# **ADMINISTRATIVE REGULATION 37xx**

**NAME OF CC DISTRICT** BUSINESS

## INFORMATION SECURITY-SECURE OPERATIONS

### Purpose and Scope

The objective of this Administrative Regulation is to describe policies for secure operations of **NAME OF CC DISTRICT** information and systems. The following topics are covered:

* Operations Processing
* Virus Management
* Patches and Updates
* Backup AR
* Third Party Management

This is one of a series of information security Administrative Regulations maintained by the District Information Technology (IT) department designed to protect **NAME OF CC DISTRICT** information systems.

#### Applicability of Assets

This Administrative Regulation applies to all electronic assets that are owned or leased by **NAME OF CC DISTRICT**, including but not limited to:

* Desktop and Laptop Computers
* Mobile Devices
* Servers
* Network Infrastructure

#### Applicability to all Employees and Volunteers

This Administrative Regulation applies to all Board of Trustees  authorized/ratified full-time and part-time regular Academic and Classified employees, Substitutes, Short-term (Temporary) staff, Professional Experts, College Work Study students, Student Help and Volunteers who are employed in the **NAME OF CC DISTRICT** for the purpose of meeting the needs of students.

#### Applicability to External Parties

This Administrative Regulation applies to all external parties, including but not limited to **NAME OF CC DISTRICT** business partners, vendors, suppliers, outsource service providers, and other third party entities with access to **NAME OF CC DISTRICT** networks and system resources.

#### References and Related Documents

Please refer to the following Administrative Regulations for additional information and references including definitions:

* AR 37xx: Acceptable Use
* AR 37xx: Change Control
* AR 3726: Data Classification
* AR 37xx: Disaster Recovery
* AR 37xx: Information Security Program Overview
* AR 3729: Logging and Monitoring
* AR 37xx: Network Security
* AR 3728: Physical Security
* AR 3730: Remote Access
* AR 37xx: Secure Operations
* AR 37xx: Security Incident Response

### Secure Operations

#### Operations Processing

All system scheduling, jobs, and dependencies must be documented. This documentation must include job start times, latest job completion times, delay procedures and handling procedures in case of failure or error.

Operating system and application processing, restart and shutdown procedures must be documented.

Application back out, restart and shutdown procedures with emergency contact information must be provided by the Applications Development team and made available to District IT operations personnel.

Refer to Physical Security AR 4000.x for data center access and other physical security controls.

#### Virus Management

All applicable systems must be configured with District IT-approved anti-virus software. The software must be configured to scan for viruses in real-time. Anti-virus programs must be capable of detecting, removing, and protecting against all known types of malicious software.

All systems with anti-virus software must be configured to update virus signatures on a daily basis.

End users must not be able to configure or disable the software.

All anti-virus mechanisms must generate audit logs to aid District IT and campus IT in detecting and responding to virus outbreaks.

All **NAME OF CC DISTRICT** employees may obtain approved anti-virus software to install on **NAME OF CC DISTRICT** assets from District IT or campus IT.

#### Patches and Updates

**NAME OF CC DISTRICT** must ensure that all system components and software are protected from known vulnerabilities by installing the latest vendor-supplied firmware, security patches, hot fixes and service packs found to be applicable to **NAME OF CC DISTRICT** computing resources.

District IT and campus IT system administrators must keep up with vendor changes and enhancements. New or modified non-urgent patches must be scheduled and installed within one month of release. Urgent patches that address security vulnerabilities must be installed as soon as is feasible without introducing instability or impacting service availability.

Where feasible, patches must be tested in a test environment prior to production deployment. Testing must ensure that systems function correctly.

Changes to servers and networks should be tested prior to implementation and follow normal change control management procedures.

District IT and campus IT must be alert to identifying new security vulnerabilities by monitoring available vendor or industry security sources. Hardening and configuration standards must be updated as soon as practical after new vulnerabilities are found.

