# ADMINISTRATIVE REGULATION 3721

**COLLEGE OF THE REDWOODS**

## INFORMATION SECURITY-CHANGE CONTROL

### Purpose and Scope

The objective of this Administrative Regulation is to ensure a standardized method for handling changes to **COLLEGE OF THE REDWOODS** infrastructure and associated software. 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 maintained by the District Information Technology (IT) department designed to protect **COLLEGE OF THE REDWOODS** information systems.

#### Applicability of Assets

This policy refers to changes made to any **COLLEGE OF THE REDWOODS** asset, including but not limited to:

* Desktop and Laptop Computers
* Mobile Devices
* Servers
* Network Infrastructure Components
* Business Applications
* Databases

#### Applicability to Employees and Volunteers

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 **COLLEGE OF THE REDWOODS** for the purpose of meeting the needs of students.

#### Applicability to External Parties

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

#### References and Related Documents

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

* AR 3720: Acceptable Use
* AR 3721: Change Control
* AR 3722: Disaster Recovery
* AR 3723: Network Security
* AR 3724: Secure Operations
* AR 3725: Security Incident Response
* AR 3726: Data Classification
* AR 3727: Physical Security
* AR 3728: Logging and Monitoring
* AR 3729: Remote Access
* Change Management Process as documented in District IT departmental procedures

### 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.

#### Change Roles

The following roles have been established to guide the Change Management process. Refer to the Change Management departmental procedures on the District Information Technology SharePoint site for details on the change workflow and steps.

* **Customer**: the individual or entity initiating a change, which may be either an internal **COLLEGE OF THE REDWOODS** 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.
* **Change Prioritization Committee (CPC)**: one or more organizational bodies that review and prioritize Change Requests submitted by Product Owners. is this the TPC?
* **Development Team**: the internal **COLLEGE OF THE REDWOODS** group responsible for implementing and/or delivering the Change Requests.

#### Process Tools

The primary tools used to manage Change Requests are/is the District-wide ~~service desk system and an Application Lifecycle Management tool.~~ *Ticketing system*

#### Change Requirements for locally maintained software

The basic requirements for Change Management are:

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

1. The Customer submits the Request
2. The Request is reviewed by District IT, the relevant Product Owner, and further

reviewed and prioritized by the CPC.

1. Once approved by the CPC, the development team schedules and implements

the change.

1. All changes must be authorized by the appropriate management.
2. All changes to production software must be completely and comprehensively tested.
3. All required documentation associated with the changes must be included with the software delivery.
4. 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.
5. Version controls for source code must be in place to maintain application integrity.
6. All change requests must be accompanied by back-out procedures to be used in the event of unexpected error conditions.
7. Production data must not be used for testing data unless it has been scrubbed.

#### Change Requirements for vendor maintained software

Software provided by vendors or other organizations must follow these basic requirements for Change Management:

1. District IS is notified by the vendor or customer of an available update or patch to a software package.
2. The update must be requested through the service desk system.
3. The update must be authorized by the appropriate user management.
4. The update must be thoroughly tested in a test environment and approved by the customer prior to installation.
5. Production data must not be used for testing data unless it has been scrubbed.
6. The update must be accompanied by back-out procedures to be used in the event of unexpected error conditions.

#### Change Requirements for infrastructure related technology

Purpose built hardware containing updateable operating systems including but not limited to network switching hardware and general purpose computing hardware such as servers and desktops must follow these basic requirements for Change Management where the device provides services to end users:

1. District IT or Local Campus IT is made aware of an update or patch to a device.
2. The update’s criticality is assessed to determine appropriate implementation scheduling.
3. Where possible, the update is tested in a non-production environment to evaluate the service impact.
4. District IT and Local Campus IT discuss the impact and scheduling of the update.
5. The rollout of the update is scheduled and announced at the weekly District IT Infrastructure stand up meeting.
6. Backups of the existing configuration settings are verified up to date and complete.
7. The rollout is completed and functional testing is performed to ensure there is no user impact to services.
8. Completion of the update is announced and the update is documented in the infrastructure change control logs.

#### 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.

#### Payment Card Industry Considerations

**COLLEGE OF THE REDWOODS** 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:

* 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).