ADMINISTRATIVE REGULATION 3727

SOUTH ORANGE COUNTY COMMUNITY COLLEGE DISTRICT

BUSINESS

INFORMATION SECURITY-ACCESS CONTROL

I. PURPOSE AND SCOPE

The objective of this administrative regulation is to provide internal controls for access to the South Orange County Community College District (SOCCCD) sites, information and applications. This administrative regulation (AR) is part of a series of ARs governing the secure use and access of Information Technology Systems and Services.

Access controls may be physical (such as locks and badges), administrative (such as the AR to safeguard passwords) or technical (protections enforced by software settings or privileges). These controls are designed to either allow or restrict the ability to view, update or delete information within the SOCCCD networks and systems, or paper documents.

A. Applicability of Assets

The scope of this AR includes all electronic assets that are owned or leased by SOCCCD. Assets may include but are not limited to:

1. Desktop and laptop computers
2. Mobile devices
3. Servers
4. Network infrastructure
5. Electronic media
6. Mobile computing devices

B. Applicability

This AR applies to all employees of SOCCCD including all consultants, contractors, temporary employees, and volunteers.

C. Applicability to External Parties

This AR 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.

D. References and Related Documents

Please refer to the following ARs for additional information and references including definitions:

1. AR 3725: Information Security Program Overview
2. AR 3726: Information Security - Data Classification
3. AR 3728: Information Security - Physical Security
4. AR 3729: Information Security - Logging and Monitoring
5. AR 3730: Information Security - Remote Access
6. AR 3731: Internally Developed Systems Change Control
7. AR 3732: Information Security - Security Incident Response
8. AR 3733: Information Security - Secure Operations
9. AR 3734: Information Security - Network Security
10. AR 3735: Information Security - Disaster Recovery
11. AR 4014: Electronic Communications

II. ACCESS CONTROL

A. Access Control Principles

There are three basic access control principles at the SOCCCD:

1. All information is made available only to those with a legitimate "need-to-know". Access is provided on this basis, guided by job requirements and data classification.
2. Access controls for SOCCCD systems will be provided in a manner that promotes individual accountability. Audit trails and monitoring of access establishes accountability and allows for follow-up of access violations and security breaches.
3. Users with the highest levels of privilege on a computer system will be restricted to the least privileges necessary to perform the job.

B. Authentication to District Systems

Authentication is the verification of a user's identity. All individuals require identification (ID) prior to gaining access to secured SOCCCD facilities or systems such as server rooms, cash handling rooms and other areas where security is in the interest of the District.

Internal (SOCCCD personnel) and external (non-personnel) users must provide a valid and unique user ID in order to authenticate to the network. In addition to a unique ID, the authentication method must include at least one of the following:

1. A password or passphrase;
2. Token device or smart card; or
3. Biometric.

If the new user is a contractor or non-employee, the user ID will be identifiable as such by its naming convention.

Group, shared, or generic accounts do not provide accountability, and are not to be used for network or application authentication. Some exceptions may apply to this requirement, such as a system account that is required for server or network processing or an account that is to be used by departments such as ivcpolice@ivc.edu that would be used as official communications account.

Physical access to secured facilities requires that SOCCCD users possess appropriate access badges or credentials in order to enter all sites. Some areas, such as computer rooms, may require additional levels of access, cards or keys. Refer to the *AR-3728: Information Security - Physical Security* for specific information.

C. Authorization to Applications

Addition, modification and deletion of user IDs and other credentials must be controlled. Data Owners (or their designee) have responsibility for making security decisions about applications that process data for which they are responsible. Assuming the role of the Data Owner may require:

1. Approving and re-certifying access by users to systems or data they control, or
2. Classifying data belonging to the application system they manage (determining the level of confidentiality or classification that should be assigned to an application's data, which will dictate its level of protection).

Access to certain functions may be provisioned automatically based on job position. Otherwise, the appropriate IT department, as authorized by Data Owners, must approve all new accounts except for those provisioned automatically. Each request for access must contain written and/or electronic evidence of approval by the Data Owner, District IT, or college Technology Services. Extension authorizations for contractor accounts must be applied by District IT or college Technology Services to provide an audit trail.

Access requests must specify access either explicitly or via a "role" that has been mapped to the required access. Outside of initial standard network access provided based on the job position of the users, access to additional applications or capabilities is discretionary and must be both requested and approved by the Data Owner. For additional access, users should submit an access request.

Departmental security administrators may set up access for some applications. District IT will pass the request on to the relevant team to set up access.

Remote access is not automatically provided to all users and must be requested and approved. Refer to the *AR-3730*: *Remote Access* for additional information.

The District IT or college Technology Services departments will maintain for a minimum of six (6) years logs or other documentation of all access request approvals, user account creations, modifications, and deletions.

D. Security Administrators

The appropriate District IT or college Technology Services department is responsible for administering overall system access within SOCCCD, and so may request information from appropriate managers or administrators, such as who has access to their applications, and the procedures that they have put in place to provision them.

