INFORMATION SECURITY-PHYSICAL SECURITY

I. PURPOSE AND SCOPE

All Yosemite Community College District (YCCD) information systems and resources must be properly protected from potential physical and environmental threats to ensure the confidentiality, integrity, and availability of the data contained within. This Administrative Regulation provides describes physical access methods, visitors, data center security and media disposal.

This is one of a series of information security Administrative Regulations maintained by the District Information Technology Services (ITS) department designed to protect YCCD information systems.

II. PHYSICAL SECURITY

All YCCD technology locations will employ security control measures to prevent unauthorized physical access, damage, or interference to the premises and information.

1. Physical Security Responsibilities

The Campus Security Department manages perimeter security for the colleges and District offices. This group has physical keys to buildings and a master badge allowing access to all facilities.

District ITS is responsible for the data center in Modesto. Card and Key access to the District ITS-specific doors and data center are administered by District ITS and Campus Security Department.

District ITS personnel at the Columbia College Campus are responsible for the backup data center located at the Columbia College Campus. key access to specific doors and data center are to be approved by District ITS.

2. Access Cards and Visitors to YCCD Data Centers

District ITS offices and secure areas are protected by entry controls designed to allow only authorized personnel to obtain building access. Authorized individuals may be issued an access card that enables electronic access to exterior doors and authorized internal doors. Additional authorization may be required for access to some doors.

District ITS visitors must be escorted by YCCD personnel.

3. Data Center Access

The District ITS data centers are critical processing facilities that must be protected by defined security perimeters with appropriate security access controls.

All persons who do not have an access card that require access to the data center must be escorted by an employee whose badge is authorized to access the data center. Approval is required from the District ITS management prior to any access to this area.

An authorized District ITS employee is responsible for making sure that visitors entering a YCCD data center are properly logged. It is mandatory that all visitors check in with District ITS, and visitors to a YCCD data center must sign in and sign out with District ITS so that the entry and purpose of the visit can be tracked for auditing and security purposes.

For data center visitors, the reception log must note the Name, Date, Company, Purpose of Visit, any escorting employee, and both sign-in and sign-out times. Spot checks of the log may be performed by District ITS and matched against the audit trail of door accesses from the access card system. Visitor logs must be retained for three months.

For audit and compliance purposes, the District ITS Management will review those authorized to access a YCCD data center at least quarterly to ensure that privileges of employees or vendors who no longer need access to the data center have been removed. Records of these reviews will be maintained for audit purposes.

4. Equipment Maintenance and Environmentals

District ITS must ensure that all utilities (e.g. UPS, generator) and other equipment are correctly maintained, security isolated and monitored in accordance with manufacturer specifications to ensure the availability, integrity and confidentiality of information contained within it.

The data center has Inergen fire suppression, HVAC units, environmental protection, redundant UPS systems, and exterior backup diesel generator.

Only authorized maintenance personnel are allowed to perform repairs. All repairs or service work must be documented. Documentation records must be maintained by District ITS.

Computer room personnel must be trained in the use of any automatic fire suppression systems, the use of portable fire extinguishers and in the proper response to smoke and fire alarms. Smoking, drinking and eating in computer processing rooms is prohibited.

5. Media Disposal and Destruction

   District ITS must ensure that electronic information storage devices (e.g., hard drives, tapes, USB sticks, removable hard disks, floppy disks, CD's and DVD's) are disposed of in a manner commensurate with their information classification per YCCD Board Policy 3310.

   All electronic storage devices must be electronically wiped by a process such that data on the storage device cannot be recovered by individuals and/or technology.

   External firms responsible for disposing of any type of YCCD information must be held to any standards specified by contract. This includes confidentiality agreements and adequate security controls.

   All Data Owners must ensure that media containing *Restricted* data is destroyed when it is no longer needed for business or legal reasons per YCCD Board Policy 6-8065.

   Employees must use proper destruction methods when disposing of YCCD information. Paper copies of sensitive information must be shredded or incinerated. Users of the information are responsible for disposing of it in secure disposal containers or using another proper destruction method per YCCD Board Policy 3310.

6. Payment Card Industry (PCI) Requirements

   The following additional physical security controls are specific to areas that may contain systems or media that are in-scope for credit card data processing or storage:

   - Video cameras must be used to monitor individual physical access to areas where credit card data is stored, processed, or transmitted.

   - Physical access to publicly accessible network jacks must be restricted. Network ports for visitors should not be enabled unless network access is explicitly authorized by appropriate IT department.

   - Physical access to wireless access points, gateways, handheld devices, networking/communications hardware, and telecommunication lines must be restricted to those authorized to work with cardholder data.

   - All media containing cardholder data must be physically secured. Media back-ups must be stored in a secure location, preferably an off-site facility, such as an alternate or back-up site, or a commercial storage facility. These locations must be reviewed at least annually.

- Internal or external distribution of any kind of media must be strictly controlled.
    - Media containing cardholder data must be classified so sensitivity of the data can be determined.
    - Secure couriers or other delivery methods that can be accurately tracked must be used.
    - Appropriate ITS management must approve any and all media that is moved from a secured area (especially when media is distributed to individuals).

- Storage and accessibility of media must be strictly controlled. Inventory logs of media must be maintained and inventoried at least annually.

- Media containing credit card data must be destroyed when it is no longer needed for business or legal reasons per YCCD Board policies 3310 and 6-8065.
    - Shred, incinerate, or pulp hardcopy materials so that cardholder data cannot be reconstructed.
    - Render cardholder data on electronic media unrecoverable so that cardholder data cannot be reconstructed.