# ADMINISTRATIVE REGULATION 3727

**COLLEGE OF THE REDWOODS**

## INFORMATION SECURITY-PHYSICAL SECURITY

### 1.0 Purpose and Scope

All **COLLEGE OF THE REDWOODS** 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 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 (IT) department designed to protect the district’s information systems.

### 2.0 Physical Security

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

#### 2.1 Physical Security Responsibilities

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.

District IT is responsible for the data center. Card access to the District IT-specific doors and data center are administered by District IT.

#### 2.2 Access Cards and Visitors to District 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.

Visitors to 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. Visitors must sign in and out daily, and be escorted by district personnel.

#### 2.3 Data Center Access

The district IT 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 management prior to any access to this area.

An authorized District IT employee is responsible for making sure that visitors entering a district data center are properly logged. It is mandatory that all visitors check in with district IT, and visitors to a district data center must sign in and sign out with District IT 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. Reception area visitor logs must be retained for three months.

#### 2.4 Equipment Maintenance and Environmentals

District IT 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.

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

Data 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.

#### 2.5 Media Disposal and Destruction

District IT 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.

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 districtinformation 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 district 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.

####  2.6 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.

* 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.
* 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.