ADMINISTRATIVE REGULATION 3728

SOUTH ORANGE COUNTY COMMUNITY COLLEGE DISTRICT

BUSINESS

INFORMATION SECURITY-PHYSICAL SECURITY

I. PURPOSE AND SCOPE

All South Orange Community College District (SOCCCD) information systems 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 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 (IT) department designed to protect SOCCCD information systems.

Please refer to *AR-3725–Information Security Program Overview* for applicability of assets, application to employees, and external parties.

II. PHYSICAL SECURITY

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

A. Physical Security Responsibilities

1. The Campus Police departments manage perimeter security for the colleges and District offices. This group has physical keys to buildings and a master badge allowing access to all facilities.
2. District IT is responsible for the data center in Mission Viejo. District IT administers card access to the District IT-specific doors and data center.
3. IVC Technology Services is responsible for the data center at IVC and ATEP Campus. Card and key access to specific doors and data center are to be approved by the IVC Technology Director.
4. Saddleback Technology Services is responsible for the data center at the Saddleback Campus. Card and key access to specific doors and data center are to be approved by the Saddleback Technology Director.

B. Access Cards and Visitors to SOCCCD Data Centers

District IT 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 Employee, Temporary, or Visitor badge that enables electronic access to exterior doors and

authorized internal doors. Additional authorization may be required for access to some doors.

Employees and visitors to SOCCCD District IT facilities must clearly display ID badges at all times. Employees must be alert for unknown persons without badges, or employees not displaying badges.

District IT visitors must be provided with a badge or keycard that expires and identifies the person as a non-employee. SOCCCD personnel must escort visitors. Visitors may be required to surrender badges after leaving the facility or at the date of expiration.

C. Data Center Access

The District IT and College 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 a badge 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 IT and/or college management prior to any access to this area.

An authorized District IT employee is responsible for making sure that visitors entering a SOCCCD data center are properly logged. It is mandatory that all visitors check in with District IT reception or college Technology departments, and visitors to a SOCCCD data center must sign in and sign out with District IT and/or college Technology Department reception 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 IT and/or college Technology departments and matched against the audit trail of door accesses from the keycard badging system. Reception area visitor logs must be retained for three months.

For audit and compliance purposes, the District IT management and/or college Technology department management will review those authorized to access a SOCCCD 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.

D. Equipment Maintenance and Environmental

District IT and college Technology departments must ensure that all utilities (e.g. UPS, generator) and other equipment is monitored in accordance with manufacturer specifications and correctly maintained to ensure the availability, integrity and confidentiality of information contained within it.

The typical data center should have dry pipe water 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 IT and/or college Technology departments.

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.

E. Media Disposal and Destruction

District IT and/or College Technology Departments must ensure that electronic information storage devices (e.g., hard drives (spinning, ssd, m.2, etc.), tapes, USB sticks, removable hard disks, floppy disks, CD's and DVD's) are disposed of in a manner commensurate with their information classification.

All electronic storage devices must be 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 SOCCCD 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.

Employees must use proper destruction methods when disposing of SOCCCD 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.

F. 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:

1. Video cameras must be used to monitor individual physical access to areas where credit card data is stored, processed, or transmitted.
2. 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 District IT or college Technology departments.
3. 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.
4. 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.

5. Internal or external distribution of any kind of media must be strictly controlled.
    a) Media containing cardholder data must be classified so sensitivity of the data can be determined.
    b) Secure couriers or other delivery methods that can be accurately tracked must be used.
    c) Appropriate IT management must approve any and all media that is moved from a secured area (especially when media is distributed to individuals).
6. Storage and accessibility of media must be strictly controlled. Inventory logs of media must be maintained and inventoried at least annually.
7. Media containing credit card data must be destroyed when it is no longer needed for business or legal reasons.
    a) Shred, incinerate, or pulp hardcopy materials so that cardholder data cannot be reconstructed.
    b) Render cardholder data on electronic media unrecoverable so that cardholder data cannot be reconstructed.

G. Policy Enforcement

Any person found to have violated this policy, intentionally or unintentionally, may be subject to disciplinary action, up to and including loss of access rights or termination of employment.

References:

NIST SP 800-53 Rev. 4 CA-7, PE-3, PE-6, PE-20
HIPAA Security Rule 45 C.F.R. §§ 164.310(a)(2)(ii), 164.310(a)(2)(iii)
PCI DSS Requirements and Security Assessment Procedures: https://www.pcisecuritystandards.org/documents/PCI_DSS_v3.pdf
PCI DSS Quick Reference Guide Version 3.0 https://www.pcisecuritystandards.org/documents/PCIDSS_QRGv3.pdf