ADMINISTRATIVE REGULATION 3730

SOUTH ORANGE COUNTY COMMUNITY COLLEGE DISTRICT

BUSINESS

INFORMATION SECURITY-REMOTE ACCESS

I. PURPOSE AND SCOPE

The objective of this administrative regulation is to control access to the South Orange County Community College District (SOCCCD) information and systems when connections are made to those systems from a remote location.

This is one of a series of information security administrative regulations maintained by the District Information Technology (IT) department designed to protect SOCCCD information systems.

Please refer to *AR-3725-Information Security Overview* for applicability of assets application to staff, and external parties.

II. REMOTE ACCESS

All connections into and out of the internal network must be documented and managed by District IT and/or college Technology departments. Remote access is not automatically provided to all personnel and must be requested and approved as described below. The exception to this is access to the Student Information System (SIS) through the MySite Portal, Workday, Jaggaer, or Tidemark using an Internet browser. Access to these are authorized for both employees and students, based on their job function and role, using assigned credentials and passwords.

Users must use established remote access mechanisms or gateways to District systems. Aside from the web-based MySite Portal, two primary approved connection methods are used to gain access to SOCCCD systems: an SSL VPN client (supplied by District IT or college Technology departments).

Remote access to Workday and other financial systems requires two-factor authentication and is granted based on the employee's job function and role, using assigned credentials and passwords.

Remote access is prohibited from any public or shared computer or Internet kiosk.

Users may not establish new remote access systems or methods unless approval has been granted as noted below.

All remote access will be audited annually by District IT management and/or college Technology department management.

A. Requests for Remote Access

Users create service desk tickets to request remote access. Refer to the *AR-3727-Information Security-Access Control* for further information.

B. Approvals for Remote Access

General remote access: For college employees, remote access must be approved by the college President or designee. For District Services employees, remote access must be approved by the Vice Chancellor of Technology and Learning Services or designee.

New remote access methods: Either District IT or the relevant college Technology Director must approve any new remote access method or system.

C. Access Controls for Remote Connections

Remote access sessions will be automatically disconnected after 15 minutes of inactivity.

Personal firewall software must be installed on all SOCCCD or employee-owned computers with direct connectivity to the Internet that are used to access a District network. Anti-virus software must also be installed and must include the most recent software updates and virus profiles.

Any remote access connection that has been established for a vendor, business partner, or other third party for purposes of support must be immediately deactivated once no longer in use by the appropriate IT staff.

D. Transmission Over Networks

If SOCCCD *Restricted* data is to be transmitted over any communications network, it must be sent only in encrypted form. Networks include SOCCCD email mail systems, connections using the Internet, and supplied SOCCCD remote access systems. All such transmissions must use software encryption approved by the District IT department. Refer to the *AR-3726 Information Security-Data Classification* for further information.

E. Payment Card Industry Considerations

SOCCCD adheres to the requirements of the Payment Card Industry Data Security Standard (PCI). Where cardholder data is present, remote access to those systems must incorporate two-factor authentication. This refers to network-level access originating from outside the SOCCCD network to the SOCCCD network by employees and third parties.

For personnel accessing cardholder data via remote-access technologies, copy, move, and storage of cardholder data onto local hard drives and removable electronic media is prohibited unless explicitly authorized by the Vice Chancellor of Technology and Learning Services for a legitimate business need.

III. REGULATION COMPLIANCE

The SOCCCD IT team will verify compliance to this policy through various methods, including but not limited to, periodic walk-through, video monitoring, business tool reports,

internal and external audits, and inspection, and will provide feedback to the policy owner and appropriate asset owner.

A. Exceptions

Any exception to this regulation must be approved in advance by the college president or designee for college employees or the Vice Chancellor of Technology and Learning Services for District Services employees.

B. Non-Compliance

An employee found to have violated this regulation may be subject to disciplinary action, up to and including termination of employment.

IV. RELATED STANDARDS, POLICIES, AND PROCESSES

Please review the following regulations and guidelines for details of protecting information when accessing the network via remote access methods, and acceptable use of SOCCCD's network:

- Administrative Regulation *4014 Electronic Communications*
- NIST SP 800-53 Rev. 4 AC-17, AC-19, AC-20
- HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(4)(i), 164.308(b)(1), 164.308(b)(3), 164.310(b), 164.312(e)(1), 164.312(e)(2)(ii)
- Family Educational Rights and Privacy Act (FERPA) (20 U.S.C. § 1232g; 34 CFR Part 99)