INFORMATION SECURITY-ACCESS CONTROL

I. PURPOSE AND SCOPE

The objective of this Administrative Regulation is to provide internal controls for access to the Yosemite County Community College District (YCCD) 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 Administrative Regulation 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 YCCD networks and systems, or paper documents.

1. Applicability of Assets

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

- Desktop and Laptop Computers
- Mobile Devices
- Servers
- Network Infrastructure
- Electronic Media
- Mobile Computing Devices

2. Applicability

This Administrative Regulation applies to all employees of YCCD including all consultants, contractors, temporary employees, and volunteers.

3. Applicability to External Parties

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

II. ACCESS CONTROL

1. Access Control Principles

There are three basic access control principles at the YCCD:

- 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.

- Access controls for YCCD 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.

- Users with the highest levels of privilege on a computer system will be restricted to the least privileges necessary to perform the job.

2. Authentication to YCCD Systems

Authentication is the verification of a user's claimed identity. Identification is required by all individuals prior to gaining access to secured YCCD facilities or systems such as server rooms, cash handling rooms and other areas where security is in the interest of the District.

Internal (YCCD 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:

- A password or passphrase
- Token device or smart card
- 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.

Physical access to secured facilities requires that YCCD 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. See Physical Security ITS-AR-1510.

3. Authorization to Applications

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

- Approving and re-certifying access by users to systems or data they control.
- 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 Information Technology Services (ITS) 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 Owner, District ITS. Extension authorizations for contractor accounts must be applied by District ITS 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.

Remote access is not automatically provided to all users and must be requested and approved.

4. Security Administrators

The IT department is responsible for administering overall system access within YCCD, 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 (District ITS) 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.

Systems administrators, 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 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.

5. Passwords

Users of the YCCD computer systems will be provided with one unique accounts and associated passwords. User account ID's shall be created using the employees Legal last name and the first initial if their first name.

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. Users must not log in to any resource allowing another user to utilize their accounts.

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 8 characters
3. Must contain three of the following four character groups
   - English uppercase characters (A thru Z)
   - English lowercase characters (a thru z)
   - Base 10 digits (0 thru 9)
   - Non-alphabetic characters (for example, !, $, #, %)
4. New passwords must be changed immediately upon first use
5. New passwords must not be the same as the five (5) previously used passwords
6. Passwords must be changed at least every 6 months (some passwords within IT are exempt from this requirement)

If a user requests a password reset via phone, or other non-face-to-face method, ITS personnel 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.

6. Account Lockout

Accounts will also be locked after six (6) invalid login attempts. Once an account is locked, a System Administrator or authorized ITS personnel 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.

7. Termination of Access Privileges

Supervisors are responsible for notifying Human Resources if personnel will be leaving YCCD. HR will contact District ITS as required so that access may be removed. Access must be disabled immediately upon notification.

8. Review of Access

A bi-annual audit of computer resource authorizations to confirm that access privileges remain appropriate will be conducted by appropriate ITS staff. As part of this review inactive accounts will be purged. Inactive account removal may not apply to certain specialized accounts (e.g., Windows Administrator, root).

District ITS, working with HR, may periodically validate employment and may immediately suspend users who are no longer employed by the district. At least annually, ITS will request that Data Owners verify continued access by users who have access to their applications.

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

9. Payment Card Industry Requirements

YCCD 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:

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