WEBER STATE UNIVERSITY Information Technology	**Data Centers** Standards and Guidelines	Revision Date: 31 Oct 2018

I. PURPOSE

Weber State University (WSU) Data Centers provide the environment for physical security, fire protection, uninterrupted power supply, emergency generator connections, and campus network backbone connections. These Data Centers allow WSU to have high availability for core enterprise systems as well as academic services. The Data Centers are physically secured by proximity door locks. In addition, security cameras provide 24-hour video surveillance.

II. REFERENCES

A. PPM 10-1, Information Security Policy

B. PPM 10-2, Acceptable Use Policy

III. DEFINITIONS

A. Academic and Research Data Center - Room 213 in the Technical Education building, 1465 Edvalson Street, Ogden, Utah 84408.

B. Authorized Staff - An individual given authorized access to a Data Center based on the need to perform their job in one of the Data Centers. These individuals may need to work on the following systems, including, but not limited to, environmental, security, fire alarm/suppression, power, network and computer systems.

C. Authorized Vendor - All non-University employees who, through contractual arrangement and appropriate approvals, have access to the Data Centers.

D. Data Center - A designated location where hardware, software and data are co-located for use by WSU in the fulfillment of its mission as an institution of higher education.

E. Data Center Employee(s) - A Data Center employee(s) is defined as a Network Engineer, System Engineer or other personnel as designated by the Data Center Steward, whose day-to-day activities involve managing and monitoring the equipment in the Data Centers.

F. Data Center Steward- Data Center Employee directly responsible for the Data Centers.

G. Davis Data Center - Room 120 in Building D2, 2750 N. University Park Boulevard, Layton, Utah 84041-9099.

H. Hurst Data Center - Room 007 in the Hurst Center, 1256 Village Drive, Ogden, Utah 84408.

I. Production Data Center - Room 212 in the Technical Education building, 1465 Edvalson Street, Ogden, Utah 84408.

J. Richfield Data Center - Is a leased space located at 350 South 900 West, Richfield, UT 84701.

K. Visitor - Anyone who is not a Data Center employee, an Authorized Staff member, or Authorized Vendor is considered a visitor.

IV. STANDARDS AND GUIDELINES

A. Rules of Conduct

In order to maintain a clean room environment and allow all work performed within the Data Centers to be carried out as efficiently as possible, all persons working within the Data Centers must adhere to the following rules of conduct:

1. All work areas must be kept clean and free of debris. Upon completion of any work in the Data Centers, personnel performing the work should ensure they have left the area as clean as it was before their work began.

2. All rack enclosures should be kept neat and free of manuals, installation media, and extra parts. These items shall not be stored in the Data Centers.

3. Doors on all racks should remain closed at all times except during performed work.

4. Cables should never be strung outside of rack enclosures. Cabling between rack enclosures of adjacent racks is accepted provided sufficient pass-through chassis are in place.

5. Under no circumstances should food or beverage, of any kind, be brought into the Data Centers.

6. All packing material must be removed from computer equipment/components before equipment/components are moved into the Data Centers.

7. No cleaning supply is allowed within the Data Centers without prior approval. This includes water.

8. No cutting of any material (pipes, floor tiles, etc.) shall be performed inside the Data Centers, unless special arrangements are made.

9. No hazardous materials are allowed in the Data Centers without permission from the Data Center Steward.

10. Visitors to the Production Data Center and Academic and Research Data Center are not permitted to lift floor tiles, touch any installed equipment, or touch any installed cables, except as necessary for their work.

B. Access

1. All personnel who access the Data Centers must have proper authorization. Individuals without proper authorization will be considered a visitor.

2. Authorized access will be reviewed on a semester basis to ensure unnecessary access is removed.

3. The Production Data Center entry log will be reviewed on a semester basis for completeness.

4. The Data Centers will be monitored through live video cameras and other services as needed.

C. Levels of Access

1. Visitor Access - Visitors to a Data Center must be accompanied by either a Data Center employee or other authorized staff member at all times while in a Data Center. Visitors will be required to comply with the Data Center standards and guidelines.

2. Authorized Vendor Access - With proper notification and approval, vendors will be allowed into the Data Centers to perform scheduled maintenance or repair work.

3. Production Data Center Access - Electronic access is available to the Data Center on a 7x24 basis for authorized card holders. Office areas (TE-209 – TE-211F) adjacent to the Production Data Center are not part of the Production Data Center. Log entries are not required for entry to these offices. To comply with PCI Data Security Standards section 7, visitors to the Production Data Center are required to log in/out when entering/exiting the Production Data Center and the purpose of the visit must be documented. Visitors must wear a visitor's badge at all times in the Production Data Center. The accompanying Data Center Employee is responsible for ensuring the visitor is logged in and receives a visitor’s badge.

