ADMINISTRATIVE REGULATION 3725

SOUTH ORANGE COUNTY COMMUNITY COLLEGE DISTRICT

GENERAL INSTITUTION

INFORMATION SECURITY PROGRAM OVERVIEW

I. PURPOSE AND SCOPE

This Administrative Regulation provides an overview of the District's information security program. Specific details of each aspect of the program are provided in other administrative regulations. The central and critical role of information systems at the District requires ensuring the protection of these systems.

This Administrative Regulation outlines the responsibilities and expectations for security of information assets managed by the District. The controls described in this Administrative Regulation are collectively known as SOCCCD's Security Program, which is designed to:

- Reflect the District business objectives,
- Prevent the unauthorized use of or access to District information systems, and
- Maintain the confidentiality, integrity, and availability of information.

This Administrative Regulation is guided by security requirements specific to District operating environment, laws, and regulations that are relevant to the District and information security best practices. These control requirements are documented and aligned with an internationally recognized industry standard for security, ISO 27002, *Code of Practice for Information Security Management* and designed to meet the requirements of the *Payment Card Industry Data Security Standard*.

This Administrative Regulation applies to all computer and network systems, software, and paper files owned by and/or administered by the District.

Computer and network systems include, but are not limited to, the following items owned or leased by the District and used by District personnel for information access: servers, storage systems, desktop or laptop computers, network equipment, telecommunications systems, and mobile devices.

Software includes operating systems, databases, and applications, whether developed by the District or purchased from application software vendors, or shareware / freeware in use within production systems.

A. Applicability

This Administrative Regulation 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 Regulation 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 following Administrative Regulations for additional information and references including definitions:

AR 3720: *Electronic Communications*
AR 3726: *Information Security – Data Classification*
AR 3728: *Information Security – Physical Security*
AR 3729: *Information Security – Logging and Monitoring*
AR 3730: *Information Security – Remote Access*
AR 3731: *Internally Developed Systems Change Control*
AR 3732: *Information Security – Security Incident Response*
AR 3733: *Information Security – Secure Operations*
AR 3734: *Information Security – Network Security*
AR 3735: *Information Security – Disaster Recovery*

II. MAINTENANCE AND SUPPORT

This Administrative Regulation is maintained by the office of the Vice Chancellor of Educational and Technology Services. It will be reviewed regularly and modified when applicable as a response to any major changes in the District's information security or regulatory requirements. Questions related to this Administrative Regulation should be directed to security@socccd.edu.

III. SECURITY ORGANIZATION

The District's security organization is designed as a distributed model with central oversight and governance, and consists of both information security and physical security elements. This organization meets periodically to address specific security issues and develop initiatives to continuously improve District information security.

A. Security Responsibilities

While information security is ultimately the responsibility of the office of the Vice Chancellor of Educational and Technology Services and their designees, everyone who uses the District's systems and networks and has access to District information, shares in the responsibility for its protection.

B. Information Security

The Executive Director of Information Technology and Security has primary responsibility for the information security program for the District. They are supported by individuals within core district-wide business areas.

C. Physical Security

Campus Police provide a safe and secure environment for students and staff, and work with District IT and the college technology departments to ensure that facilities and secure areas are controlled.

D. Data Owners

Data Owners are responsible for data quality and determining the appropriate classification level for the information contained within the respective applications under their purview. All applications have one or more designated Data Owner(s). The Data Owner may delegate responsibilities regarding classification and handling, but is ultimately accountable for determining that the responsibility has been correctly discharged.

E. Security Program Governance

The office of the Vice Chancellor of Educational and Technology Services is responsible for establishing administrative regulations that provide operational oversight and direction to the District's information security program.

IV. DATA CLASSIFICATION

Classifying information is at the core of an information security program because it specifies how information will be secured and handled, based on its sensitivity and value.

A. Data Classification Objectives

The District's strategy is to classify information regardless of medium (paper or electronic) according to its sensitivity and the potential impact of disclosure. In general, information is disclosed to employees or others only when there is a business need-to-know.

Information must be consistently handled according to its requirements for confidentiality and disclosure. Data Owners are responsible for determining the appropriate classification level for the information contained within the respective applications they own.

Information on paper documents or other media has the same classification level as in an electronic format.

District IT will provide appropriate security technology solutions (such as encryption) for electronically stored information should this level of protection be required.

B. Data Classification Categories

District data is classified into three categories. The definitions below are supplemented by the information and definitions in the *AR 3726*: *Data Classification*. The correct classification level is established by the Data Owner.

- Public information applies to information made available for public distribution through authorized District or college channels. Examples would include press releases, marketing materials, public web pages, and other data routinely available to the public.

