COUNTY OF SAN MATEO

Data Center Policy

Policy Updated: 05/21/2018

Overview

The security of the equipment and data in the County data centers is vitally important to the daily functioning of San Mateo County. Every component of the County's network and communications systems, including the data that is stored and transmitted, must be protected and preserved.

The data center is a restricted area that may only be used to conduct authorized business for the County.

Policy Purpose

The purpose of this policy is to restrict entry and to apply stringent use behaviors to authorized personnel using the data centers. Additionally, this policy serves to establish minimum requirements for data center safety and cleanliness.

Scope

This policy addresses the use and maintenance of the data center and applies to anyone (collectively, "users") accessing and using the data center.

Policy

Data Center Access

A. Any user requiring access shall be submitted for authorization through a ServiceNow ticket request, with appropriate written justification by the individual's manager.

B. The ServiceNow ticket request shall be submitted for approval by the Chief Information Officer (CIO) or his/her designee.

C. Once granted authorization for entry, all authorized users shall enter and leave through the main entrance of the data center.

   1. Authorized users shall only enter the Data Center to perform tasks that cannot be performed remotely.
   2. All authorized users must log-in upon entering into the datacenter as well as log out upon leaving.
      - a. The log will be audited periodically for compliance.

D. The data center access doors must remain closed and locked at all times.

E. All non-County employees must always be escorted by the Chief Information Officer (CIO) or his/her designee or authorized user while in the data center.

F. No tours of the data center shall be permitted without the written approval of the Chief Information Officer (CIO) or his/her designee.

G. No camera or photographic equipment shall be allowed within the data center without the written approval of the Chief Information Officer (CIO) or his/her designee.

H. Users shall not access, tamper, or interfere with any equipment they are not directly responsible for or authorized to do so.

I. Users shall report any violations of this policy or safety issues to the Chief Information Officer (CIO) or his/her designee or the ISD Service Desk.

J. Cameras may monitor the Data Centers at times; therefore, the activities of all individuals in the Data Centers may be recorded.

Safety

A. Every effort must be made to ensure personal safety in the data center.
    1. All personnel who work in the data center shall be annually trained on local safety and fire procedures for each room. This training shall be performed by the Chief Information Officer (CIO) or his/her designee or a designated individual.
    2. All personnel shall evacuate, without delay, when an evacuation is called either verbally or by instrument (i.e. alarm, light signal).

B. Any posted signs, placards or verbal and written instructions must be followed.

C. No cables are to be run on top of the floor at any time.

D. Missing floor tiles shall be adequately marked.

E. All boxes and debris shall not be left unattended and must be promptly removed.

Environment

A. Air conditioning and air quality shall be maintained within the acknowledged data center standards in accordance with all OSHA and CAL-OSHA regulations.

B. Humidity and temperature levels in the data center shall be maintained at ASHRE and/or TIA standards.
    1. Only authorized personnel shall perform maintenance activities to the HVAC systems on an as-needed basis with notice through the ISD Change Management Process.

C. All tile alterations shall be approved and coordinated by the Chief Information Officer (CIO) or his/her designee.
    1. In the event that holes are to be cut in the floor panels to accommodate new equipment, the floor panel shall be removed from the data center.
        a. If the panel cannot be removed from the data center, an environment appropriate vacuum must be used to capture the dust particles

created by the sawing action both above and below the raised floor surface.

2. The number of tiles pulled shall be kept to a minimum and all floor tiles shall be returned to the position from which they were removed.
   a. No holes shall be left exposed; cones and safety tape shall be used to cordon off the open space.
   b. Additional vents, grilles, or perforated tiles shall not be added without coordination and approval of the Chief Information Officer (CIO) or his/her designee.

3. All holes in the walls or ceiling shall not be left exposed or unsealed and must be properly sealed to meet fire code.
   a. If a wall is drilled for a cable, that hole must be sealed to meet fire code.

D. No food or drink shall be allowed in the data center at any time.

E. Ammoniated or chlorinated products shall not be allowed in the data center.
   1. Industrial cleaning liquids/fluids shall not be left in the data center unattended.
   2. Combustible items are strictly prohibited.

F. New equipment for the data center should be unpacked outside of the data center.
   1. No packing materials and/or boxes shall be left in the data center.

Electrical Installation

A. Electrical Power in the data center shall comply with accepted standards as specified by IEEE STD 1100-1999 (Emerald Book) and local and national electrical codes for data centers and commercial buildings TIA 942 and 607.
   1. Only authorized personnel shall open or change any power panel, UPS, or power distribution unit.
   2. All power cables shall be dedicated and equipped with isolation ground within the raised floor areas.

