/

## 3.4    Modifications and Changes

3.4.1    All modifications and changes within the UW data centers and mission critical facilities including but not limited to infrastructure modifications,

commissioning and decommissioning of equipment, scheduled preventive maintenance and emergency maintenance of equipment, and testing of back-up systems must be scheduled according to change management procedures (if applicable), and must be coordinated with the DCFM manager or data center planner. Please see page for contact information for DCFM.

3.4.2    All changes within the data centers and mission critical facilities are subject to approval of the DCFM manager and the associated units affected.

3.4.3    Any work performed within the data centers and mission critical facilities must be pre-approved by the DCFM manager or data center planner. It will be the responsibility of the DCFM manager or data center planner to provide written notification to the UW-IT Computer Operations data center team and/ or other stakeholders of these facilities by stating the hours of work, type of work being performed, and the names of the parties involved in the work.

3.4.4    No hardware, furniture, shelving or other materials may be removed or added to the data centers or other mission critical facilities without written request and approval of the DCFM manager or data center planner.

3.4.5    All space allocations within the data centers and mission critical facilities will be the responsibility of the DCFM manager or data center planner. All special projects must be coordinated with the DCFM manager.

3.4.6    All equipment must be rack-mountable. Exceptions must be approved by the DCFM manager or data center planner. Racks used in the data centers and mission critical facilities must be assigned by the DCFM manager or data center planner. Any exceptions must be approved by the DCFM manager.

3.4.7    Network copper cabling color standards are as follows: yellow for the front door connection, blue for the backdoor connection, and green for the managed network connection.

## 3.5    Decommissioned Equipment

3.5.1    Removal of all decommissioned equipment must be coordinated with the DCFM manager or data center planner. The data center planner will schedule a removal date and coordinate the equipment's disposition with the owner.

3.5.2     All decommissioned/ abandoned equipment will be removed from the data centers and mission critical facilities within 60 days of notification and surplused using the B&F process in place (UW-IT) or the process required by individual departments.

3.5.3     All decommissioned communications cabling--including voice, data and fiber cabling--must be removed from the data centers and mission critical facilities by the appropriate party within 60 days of notification that the surplus process has been completed.  Decommissioned cables are defined as cables that are abandoned or no longer to be used in the data centers or mission critical facilities.

## 3.6     Electrical Power Requirements

3.6.1     Only a DCFM-authorized electrical service provider may open or change any electrical panel or power distribution unit.  All power strip outlets will be configured off as a default. A customer must specify to DCFM how many outlets will be required for the installation.

3.6.2     Electrical cables under the raised floor or at a service connection may not be plugged in or unplugged by anyone other than DCFM or DCFM-authorized personnel.

3.6.3     Power outlets may only be used or installed with the approval of the DCFM manager.  DCFM staff is responsible for plugging in and unplugging equipment power cords under the raised floor or at a service connection as equipment is commissioned or decommissioned.  Cleaning equipment or tools used to perform authorized work in the data centers and mission critical facilities may only be plugged into wall sockets designated as "House Power."

3.6.4     All electrical cables within the data centers and mission critical facilities are installed for specific purposes; thus, no cables may be used without the approval of the DCFM manager or data center planner.

3.6.5     All electrical cables will be plenum rated flexible metallic sealtight conduit and must be dedicated to a specific location and equipped with a separate ground conductor. Request to use any other cable may be submitted to DCFM for approval prior to installation.

3.6.6     Electrical cable requirements for new equipment must be given to the DCFM manager or data center planner before implementation.  The DCFM manager or data center planner must coordinate with a DCFM-authorized electrical service provider for installation of new power sources.

3.6.7    Power strips that are not data center approved will not be used in the data centers and mission critical facilities.  The only exception to this will be in a case of an emergency situation that requires equipment to be brought into service before a permanent power source can be installed. In such an instance, the power strip must be tagged, dated and approved by the DCFM manager or data center planner and removed once a data center approved power strip is available.

3.6.8    No secondary uninterruptible power supplies (UPS's) are to be installed within the data centers. Requests for any secondary UPS must be in writing to the DCFM manager for determination and review.

**3.7    Documentation and Labeling**

3.7.1    Sufficient documentation must be maintained to facilitate the timely resolution of problems in the data centers and mission critical facilities.

3.7.2    All equipment and servers must be labeled with identification information. This identification will be legible and consistent for all data center and mission critical facilities.

3.7.3    All rack and power strip equipment must have labels affixed that identify the circuit and power distribution unit to which each is attached.