#### 2.4 Software and Asset Management

The Electronic Communications AR 4000.2 and the Acceptable Use AR 37xx set forth usage policies for critical technologies that include e-mail usage and Internet usage and define proper use of these technologies. District IT may also issue mobile devices (such as laptops or removable storage devices), and will maintain a list of issued devices and personnel with access to assist in determining owner, contact information and purpose.

District IT and campus IT will maintain a list of company-approved products and software.

#### 2.5 Backup and Media

Users must store all critical files on the local area network so that they can be properly backed up. If an end-user chooses to store essential data elsewhere, it must be approved by District IT management or campus IT management and the user is for ensuring the data can be recovered.

Any media containing backup data that is stored onsite must be classified so that operations personnel can determine the sensitivity of the data stored on tape or other formats. Refer to the Data Handling Procedures for classification and handling information.

Any backup media that must be transferred that contains *restricted* information must be sent by secured courier or other delivery method that can be accurately tracked. Management must approve any and all media that is moved from a secured area (especially when media is distributed to individuals).

Strict control must be maintained over the storage and accessibility of backup media. Inventory logs of all media must be maintained and reviewed at least annually.

Media must be destroyed when it is no longer needed for business or legal reasons. Data retention requirements must be documented.

#### 2.6 Third Party Management

A third party user is a non-**NAME OF CC DISTRICT** employee or entity that is authorized to access **NAME OF CC DISTRICT** systems and networks. Examples of third party users include consultants, contractors, temporary employees, interns, vendors, business partners, service providers, and suppliers of products, services, or information.

A process for engaging service providers must include proper due diligence prior to beginning the engagement. A list of all third party providers must be maintained.

Network connections between the **NAME OF CC DISTRICT** environment and third parties must follow agreed-upon security procedures and/or confidentiality requirements. Such connections and other third-party access to **NAME OF CC DISTRICT**’s systems must be governed by formal written agreements or contracts.

These agreements may require signed Confidentiality and Non-Disclosure statements restricting the subsequent usage and dissemination of **NAME OF CC DISTRICT** information.

Vendors or other third parties with access to **NAME OF CC DISTRICT**-owned or leased equipment or systems housed in **NAME OF CC DISTRICT** data center are restricted to only the specific equipment and systems they are authorized to maintain or monitor.

##### 2.6.2 HIPAA Third Party Agreements

HIPAA regulations specify that formal written agreements must be established with each party (often considered a “business associate”) who will access protected health information (PHI). The parties must agree to protect the integrity and confidentiality of the information being exchanged, and the agreement would clearly define responsibilities of both parties.

* **NAME OF CC DISTRICT** security policies and security mandates, including any fines and penalties that may be incurred for HIPPA or PCI non-compliance for lack of compliance with the regulations
* Ownership and acceptable uses of PHI and other classified information
* Requirements for business continuity by the third party, in the event of a major disruption, disaster or failure
* Audit provisions for **NAME OF CC DISTRICT** or **NAME OF CC DISTRICT**-approved entities in the event of a data compromise. Provisions to ensure that **NAME OF CC DISTRICT**, or a **NAME OF CC DISTRICT**-approved auditor, will be provided with full cooperation and access to conduct a thorough security review after a security intrusion. The review will validate compliance with **NAME OF CC DISTRICT** standards and HIPAA regulators for protecting PHI and other **NAME OF CC DISTRICT** information.
* Security of PHI and **NAME OF CC DISTRICT** information during third party contract terminations or data transfers.

##### 2.6.3 PCI Third Party Requirements

**NAME OF CC DISTRICT** maintains a program to monitor its PCI DSS service providers’ compliance status at least annually.

Payment Card Industry Data Security Standard (PCI DSS) requires that shared hosting providers protect each entity’s hosted environment and cardholder data. These providers must meet specific requirements as detailed in Appendix A of the PCI DSS.

A written agreement that includes an acknowledgement from any PCI service providers must be maintained to ensure that the third party accepts responsibility for the security of cardholder data the service providers possess.

All service providers providing PCI services must be monitored at least annually to ensure their continued compliance with PCI DSS.