Status Active PolicyStat ID 17258391

Origination	12/2024
Last Approved	12/2024
Effective	12/2024
Last Revised	12/2024
Next Review	12/2034

Chapter Lead	Nohemy Ornelas: Chapter 3(CC),4&5
Policy Area	Chapter 3 General Institution
References	Non CCLC

AP 3733 Information Security Security Secure Operations

1. PURPOSE AND SCOPE

   The objective of this Administrative Procedure is to describe policies for secure operations of District information and systems. The following topics are covered:

   - Operations Processing
   - Application Development
   - Virus Management
   - Patches and Updates
   - Backup AR
   - Third Party Management

     This is one of a series of information security Administrative Procedures designed to protect the District's information systems. The District Information Technology (IT) department has district-wide fiduciary responsibility to set, maintain, and ensure the provisions of this regulation. District IT accomplishes this through collaborative engagement with the campus Technology Services departments.

   a. Applicability

      This Administrative Procedure applies to all full-time and part-time regular academic and classified employees, such as, short-term (temporary) staff, substitutes, professional experts, Federal Work Study students, and student help who are employed by, and volunteers who assist, the District for the purpose of meeting the needs of students.

   b. Applicability to External Parties

This Administrative Procedure applies to all external parties, including but not limited to District business partners, vendors, suppliers, service providers, and other third-party entities with access to District networks and system resources.

c. References and Related Documents

   Please refer to the Information Security Administrative Procedures for additional information and references, and definitions.

2. SECURE OPERATIONS

   a. 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 AR 3728: Information Security – Physical Security for data center access and other physical security controls.

   b. 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 daily.

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

   c. All anti-virus mechanisms must generate audit logs to aid District IT and college Technology Departments in detecting and responding to virus outbreaks.

   d. District IT or college Technology Services departments may install approved anti-virus software on any District assets or allow users to install it themselves.

   e. Patches and Updates

      The 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 District computing resources.

District IT and college Technology Services network administrators must keep up with vendor changes and enhancements. New or modified non-urgent security patches must be scheduled and installed within one month of release. College Technology Services departments may elect not to install system updates that are unrelated to District business and that do not affect security. Urgent patches that address security vulnerabilities must be installed as soon as 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 technology departments must be alerted 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.

f. Software and Asset Management

The AP 3720: Electronic Communications sets forth usage policies for critical technologies that include e-mail usage and Internet usage and defines proper use of these technologies. District IT and college Technology Services departments 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 the owner, contact information, and purpose.

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

g. .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 college Technology Services management, and the user is responsible 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 AP 3726: Information Security - Data Classification 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.

h. Third Party Management

A third-party user is a non-District employee or entity that is authorized to access District systems and networks. Examples of third-party users include consultants, contractors, project specialists, 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 District's environment and third parties must follow agreed-upon security procedures and/or confidentiality requirements. Such connections and other third-party access to the District's systems must be governed by formal written agreements or contracts. The third party must agree to adhere to the District Information Security Administrative Procedure.

These agreements may require signed Confidentiality and Non-Disclosure statements restricting the subsequent usage and dissemination of District information.

Vendors or other third parties with access to District-owned or leased equipment or systems housed in the District's data center are restricted to only the specific equipment and systems they are authorized to maintain or monitor.

i. G.1 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 as follows:
- 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 District or District-approved entities in the event of a data compromise. Provisions to ensure that District, or a 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 District standards and HIPAA regulators for protecting PHI and other District information.

- Security of PHI and District information during third-party contract terminations or data transfers.

ii. G.2 PCI Third-Party Requirements

The District maintains a program to monitor its Payment Card Industry Data Security Standard (PCI DSS) service providers' compliance status at least annually.

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 acknowledgment from any PCI service provider must be maintained to ensure that the third party accepts responsibility for the security of cardholder data the service provider possesses.

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

Refer to AP 3737 Information Security - Payment Card Industry Requirements (PCI).

Approval Signatures

Step Description	Approver	Date
Approved per Level 2 process in AP 2410	Kelly Goodrich: PPAC Support	12/2024