4. Academic and Research Data Center Access - Electronic access is available to the Data Center on a 7x24 basis for authorized card holders. Office areas (TE-209 – TE-211F) adjacent to the Academic and Research Data Center are not part of the Academic and Research Data Center. Log entries are not required for entry to these offices. PCI Data may not be stored in the Academic and Research Data Center.

5. Davis Campus Data Center - Electronic access is available to the Data Center on a 7x24 basis for authorized card holders.

6. Hurst Data Center - Electronic access is available to the Data Center on a 7x24 basis for authorized card holders.

7. Richfield Data Center - Access is controlled by the Richfield Data Center. Contact them for access.

D. Doors

Doors must remain locked at all times and may only be temporarily opened for periods not to exceed the minimum necessary in order to:

1. Allow officially approved entrance and exit of authorized individuals.

2. Permit the transfer of supplies/equipment as needed.

E. Equipment Requirements

In an effort to maximize security and minimize disruptions, the following applies to all equipment housed in the Data Centers.

1. Schedule a meeting with the Data Center Steward to initiate the move of equipment to the Academic and Research or Production Data Centers.

2. Be rack-mountable and housed in standard racks using standard rack configurations. Special considerations can be made for equipment that does not meet the requirements at the discretion the Data Center Steward.

3. Changes to Power Distribution Units and power whips to properly supply the new equipment is at the expense of the organization installing the equipment. Modification must be approved by the Data Center Steward and be performed by qualified personnel.

Servers

Servers must be configured with remote management technology. The remote management must allow for console access to the server. This access must include remote GUI capabilities. Some systems require higher licensing to allow GUI access. Remote management access should be configured by using Active Directory groups and not local accounts when possible.

Servers must be configured with Dual NICs. These are preferably 10Gb and support TCP/IP offloading. Some servers will need NICs depending on the type of load. Systems running iSCSI should have dedicated NICs for that purpose. NICs must be configured in a redundant manner.

Servers should have power supplies that use 110-240V not just 110V or 240V. Power supplies must be redundant.

Servers should be located in an appropriate Data Center. These Data Centers allow for redundant power, sufficient cooling, physical security, and redundant networking.

Servers must have a minimum of a 5-year warranty, preferably longer when possible. Dell allows some servers to have a 7-year warranty. Our current VMware servers have 7-year warranties. Selection of the level of support on the warranty depends on a few factors. If the service the servers provides is highly redundant, a next business day warranty may be ok to use. If the system is critical and is not redundant then a 4-hour response with parts and technician would be acceptable. Other non-critical servers may select support levels as appropriate.

Servers must be joined to Active Directory and use AD groups to assign rights. Local accounts (except the local Administrator or root) should be avoided where possible.

Storage

Storage connectivity should be redundant when using Fiber channel or Ethernet Networking (iSCSI or NAS).

Power supplies should be redundant and should run 110-240v power.

Warranty should be 3-5 years or longer when purchasing new SAN and support should have 4 hour or less response time.

When adding trays/disks, consideration should be made to have the warranty renewal date and remaining time set to the same as the rest of the storage devices in that collection.

Disks, power supplies, and controllers should not be swappable.

Upgrades to code should be non-disrupting.

Academic Data Center

The IT Division encourages that the equipment in the Academic Data Center follow the guide of redundancy for power and networking but it is not required. It is strongly discouraged to use equipment that is not rack mountable. The type of data being used and security is the responsibility of the owner and must comply with University policy (PPM 10-1 and PPM 10-2).

F. Requesting Access to the Academic and Research Data Centers
Access requests for the Academic and Research Data Centers will be considered on a case by case basis. Contact the Data Center Steward for this access. Notification will be provided via email if the request has been approved or denied.

G. Requesting Access to the Production Data Center

PCI compliance requires adherence to PCI Data Security Standards Version 1.2.1 sections 7-1 and 7-2. Access requests for the Production Data Center will be considered on a case by case basis. Contact the Data Center Steward for this access. You will be notified via email once your request has been approved or denied.

H. Steel Keys

Access to the Data Centers will be limited to Electronic access only unless there is an emergency. A steel key will be kept in a secure location where the Data Center Steward can grant access in case of emergency. This location will be made known to proper Data Center Employees.

Academic Data Center

The Academic Data Center uses electronic locks to control physical access to the room.

I. Tours
Tours may be scheduled by contacting the Data Center Steward.