ADMINISTRATIVE REGULATION 3734

SOUTH ORANGE COUNTY BUSINESS
COMMUNITY COLLEGE DISTRICT

INFORMATION SECURITY- NETWORK SECURITY

I. PURPOSE AND SCOPE

The objective of this Administrative Regulation is to describe controls required to protect South Orange County Community College District (SOCCCD) information and systems. Network infrastructure must be configured securely in order to protect SOCCCD systems and maintain network integrity and availability. Effective network security will reduce potential vulnerabilities and help to enforce secure access to SOCCCD information and technology.

This is one of a series of information security Administrative Regulations designed to protect SOCCCD information systems. District Information Technology (IT) department has the primary responsibility to maintain and implement the provisions of this AR with input from the college Technology Services departments.

1. Applicability of Assets
   This Administrative Regulation applies to all electronic assets that are owned or leased by SOCCCD, including but not limited to:
   - Servers
   - Network Infrastructure
   - Mobile Devices
   - Infrastructure as a Service or IaaS

2. Applicability
   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 South Orange County Community College District for meeting the needs of students.

3. Applicability to External Parties
   This Administrative Regulation applies to all external parties, including but not limited to SOCCCD business partners, vendors, suppliers, outsource service providers, and other third-party entities with access to SOCCCD networks and system resources.

4. References and Related Documents
   Please refer to the following Administrative Regulations for additional information and references including definitions:

AR 3725: Information Security Program Overview
AR 3726: Data Classification
AR 3728: Physical Security
AR 3729: Logging and Monitoring
AR 3730: Remote Access
AR 3731: Change Control
AR 3732: Security Incident Response
AR 3733: Secure Operations
AR 3735: Disaster Recovery
AR 4000.2: Electronic Communications

II. NETWORK SECURITY

District IT has primary responsibility for the SOCCCD network and security. District IT in collaboration with the college technology departments manages and administers campus infrastructure and network components. Network administrators and network technicians, supervised by the IT Director: Infrastructure and Security or College Technology Directors are the operational managers of campus firewalls and network equipment. All other firewalls and network equipment are maintained directly by District IT.

1. General Network Controls

System configuration standards are in place for critical network and server components that are managed by District IT and campus technology departments. Standards must address known security vulnerabilities and industry best practices, and provide specifications for “hardening” the native operating system or platform from known security weaknesses.

District IT must maintain appropriate network documentation, including a high-level network diagram specifically noting inbound and outbound network connections. This must include wireless network components and show connections to all networks, any cardholder data (PCI) locations, and wireless networks.

Network diagrams and configuration details must not be disclosed to unauthorized parties unless identifying IP addresses and names have been removed. The data classification level for sanitized (IP addresses, server names, and other identifying elements removed) diagrams is *Internal*. Unsanitized network diagrams have a data classification of *Restricted*. Refer to the *AR 3726: Information Security - Data Classification* for classification requirements.

Only necessary and secure services, protocols, services/daemons, etc., should be enabled as required for the function of the system. For any required services, protocols or services/daemons that are insecure, appropriate security features must be enabled. For example, secure technologies such as SSH, S-FTP, SSL, or IPsec VPN should be used to protect insecure services such as NetBIOS, file-sharing, Telnet, FTP, etc.

Documentation and business justification for use of all services, protocols, and ports allowed, including documentation of security features implemented for those protocols considered to be unsecure must be maintained by District IT or College Technology Services.

Vendor-supplied defaults must be changed before installing a system on the network, including but not limited to passwords, simple network management protocol (SNMP) community strings, and elimination of unnecessary accounts.

System security parameters must be configured to prevent misuse. All unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers, must be removed.

Publicly accessible network jacks should be restricted to authorized systems.

2. External Connections and Firewalls
District IT management or campus technology management must approve all new external connections, inbound or outbound, to the SOCCCD internal network. All connections into and out of the internal network must be documented, managed, and internally coordinated.

Firewalls must be deployed to restrict inbound and outbound connections to the SOCCCD network.

New network connections requested to be allowed through SOCCCD firewalls must be approved by District IT management or College Technology Department management and require a business case justification.

Ad-hoc modification of firewall rules can jeopardize the security of SOCCCD network. Established change control procedures must be followed for all firewall changes.

Where technically possible, firewall rules should be tested prior to implementation.

A review of all firewall and routers must be reviewed every six months. This activity must include a review of the specific ports/services/protocols allowed into the environment and proper documentation of the review.

For specific processes and procedures, refer to the *AR 3731: Internally Developed Systems- Change Control* and *Firewall Security Departmental Procedures*.

3. Wireless Security
Wireless connectivity is provided as a convenience for staff and students utilizing College campus (Saddleback, IVC, ATEP) wireless implementation. Either a student or staff SSID must be entered to gain access. Refer to *Wireless Security Departmental Procedures* for additional information on using wireless services.

Any other permanent wireless network implementations must be approved by District IT.

Wireless vendor defaults, including but not limited to default wireless encryption keys, passwords, and SNMP community strings, must be changed prior to implementation.

District IT and College Technology Departments will test for the presence of wireless access points and detect unauthorized wireless access points on a quarterly basis.

3.1 Wireless Environments and PCI

Whenever possible, cellular networks must be used for wireless transmission of cardholder data.

Firewalls are installed between wireless networks and the cardholder data environment, and configure these firewalls to deny or control (if such traffic is necessary for business purposes) any traffic from the wireless environment into the cardholder data environment.

