INFORMATION SECURITY - REMOTE ACCESS

I. PURPOSE AND SCOPE

The objective of this Administrative Regulation is to control access to 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 Local Campus IT. 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 using an Internet browser. Access to the Portal is authorized for both staff 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 Local Campus IT) or the “GoToMyPC” software.

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 Local Campus IT management.

   a. Requests for Remote Access
Users create service desk tickets to request remote access. Refer to the AR-3727-Access Control for further information.

b. Approvals for Remote Access

General remote access: For college staff, remote access must be approved by the college President or designee. For District Services, 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 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.