- Internal information is available that must be protected due to proprietary or business considerations, but which is not personally identifiable or sensitive, such as internal policies, telephone listings, or data on the intranet that has not been approved for external communication. *Internal* information is generally available to all employees and other authorized users.

- Restricted information is sensitive in nature, proprietary, and specific to the District's business. Unauthorized compromise or disclosure would likely have serious financial, legal, or regulatory impacts. Examples include personally identifiable data, credit card data, health care data, human resources data, or computer system details. *Restricted* information is only available on a need-to-know basis. It may be appropriate to mark this type of information as "Confidential" or "Restricted Information".

For purposes of this Administrative Regulation, the term "personally identifiable information" means an individual's first name and last name or first initial and last name in combination with any one or more items of personal information, such as social security number or other identity verification number, driver's license number or state-issued identification card number, financial account number, credit or debit card number, date or place of birth, and gender; provided, however, that "personally identifiable information" shall not include information that is lawfully obtained from publicly available information, or from federal, state, or local government records lawfully made available to the general public.

Both the District and any computer service providers are required to comply with regulations designed to protect sensitive and personally identifiable information from unauthorized disclosure and identity theft. Encryption is mandated by many laws and standards for some information transmission or storage. Refer to the handling standards described in *AR 3726*: *Data Classification* for guidance.

V. HUMAN RESOURCES

A. Acknowledgement

In addition to the other agreements that may be required, acknowledgement of this Administrative Regulation and the *AR 3720*: *Electronic Communications* are part of the terms and conditions of employment with the District. Acknowledgement is required at the time of initial employment and annually thereafter.

Where applicable, the sponsoring District manager must ensure that temporary workers, project specialists, consultants, or contractors working for the District have been provided with a copy of this Administrative Regulation and *AR 3720*: *Electronic Communications*. Additionally, it is the responsibility of the sponsoring manager to ensure compliance with this and all District information security Administrative Regulations.

All employees are required to participate in security awareness training either annually or bi-annually as specified in the respective collective bargaining agreements.

B. Employee Administration

The Human Resources department initiates the addition of new access by providing notification to IT and other business areas who administer application security. HR updates the Human Resources System with new hires, transfer, and termination information.

Managers are responsible for notifying HR and IT when an employee, contractor, consultant, temporary worker, or intern is no longer associated with the District for any reason so that access can be disabled or removed.

Pre-employment background checks (Live Scans) are conducted on all permanent employees and some temporary employees whose job responsibilities require them to access credit card information and other data classified as restricted (see *AR 3726*: *Data Classification*).

C. Contractors and Temporary Workers

Temporary workers are processed through HR. Contractors must complete an agreement and be approved by the Board. Once a contractor has been identified, managers must work with HR and District IT to submit the appropriate forms so that access can be established.

D. Acceptable Use

The District's information and technology resources must be used in an approved, ethical, and lawful manner. Employees and contractors must always be alert to actions and activities they may perform that could breach the *AR 3720*: *Electronic Communications*, which details specific restrictions regarding the Internet, electronic mail, social networking, and use of the District's computing resources.

All computer systems belong to the District and may only be used for business purposes. District personnel should not have an expectation of privacy in anything they create, store, send, or receive via the computing environment.

District personnel shall never send unprotected primary account numbers (PANs) by end-user messaging technologies (for example, e-mail, instant messaging, SMS, chat, etc.)

If users have any uncertainty on the appropriateness of their actions, they should clarify their understanding with their manager or contact security@socccd.edu for guidance.

VI. PHYSICAL SECURITY

A. Physical Security Controls

Information protection is dependent on adequate physical security. All District information technology facilities employ access control measures to ensure that all facilities remain secure.

Campus Police, District IT along with College Technology Services Departments have responsibility for physical security and work together to investigate incidents that could involve information compromise. Campus police provides continuous surveillance of the facilities.

B. Access Cards to Secure Areas

District information technology secure areas are protected by entry controls designed to allow only authorized personnel to obtain access. Each secure area may have slightly different procedures for entry. Authorized individuals are issued an employee or visitor badge, or another form of access device that enables electronic or controlled physical access to exterior doors and authorized internal doors.

Visitors to secure areas must be issued a badge and must be escorted by District personnel. Visitors to secure areas must sign in and out daily on a Visitor's Log located at the site's Reception desk where present. Visitor badges must be turned in daily.

All visitors to a District Data Center or facility with network or server equipment must be escorted at all times and must also sign in and out with College IT or District IT.

C. Equipment and Media Security

Lost or stolen electronic devices must be reported to district-wide Service Desk immediately. This includes District issued laptops, smart phones, or removable storage devices that contain District data.

