Introduction
The following guidelines regulate the activities in the Cal Poly Pomona data centers (referred to as “data center” in this document). These guidelines are intended to ensure the safety and security of individuals and equipment in a data center. Data centers are critical spaces for the campus and violation of these rules places the services provided to the campus at risk of outage. Extreme care should be exercised while working within a data center to prevent unplanned outages.

This document consists of common guidelines that apply to all data centers as well as data center specific guidelines which can be modified by the designated party responsible for a data center. All changes to the data center specific guidelines section contained within this document should be submitted to the Director of Systems and Data Centers for approval.

Applicable policies and laws
The current Appropriate Use Policy for Information Technology applies to all data centers. Additionally, all data centers must comply with Integrated California State University Administrative Manual (ICSUAM) §8080 (http://www.calstate.edu/icsuam/sections/8000/index.shtml) and State Administrative Manual (SAM) §5330 (http://sam.dgs.ca.gov/TOC/5300.aspx).

Scope
The guidelines apply to all persons accessing a data center (including, but not limited to employees, auxiliaries, students, contractors, visitors, and vendors.) For purposes of this document, “data centers” are defined as spaces housing computer systems that are providing remote services to multiple end-users. Storage rooms attached to the data center are not included in the scope of this guideline.

Common Guidelines
The purpose of this section is to provide a baseline for the management of campus data centers. This section applies to all campus data centers. These guidelines are intended to insure that the data center environment is secure, reliable, and safe.

General
1. Food and drink is not permitted in the data center at any time.
2. Combustible and flammable material (including, but not limited to cardboard, wood, plastic, and paper goods) should not be left in the data center.
3. For safety reasons, all persons entering the data center should be wearing closed toed shoes.
4. When work requires the removal of floor tiles, eye protection should be worn. Also, floor tiles should remain open only while work is being performed in the immediate vicinity of the tile. If the area is to be left unattended, the floor tile must be replaced.

5. Each data center should have a person designated as a responsible party. The responsible party should ensure that these guidelines are adhered to and may request data center specific guidelines.

6. All people with ongoing access to a data center should receive training regarding the specific guidelines for each data center that they can access. The responsible party for each data center should maintain a list, including signatures, of everyone who has received training.

7. Each data center should have fire protection mechanisms.

8. Backup power should be available to power, at a minimum, the server and networking equipment in the room.

9. An environment monitoring system should be in place to monitor, at a minimum, temperature and humidity.

Physical Security

Campus Data Centers are Limited Access Areas based on CSU’s Policy Section 8080 Physical Security Standard. Campus and/or departmental servers storing Level 1 Confidential data, as defined by the CSU Information Security Standards, should be located in a physically controlled campus Data Center.

1. Access to the data center should be kept to a minimum.

2. Security cameras must in use in the data center. All cameras should recorded and may be reviewed by security personnel.

3. Doors leading to the data center must be secured using a card access system where the identity of each individual unlocking the door should be logged.

4. Doors leading to the data center should not be propped open. The doors are a fire barrier and propping the doors open for extended periods of time is a violation of fire code and poses a security risk.

Networking

1. All networking equipment, including switching, routing, and wireless equipment must be supplied, installed, and maintained by the IT Networks and Telecommunications department.

2. Installation of packet capture devices requires approval of the Director of Networks and Telecommunications. The exception to this is capture software that is only capable of capturing traffic to/from the host on which it is installed.

Data Center Specific Guidelines

 Applies to: 

The guidelines in this section apply to all data centers, unless amended set of guidelines have been submitted to and approved by the Director of Systems and Data Centers. Each data center owner may customize this section to fit the specific needs of their respective data center(s). The items in this section may reinforce the items in the “Common Guidelines” section, define the operational practices employed in the data center, or define the appropriate usage of the affected data center.

For questions or concerns, contact David Drivdahl – davidd@cpp.edu 909-979-6372
Last Modified: 4/3/2015
General
1. All work areas must be kept clean and free of debris. Upon completion of any work in the data center, persons performing the work should ensure they have left the area as clean as it was before their work began.
2. Doors on the equipment racks should be in place and closed when work is not being performed within that rack.
3. The data center is not to be used as storage. This includes yet-to-be-deployed servers, switches, storage, or other IT equipment not in use. The data center floor should be clear to allow access to floor tiles for cleaning and for access to the sub-floor.
4. Cardboard entering the data center should be kept to a minimum. Cardboard boxes bring in dust and dirt and should stay out of the data center area. Though not practical in all situations, the preference is to unbox new equipment in an adjacent room rather than in the data center.
5. Palletized equipment is never permitted in the data center. Exceptions to this item requires approval from the Director of Systems and Data Centers.

Physical Security
1. Only those with a specific need for access should be granted access and those with access should only enter the data center when required to perform a given task.
2. Personally assigned access cards should not be shared with other individuals. Checkout cards may be available and should be assigned to the person using the card at the time.

Equipment Installation
1. All equipment housed in the data center (including, but not limited to servers, networking equipment, and storage) will be rack mounted within designated racks. Floor standing equipment outside of server racks is not permitted.
2. Cable wrapping, wire management, and/or Velcro must be used to organize cabling in a rack.
3. Each rack, other than in colo, should have a designated “owning” department.
4. The installation of equipment or cabling in a given server rack will be done solely by, or under the direction of the owning department of the rack.
5. All new racks and power distribution within the data center will be of the current standard in use at the time. Exceptions to this may be made for equipment shipped in vendor supplied racks at the discretion of the Director of Systems and Data Center.
6. Servers should be labeled to identify the host name assigned to the server. All equipment installed in the data center should be added to Rack Monkey, including the serial number, host name, FQDN, CPK number, and purchase date at a minimum.
7. Excess cabling should be kept to a minimum and patch cables and power cables should be of the shortest length required.

Equipment Removal
1. Servers being decommissioned should be powered off, unplugged from the network, removed from the rack, and securely wiped.
2. The removal of equipment or cabling in a given server rack will be done solely by, or under the direction of the owning department of the rack.
3. Servers should not leave the data center without having been appropriately and securely wiped.

For questions or concerns, contact David Drivdahl – davidd@cpp.edu 909-979-6372
Last Modified: 4/3/2015
4. When servers are removed from a rack, blanking panels should be used to fill in the opening left by the server.
5. Unused cabling should be removed from the racks and properly stored in an appropriate location.
6. After removal from the rack, all equipment should be marked as “decommissioned” in Rack Monkey.
7. Equipment should be removed from the data center promptly after the equipment has been securely wiped (where applicable) and removed from the racks.

Approvals

Data Center Specific Amendments
This section is to be completed when amendments to the data center specific guidelines are requested by the designated responsible party.

Requested by: ____________________________ Date: ____________________________

Approved by: ____________________________ Date: ____________________________

Director of Systems and Data Center

Guideline Approval

______________
Vice President & CIO John McGuthry
California State Polytechnic University, Pomona