B. Electricians, authorized by the Chief Information Officer (CIO) or his/her designee, shall perform all modifications and testing to electrical service.

C. No power outlets or power cables shall be used or installed without the approval of the Chief Information Officer (CIO) or his/her designee; requests must be made through ServiceNow.
   1. Primary source power cable requirements for new equipment shall be given to the Chief Information Officer (CIO) or his/her designee before implementation.
   2. All power cables must be labeled and documented as noted on this policy.

D. Power strips shall not be used in the data center except:

a. In cases of emergency installations where equipment must be brought into service before the permanent power source can be installed. If used in this manner, the power strip must be tagged, dated and approved by the Chief Information Officer (CIO) or his/her designee.
b. For certain types of telecommunications equipment where power strips are deemed the preferred means of supplying power and such arrangement is approved by the Chief Information Officer (CIO) or his/her designee.

E. No radios or other non-computer related equipment shall be plugged into any dedicated circuit or equipment without the approval of the Chief Information Officer (CIO) or his/her designee.

F. Consumer rated computing equipment installation and use must be approved by the Chief Information Officer (CIO) or his/her designee prior to installation.
   1. Consumer rated equipment found to be operated without approval may be disconnected and powered off without warning.

Change Management

A. All modifications and changes within the data center shall be managed as specified in the Change Management Policy and shall be subject to the approval of the Chief Information Officer (CIO) or his/her designee.

B. No hardware, software, furniture, shelving or other materials shall be removed or added to the data center without prior approval of the Chief Information Officer (CIO) or his/her designee.

C. All space allocations within the data center shall be the responsibility of the Chief Information Officer (CIO) or his/her designee.

D. All equipment installed must be rack mountable, desktop/consumer appliances (PC's, NAS storage, and external drives) and accessories are not appropriate and not permitted.

E. Peripheral devices, for example, KVM switches, monitors, keyboards, etc., shall require approval by the Chief Information Officer (CIO) or his/her designee prior to installation.

Installation

A. All non-bus and tag cables shall be installed with an overhead cable conveyance system designated by ISD.

B. All cable runs shall be run in an orderly manner and when turns are required, all turns shall be as near to 90 degrees as possible.
   1. No cables shall run diagonally in the sub-floor without prior approval.
   2. Electrical and computer cables must run perpendicularly.
   3. Telecommunications cables may be run parallel when industry specifications are met, but when cables cross paths they shall do so in a

perpendicular manner.

C. All equipment deliveries to the data center shall be coordinated with the Chief Information Officer (CIO) or his/her designee to ensure proper receipt and storage.
D. All equipment installed/placed in the data center shall be included in the Master Data Center Inventory.

Equipment Security

A. All computer cabinets and doors shall remain closed and locked (as applicable) unless being serviced.

B. Locked computer cabinets are to be approved by the Chief Information Officer (CIO) or his/her designee.
    1. Computer cabinets that are locked must have access keys and/or combinations readily available to data center staff in the event of emergencies.

Documentation

A. All equipment should be labeled on the front panels with identification information.
    1. All equipment shall have a label affixed identifying the power distribution unit and the main power panel to which it is attached.
    2. All storage cabinets and shelves shall be labeled with the owner and local contact information.

B. Each piece of equipment shall have a log to record changes, vendor visits, etc. The written log shall be maintained by the Chief Information Officer (CIO) or his/her designee.

C. All power cables shall be labeled and identified for its specific use and identified by its amperage, voltage, type connector and length of cable.
    1. All device-to-device cables installed within the data center shall be labeled, at both ends, to identify their use and/or purpose.

D. When equipment is removed from the data center, the request must be made through ServiceNow to the Chief Information Officer (CIO) or his/her designee and the written log, maintained by the Data Center Manager, must be updated.

Decommissioned Equipment

A. All decommissioned equipment shall be removed from the data center within sixty (60) days.
    1. The Chief Information Officer (CIO) or his/her designee shall be notified in writing to remove decommissioned items from the Master Data Center Inventory.

2. A yearly audit of data center contents shall be performed to verify the Master Data Center Inventory.

B. Decommissioned cables shall be defined as cables that are abandoned and shall no longer be used in the data center.

C. Storing of any unused or decommissioned equipment asset is prohibited; any such items found in the data center shall be removed and disposed accordingly.

Responsibility

Oversight of the data centers is the responsibility of the Chief Information Officer (CIO) or his/her designee. The Data Center Manager shall be responsible for the maintenance of the Master Data Center Inventory.

Policy Enforcement

Violations will be investigated and may result in disciplinary action. The County has other policies that address specific areas of this policy in further detail including Change Management Policy.

Revision History

Effective Date	**Changes Made**
07/19/2005	Policy established
05/21/2018	Policy updated