Strict control must be maintained over the internal or external distribution of any media that contains restricted information. District information that is classified as *Restricted*

is limited to authorized users on a need-to-know basis and must not be copied to unencrypted devices, e-mailed without encryption, or printed without adequate physical controls.

Users must shred or securely dispose of classified information in accordance with established retention policies. If secure disposal methods are required, contact the district-wide Service Desk.

Contractors or consultants using personal equipment to conduct District business are responsible for physically securing equipment in their possession that contains classified information. Loss of equipment containing *Restricted* information, even if personally owned, must be reported immediately to the district-wide Service Desk.

D. Payment Card Industry (PCI) Data Security Standard
In order to comply with PCI standards, the District will:
1. Limit access to system components and cardholder data to only those individuals whose job requires such access;
2. Restrict access to privileged user IDs to least privileges necessary to perform job responsibilities;
3. Protect devices that capture payment card data via direct physical interaction with the card from tampering and substitution; and
4. Periodically inspect device surfaces to detect tampering (for example, addition of card skimmers to devices), or substitution (for example, by checking the serial number or other device characteristics to verify it has not been swapped with a fraudulent device.)

VII. IT SECURITY CONTROLS

District IT has district-wide fiduciary responsibility for the security of computing infrastructure and controls such as cloud, networks, servers, databases, and desktop computing. District IT accomplishes this through collaborative engagement with the campus Technology Services departments.

Users must not disable, uninstall, or modify the security software, settings, or encryption installed on laptops or mobile devices.

A. Security Logging and Monitoring

Logs of key system events and access to sensitive information are in place and maintained by District IT and College Technology Services Department personnel. Systems that provide initial entry / authentication into the District network and any application system that processes District *Restricted* information must be configured to capture security audit log data.

Activities of those with privileged accounts (who have a higher level of access on servers or within applications) must also be captured and recorded in security audit logs.

Logs are protected from unauthorized modification or destruction and are retained for a minimum of 180 days (six months) or as required.

System or application administrators must routinely monitor system or application logs for anomalies regarding access to information. Exceptions must be investigated and appropriate action taken.

B. Third-Party Access

Third-party (non-employee) access to the District's systems must be governed by formal written agreements or contracts. Network connections between the District environment and third parties must follow agreed-upon security procedures. 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 a District data center are restricted to only the specific equipment and systems they are authorized to maintain or monitor.

VIII. ACCESS CONTROLS

A. Access Control

Access to District systems and applications is role-based and will be granted to authorized users based on job classification and need. Users are limited to the system capabilities they need based on job function or role and as authorized by management. Guests, visitors, and vendors can request access to college resources for a limited duration by obtaining approval from the Technology Department of the respective site.

A warning banner must be displayed on all District login gateways indicating that only authorized users may access the network or system.

Except for instructor classroom computers, District computers are equipped with screen saver locks that will activate after 15 minutes of inactivity as required by the current PCI Data Security Standard (PCI DSS). Users must manually logoff or lock workstations if they will be unattended prior to activation of the screen saver lock. Instructors are required to lock or logout of instructor classroom computers when leaving the classroom.

B. System and User Accounts

Accounts are assigned to an individual and may not be shared. Guest accounts must be disabled if a system or application is provided with one. Vendor-supplied default accounts and passwords must be disabled or changed.

Unnecessary default accounts (including accounts used by operating systems, security software, applications, systems, POS terminals, SNMP, etc.) are removed or disabled before a system is installed on the network.

System and Kiosks accounts, such as background accounts that are used for internal processing, are exempt from time-based password change requirements because requiring password expiration could interrupt normal data processing cycles.

C. Passwords

Passwords are confidential and must not be shared. Passwords must be changed on first use or if they have been reset for the user by the District IT or appropriate college technology department.

District IT and College Technology Services Department staff resetting passwords must verify the identity of all users requesting a password reset prior to performing the reset.

The primary user password must be changed at least every 90 days as required by the current PCI DSS. Accounts used for system administration that have a higher level of privilege must also be changed at every 90 days, or more frequently if the situation warrants. Refer to *AR 3727*: *Access Control* for further information.

D. Account Review

Senior management of District IT and College Technology Services in conjunction with Data Owners or their designees must review the user accounts for the systems and applications they administer and verify the appropriateness of continued access. This review must be performed at least every six (6) months.

Network and system access should be disabled immediately upon notification from Human Resources that an employee (or appropriate department in the case of a contractor) is no longer with the District.

E. Network Connectivity

District IT and College Technology Services Departments maintain the operation of the District's network. All new wired connections must be requested through them. Wired devices, such as servers, that will be connected to the network must be approved and implemented by District IT or the respective College Technology Services Departments.