3.7.4    All main power feeder cables must be labeled and identified as to specific use, as well as the amperage, voltage, type, connector, grid location of either end (if applicable) and length of the cable.

3.7.5    Each branch circuit and device cable installed within the data centers and mission critical facilities must be labeled with its floor grid location (raised floor only), PDU and circuit number.  Identical labels must be affixed at each end of the cable or branch circuit.

3.7.6    When equipment is removed from the data centers and mission critical facilities, all pertinent documentation must be updated by DCFM.

3.7.7    All cables within the data centers and mission critical facilities will be labeled to identify them in a meaningful way for others to understand their use.

### 3.8    Equipment and Cables

3.8.1     Equipment, peripherals and associated cabling in the data centers and mission critical facilities must be installed in accordance with TIA 942, and in such a manner as to maximize management and the effectiveness of environmental equipment. *A color code for Ethernet cables* has been established: yellow for general access, blue for limited access, and green for management access. All cables will be tied or lashed down with either Velcro strips or appropriate string ties.

3.8.2     DCFM staff is responsible for all information technology (IT) and environmental equipment installed in UW-IT centrally managed data centers and mission critical facilities. DCFM is available to perform or contract out the installation of equipment. If a customer or his/her contractor is authorized by the DCFM manager to perform the installation, this installation will be inspected by the DCFM manager or his/her delegated data center planner. Inspections will determine if the installation is compliant with this document and possible other required compliances such as building code, electrical code and structural integrity. DCFM has the final approval for all installations and all discrepancies will be repaired, redone or replaced in a timely manner. Request for exceptions or appeals can be sent in writing to the DCFM manager for review and determination. If an impasse is reached, escalation to the Executive Director of Planning and Facilities will occur for a final determination.

3.8.3     All telecommunications cabling in the overhead conveyance system must be run by UW Network Services, DCFM or their contractors.  No other cabling may be run in the Network Services' tray system without the prior approval of the Network Services manager or DCFM manager. Exceptions will be cable trays physically attached to server cabinets for the sole purpose of running copper cables in and out of cabinets in a row. Copper cables will not traverse between rows.

3.8.4     All cables must run in an orderly manner; when turns are required they must be as near to 90 degrees as possible.  Cables may not be run diagonally in the sub-floor. Cables may not be run in cold aisles. Where under floor cable trays exist, all cables will be run in the cable tray and secured with Velcro strips to the copper cable side or fiber cable side depending on the cable type. Electrical and computer cables may run perpendicularly to one another.  Telecommunications cables may be run parallel; when cables cross paths, however, they must be run in a perpendicular manner.

3.8.5     All furniture items within the data centers and mission critical facilities, including desks, chairs, tables, and shelving and server cabinets, are the

responsibility of the DCFM manager.  Furniture items may not be added, removed or relocated without DCFM approval.

3.8.6     All contractors hired to perform work in the data centers and mission critical facilities, including electrical, mechanical and telecommunications contractors, must coordinate their work with the DCFM manager or data center planner.

3.8.7     All equipment deliveries to the data centers and mission critical facilities must be coordinated with the DCFM manager or data center planner to ensure proper receipt and storage.  Each unit ordering equipment will be responsible for notification and acceptance of the equipment.

**3.9      Environmental Cleanliness**

3.9.1     All data centers and mission critical facilities must receive an annual cleaning both above and below the raised floor (only in raised floor facilities). This will include: cleaning in and around the wiring under the floor; aggressive cleaning of the floor and floor tile; and dusting of the server racks, including the tops and non-disruptive open areas around the server racks. This work must be contracted to a qualified professional data center cleaning service.

3.9.2     It is the responsibility of the equipment owners to clean the surfaces of their equipment. This will be done at least twice a year. When more than twice a year cleaning is necessary the DCFM office will notify the equipment owner.

3.9.3     Weekly cleaning by the building janitorial service shall be on a site-by-site basis. All cleaning personnel must receive training from DCFM staff prior to any work.

3.9.4     Any garbage, packing materials or waste brought into the data centers and mission critical facilities by personnel, or produced as a result of work within the data centers and mission critical facilities, must be removed the same day from the data centers and mission critical facilities.

**4.0      Conduct of Authorized Users**

4.01      No food or drink is allowed within the data centers and mission critical facilities.

4.02      Authorized users may not tamper or interact with equipment or cabinets that are not assigned to them.

4.03     Customers who purchase shared server cabinets (co-habituating) will not tamper or interact with other customers' equipment housed in the same cabinet.  If a major reconfiguration is required by either co-habituating customer, the work must be coordinated with, and approved by, the UW Information Technology's Data Center Planner.