For wireless environments connected to the cardholder data environment or transmitting cardholder data, vendor defaults must be changed. This includes but is not limited to default wireless encryption keys, passwords, and SNMP community strings.

4. Encryption

Encryption scrambles sensitive information that is stored or transmitted electronically. Cryptographic solutions must adhere to international export laws or any applicable legal or regulatory controls. Encryption must be used at SOCCCD in the following situations.

4.1 Passwords

All passwords must be encrypted and unreadable. This includes password files for users, firewalls, routers, operating systems, applications, databases, and web servers.

Password or credential files stored on third party platforms must also be encrypted.

4.2 Restricted Data

AR 3726: Information Security-Data Classification describes how data is categorized based on its sensitivity, need for confidentiality, or value to SOCCCD. Data classified as *Restricted* is the most sensitive category. Its unauthorized disclosure may violate regulations or standards, such as PCI, or contractual agreements with third parties or service providers.

Restricted data may exist in applications, databases or files. Various access controls protect data when in its original location, but when copied, reproduced or transmitted, the original protections are lost. However, the classification and level of protection for a data element must travel with it regardless of its location or format.

Storing *Restricted* data on unencrypted removable devices, personal drives, or various types of USB storage may expose sensitive or confidential data to unauthorized disclosure and is against SOCCCD administrative regulations. If transporting or storing restricted data must be on a removable device, users must work with District IT or campus IT to ensure the data is secure.

If *Restricted* data is copied from its original location (e.g., to other files, removable devices, or on backup media) it must be encrypted. If sent via e-mail or other transmission means on public networks, it must be encrypted. Refer to the *Encryption Departmental Procedures* for specific encryption methods and procedures.

4.2 Remote Administrator Access
Remote access by security, system, or firewall administrators to perform maintenance or troubleshoot problems presents a greater security risk due to the elevated privileges these individuals possess. System Administrators must connect securely using the SSL VPN to ensure that communications with SOCCCD networks from a remote location are over an encrypted channel. This includes any non-console administrative access. Two-factor authentication is required where technically feasible.

4.3 Key Management
Key management procedures must be documented for all processes and procedures involving encryption keys, especially if used for cardholder data. PCI DSS requirements mandate strong keys, secure key distribution and storage, periodic key changes, and other requirements. Please refer to the *Encryption Departmental Procedures* for detailed information.

5. Scanning and Vulnerability Management
District IT and College Technology Departments must be informed of information security issues and vulnerabilities applicable to SOCCCD computing systems. When security issues are identified, District IT is responsible for notifying appropriate personnel, including system and network administrators/technicians and College Technology Directors.

The primary method for identifying new threats as they arise will be through vendor and security Internet mailing lists. SOCCCD will identify and assign a risk ranking to newly discovered security vulnerabilities. As appropriate, platform hardening standards must be updated to reflect measures required for protection from any newly discovered vulnerability.

SOCCCD performs quarterly external vulnerability scans on critical and networks in-scope for PCI compliance. External vulnerability scans are performed by an Approved

Scanning Vendor (ASV) as designated by the Payment Card Industry Security Standards Council (PCI SSC).

SOCCCD performs internal vulnerability scans on a periodic (at least semi-annual) basis or after any significant network changes.

Penetration tests must be performed at least once a year and after any significant infrastructure or application upgrade or modification (such as an operating system upgrade, a sub- network added to the environment, or a web server added to the environment). These penetration tests must include both network-layer and application-layer tests.

An annual process is in place to identify threats and vulnerabilities that results in a formal risk assessment.

6. Network Time Protocol (NTP)
All critical system clocks and times must be configured to acquire, distribute, and store a consistent time. All SOCCCD production systems must be configured to use one of the internal NTP servers to maintain time synchronization with other systems in the environment.

Internal NTP servers will be configured to request time updates from the Internet site http://time.nist.gov. Client systems able to retrieve time settings from the NTP server will be limited through Access Control Lists (ACL).

The NTP system will always run the latest available version of the software.

7. Payment Card Industry (PCI) Requirements

The following additional network controls are specific to network locations in-scope for PCI:

- Restrict inbound and outbound traffic to that which is necessary for the cardholder data environment.

- Firewall and router configurations must restrict connections between untrusted networks and any system components in the cardholder data environment. An “untrusted network” is any network that is external to the networks belonging to the entity under review, and/or which is out of the entity's ability to control or manage.

- Prohibit direct public access between the Internet and any system component in the cardholder data environment. Do not allow any direct connections inbound or outbound for traffic between the Internet and the cardholder data environment

- Implement a DMZ to limit inbound traffic to only system components that provide authorized publicly accessible services, protocols, and ports. Limit inbound Internet traffic to IP addresses within the DMZ.

- Install a firewall at each Internet connection and between any demilitarized zone (DMZ) and the internal network zone
    - Do not allow internal addresses to pass from the Internet into the DMZ.
    - Do not allow unauthorized outbound traffic from the cardholder data environment to the Internet.

- Implement stateful inspection, also known as dynamic packet filtering. (That is, only "established" connections are allowed into the network.)

- Place system components that store cardholder data (such as a database) in an internal network zone.

- Where feasible, implement only one primary function per server to prevent functions that require different security levels from co-existing on the same server. (For example, web servers, database servers, and DNS should be implemented on separate servers.)

- Use intrusion-detection systems, and/or intrusion-prevention systems to monitor all traffic at the perimeter of the cardholder data environment as well as at critical points inside of the cardholder data environment, and alert personnel to suspected compromises.

- Never send unprotected PANs by end-user messaging technologies (for example, e-mail, instant messaging, chat, etc.).