ADMINISTRATIVE REGULATION 3731

SOUTH ORANGE COUNTY COMMUNITY COLLEGE DISTRICT

BUSINESS

INTERNALLY DEVELOPED SYSTEMS CHANGE CONTROL

I. PURPOSE AND SCOPE

The objective of this Administrative Regulation is to ensure a standardized method for handling changes to South Orange County Community College District (SOCCCD) internally developed systems. Change control promotes the stability of the environment, which is essential to its security and integrity.

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 provisons of this AR with input from the college Technology Services departments

1. 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 the purpose of meeting the needs of students.

2. 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.

3. 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 3733: Secure Operations
   AR 3732: Security Incident Response
   AR 3734: Network Security
   AR 3735: Disaster Recovery

II. CHANGE CONTROL

A change is any modification or enhancement to an existing production system. Modifications can be in the form of updates to existing data, functionality, or system process. The District Information Technology department shall adhere to industry best practices in the development and maintenance of all internally developed systems.

1. Change Roles

   The following roles have been established to guide the Change Management process for internally developed applications:

   - Release Manager: Oversees the change being released into production
   - User: the individual or entity initiating a change, which may be either an internal SOCCCD employee or contractor, or an external organization.
   - Product Owner: the role that qualifies and prioritizes Change Requests from the Customer. The Product Owner may represent interests within a specific organizational entity.
   - Prioritization Committee one or more organizational bodies that review and prioritize Change Requests submitted by Product Owners or the user community.
   - Quality Assurance Team: the internal department to test developed changes prior to introducing into production. This group must be independent of the development group.
   - Release Team: Internal team designed to schedule and implement changes into production
   - Development Team: the internal SOCCCD group responsible for implementing and/or delivering the Change Requests.

2. Process Tools

   The primary tools used to manage Change Requests are the District-wide Service Desk system and an Application Lifecycle Management tool.

3. Change Requirements

   The basic requirements for Change Management are:

   3.1 Changes that are part of the production environment must follow defined procedures by submitting a Change Request through the service desk system.

   3.1.1 The User submits the Request

   3.1.2 The Request is reviewed by District IT, the relevant Product Owner, and further reviewed and prioritized by the Prioritization Committee.

   3.1.3 Once approved by the Prioritization Committee, the development team schedules and implements the change.

   3.1.4 All changes must be authorized by the appropriate management.

3.1.5 All changes to production software must be completely and comprehensively tested.

3.1.6 All required documentation associated with the changes must be included with the software delivery.

3.1.7 Program source code must be protected by restricting access to those within the Development team who have a need-to-know. Segregation of duties must be maintained.

3.1.8 Version controls for source code must be in place to maintain application integrity.

3.1.9 All change requests must be accompanied by back-out procedures to be used in the event of unexpected error conditions.

3.1.10 Production data must not be used for testing data unless it has been scrubbed.

4. Application Security Knowledge Transfer

   Changes related to new or significant implementation efforts should include a knowledge transfer of relevant security information from the Development team to the Network and Security staff and other interested parties.

5. Payment Card Industry Considerations

   SOCCCD adheres to the requirements of the Payment Card Industry Data Security Standard (PCI DSS). 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:

   - Development / test and production environments must be separate (6.4.1)
   - Separation of duties between development/test and production environments (6.4.2)
   - Production data (live PANs) are not used for testing or development (6.4.3)
   - Removal of test data and accounts before production systems become active (6.4.4)
   - Change control procedures for the implementation of security patches and software modifications must include the following:
     - Description of the impact of the change (6.4.5.1),
     - Documented change approval by authorized parties (6.4.5.2)
     - Functionality testing to verify that the change does not adversely impact the security of the system (6.4.5.3)
     - Back-out procedures (6.4.5.4).