Employees and other authorized users must request remote access and use established connectivity methods to connect to District networks from a remote location. Use of other remote connectivity methods is prohibited. Refer to the *AR 3734*: *Network Security* and *AR 3730*: *Remote Access* for additional information.

IX. APPLICATION DEVELOPMENT

A. Changes to Applications

Application change control is a security issue because unauthorized or accidental changes to applications may impact the integrity and availability of the data. The ability to change applications in production is limited to authorized users.

Change Control processes are required to mitigate risk associated with changing business applications, minimize the impact of change, and provide a stronger linkage between production problems and the events that caused them. Applications developed and/or managed by the District must be controlled as described in AR 3731: *Internally Developed Systems Change Control.*

B. Application Security Standards

Application managers must consider secure coding practices that will prevent or minimize security vulnerabilities, especially for any Internet-facing application. If a third party is hosting an application, data protection controls provided by the third party must be adequate to meet regulatory and contractual requirements for security.

X. SECURITY RESPONSE/DISASTER RECOVERY

A. Security Incident Response

All users must report suspicious activities or actual occurrence of any unauthorized activities to the district-wide Service Desk. Notification should be made immediately or as soon as reasonably possible. This includes unauthorized use of accounts, logon IDs, passwords, loss of district-owned laptops or other devices, or potential breaches of District computer systems and networks. District IT or the respective College Technology Services Department, as appropriate, will complete an Incident Report and conduct any Chancellor or designee authorized investigation that may be required.

Incidents that involve information compromise, such as a data breach or other loss of information, will be handled according to the *AR 3732*: *Security Incident Response*. District IT will work with other business areas as required to resolve the incident and ensure that correct notification procedures are followed.

Users detecting potential information security events should immediately report them to the district-wide Service Desk.

B. Business Continuity / Disaster Recovery

Business Continuity Plans are departmental plans that describe in detail how business areas will continue functioning in the event of a major system outage or a disaster. Each business area is responsible for documenting a Business Continuity Plan and designating a Business Recovery Coordinator who will develop and maintain their plan and participate in notification and recovery activities.

Disaster recovery plans describe how IT systems and resources will respond to a disaster situation and restore processing to the business based on the District's business objectives and timeframes for recovery of critical applications. District IT working in conjunction with College Technology Services and Campus Police will provide overall coordination and management in the event of a disaster, and assemble the necessary recovery and business teams to provide a timely response. Basic information is documented in *AR 3735*: *Disaster Recovery*.

C. Backups

The District's data is regularly backed up based on defined business requirements for information recovery.

Critical information must be stored on network file servers or production servers to ensure regular and automatic backup and recovery. Critical information should not be stored on personal computers or laptops alone, or on unencrypted personally-owned devices. If additional storage space is needed, contact the IT Service Desk for options.

XI. COMPLIANCE AND AUDIT

A. Compliance with Legal Requirements

The Information Security Program supports compliance with state and federal laws and applicable international laws and standards, including HIPAA, PCI, GLBA, and FERPA.

B. Third Party Service Providers

Additional security requirements may be required for any third-party service provider that receives, stores, maintains, processes, or otherwise is permitted access to personally identifiable information provided to them by the District.

Whenever selecting and retaining any third-party service provider, the responsible District business person will (1) take reasonable steps to confirm that the service provider can maintain appropriate security measures to protect personally identifiable information consistent with all applicable laws and regulations, and (2) require the service provider to contractually agree in writing with the District to implement and maintain such appropriate security measures.

C. Audit

Audit reviews are conducted by an external auditor and by IT consultants at least annually. Selected application security reviews may be performed as part of internal audit plans or general controls audits. Findings from the audits are to be reviewed and implemented by District IT and College Technology Services.

XII. ENFORCEMENT AND COMPLIANCE

A. Enforcement

Those detecting violations of this Administrative Regulation must report the violation to their direct manager immediately, who will verify the nature of the violation and report it to the district-wide service desk and the Vice Chancellor of Educational and Technology Services, who will determine the extent of risk that any non-compliance condition presents and remediation activities that are required.

Users who deliberately violate information security policies will be subject to disciplinary action up to and including termination from employment or association with the District.

B. Exceptions

Business needs may occasionally require variance from established Administrative Regulations and standards. A business function may not be able to be performed effectively, reasonably, or cost-effectively if the Administrative Regulation is followed. In these instances, the Vice Chancellor of Educational and Technology Services must be notified through email to security@socccd.edu, briefly stating the underlying business problem and recommended approach or acceptable alternatives. Alternatives and any potential risks or problems the alternatives may cause will be considered. As a part of the annual review of this regulation pursuant to section II, the regulation may be revised to incorporate any frequent and recurring exception as appropriate.