Some users (in District IT, college Technology departments, or business departments) may have a higher level of access privilege in order to administer systems or applications. They may have the ability to add, modify, or delete other users for the applications they control. To maintain system access to District owned or developed software, District IT or the college Technology departments shall be provided an Administrative Account that will be used for recovery and auditing elevated access periodically.

Systems administrators and network technicians, under management supervision, have a responsibility to maintain appropriate access controls for the applications they maintain in order to protect information from unauthorized access. The number of administrators should be tightly controlled and limited to as few as necessary.

Security administrators should have their accounts setup with the proper access and log in with their account to conduct any privilege access. A log should be kept to review any privilege access and changes and a report should be delivered and reviewed periodically each year by the Security Director and college Technology Directors. Security administrators should only use their privileged accounts to carry out administrative tasks that require privileged access. A non-privileged account should be used to perform routine tasks.

E. Passwords

Users of the SOCCCD computer systems will be provided with one or more unique accounts and associated passwords.

Users are held accountable for work performed with the account(s) issued to them, and are responsible for the confidentiality of their passwords. Passwords must be difficult to guess and kept private. Users must not disclose their password to anyone.

The following rules apply to password composition:

1. Must not be left blank when a new account is created. New passwords must not be the same for all users;
2. Must have a minimum length of eight (8) characters;
3. Must contain both numeric, special and alphabetic characters /be alphanumeric and contain one upper case letter;
4. New passwords must be changed immediately upon first use;

5. New passwords must not be the same as the four previously used passwords or used within a one year period; and
6. Passwords must be changed at least every 90 days (some passwords within IT are exempt from this requirement).

If a user requests a password reset via phone, email, web, or other non-face-to-face method, Administrators who have the ability to reset passwords must verify the user's identity, such as by providing an element of personal information, prior to changing the password.

F. Account Lockout

Accounts will be locked after six (6) invalid login attempts. Once an account is locked, an authorized District IT or college Technology department staff, automated recovery system or authorized student services representative is required to reset the account after the user's identity has been verified. The lockout duration will be set to a minimum of 30 minutes or until an administrator enables the account.

Faculty classroom/lab workstations have a session idle time of 30 minutes after which the session will be locked. With the exception of some system accounts, all other user accounts have a session idle time of 15 minutes after which the session will be locked.

G. Emergency Accounts

An Emergency Account / User ID will be established when access is needed to diagnose or correct a problem. The request to create the Emergency ID must be made through the appropriate college Technology Director or District IT manager or administrator. The ID will be enabled only for a 24-hour period unless a specific time period is requested.

The Requestor must inform the appropriate college Technology Director or District IT manager upon completion of the work so that the ID can be disabled.

H. Termination of Access Privileges

Supervisors are responsible for notifying Human Resources if personnel will be leaving SOCCCD. HR will contact District IT and other Security Administrators as required so that access may be removed. Access must be disabled immediately upon notification or at the end of the last day of work.

I. Review of Access

A bi-annual audit of computer resource authorizations to confirm that access privileges remain appropriate will be conducted by appropriate IT staff. After an additional sixty (60) days, inactive accounts will be purged. These requirements may not apply to certain specialized accounts (e.g., Windows Administrator, root). Student accounts maybe be exempt and regulated by the District established provisioning process.

District IT and/or college Technology departments, working with HR, may periodically validate employment and may immediately suspend users who are on leave-of-absence or extended disability. At least annually, IT will request that Data Owners verify continued access by users who have access to their applications.

District IT, college Technology departments and/or external auditors will periodically review security administration procedures for specific applications, and may employ monitoring tools to audit and verify access controls.

J. Payment Card Industry Requirements

SOCCCD adheres to the requirements of the Payment Card Industry Data Security Standard (PCI). The following additional requirements are mandatory for systems that store, process, or transmit cardholder data. References to the relevant PCI section numbers are in parentheses after each requirement:

1. Implementation of an automated access control system (7.1.4).
2. The access control system must cover all (PCI) system components (7.2.1).
3. The access control system must assign privileges based on job classification and function (7.2.2).
4. The access control system must be set to a default "deny all" setting (7.2.3).
5. Render all passwords unreadable during transmission and storage on all system components using strong cryptography (8.4).
6. Set the lockout duration to a minimum of 30 minutes or until administrator enables the user ID (8.5.14).
7. Authenticate all access to any database containing cardholder data. This includes access by applications, administrators, and all other users (8.5.16).

References:

PCI DSS Requirements and Security Assessment Procedures:
https://www.pcisecuritystandards.org/documents/PCI_DSS_v3.pdf
PCI DSS Quick Reference Guide
Version3.0: https://www.pcisecuritystandards.org/documents/PCIDSS_QRGv3.pdf
NIST SP 800-53 Rev. 4 AC-2, IA Family
HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(3)(ii)(B), 164.308(a)(3)(ii)(C), 164.308(a)(4)(i), 164.308(a)(4)(ii)(B), 164.308(a)(4)(ii)(C), 164.312(a)(2)(i), 164.312(a)(2)(ii), 164.312(a)(2)(iii), 164.312(d)