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
I. Policy Statement

University of Washington Information Technology (UW-IT) is responsible for ensuring the safe and efficient operation of all UW-IT centrally managed data centers and other mission critical support facilities for the University of Washington. These facilities are to be operated in such a way as to protect the environment around all data centers and other mission critical facilities but specifically the physical security access, fire alarms/suppression, heating, ventilation and air conditioning (HVAC), uninterruptible power supplies (UPS), campus backbone connectivity, and a number of other elements meant to maintain the required environment for information technology (IT) equipment. It is important that all personnel (staff, co-location customers and contractors) understand and abide by this policy while working in, or otherwise making use of, UW centrally managed data center facilities and other mission critical support facilities.

II. Purpose

The purpose of this policy is to maintain the data center environment by:

- Keeping the data center safe for all personnel
- Allowing entry to authorized individuals only
- Ensuring the air flow, temperature and humidity remains constant and within IT equipment design
- Constantly monitoring electrical power to predict possible overload conditions and conform to all governing codes
- Maintaining the data center as a “clean room” type of environment, with no expended equipment or materials stored in data center spaces

The supporting attached documents provide the guidelines and describe which types of activities may be performed inside the data centers and mission critical spaces, and which must be performed outside the spaces. They also describe moving equipment in and out of these spaces.

III. Application

The areas in which this policy applies include the following:

- The UW data centers at 4545, Academic Computing Center (ACC), UW Tower C-2, and Sabey B
- Remote data centers and co-location centers at Tierpoint, Pittock, and the Westin Building
• All Network Routing Hubs located in various academic and residence buildings across UW Seattle, UW Bothell, and UW Tacoma.

The activities to which this policy applies include but are not limited to:

• Periodic preventative maintenance
• Equipment installation and de-installation
• Equipment firmware and software upgrades
• Users interfacing with owned equipment
• Construction

This policy applies to all University of Washington staff, faculty, students, and visitors and includes those in partnership with the UW through affiliations, as well as recognized vendors and/or those operating under contractual obligations.

Failure to comply with this policy will constitute grounds for loss of access, or the ability to work independently within any data center or mission critical facilities.

Attachment A:

UW Information Technology Data Center and Mission Critical Facilities Operations Procedures