INFORMATION SECURITY-CHANGE MANAGMENT

This is one of a series of information security Administrative Regulations maintained by the Yosemite Community College District (YCCD) Information Technology Services (ITS) department designed to protect YCCD information systems and data.

1.0 Purpose and Scope

The objective of this Administrative Regulation is to ensure a standardized method for handling requests for changes to YCCD Information Technology infrastructure and associated software. Change Management promotes the stability of the environment, which is essential to its security and integrity.

1.1 Applicability To Assets

This policy refers to changes made to any YCCD asset, including but not limited to:

- Servers
- Network Infrastructure Components
- Business Applications
- Databases
- Software and Applications including Ellucian Colleague

1.2 Applicability to Staff and Temporary Workers

This Administrative Regulation applies to all current and future employees of YCCD and all current and future consultants and contractors.

1.3 Applicability to External Parties

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

2.0 Change Management

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's.

2.1 Change Roles

The following roles have been established to guide the Change Management process.

- **Customer**: the individual or entity initiating a change. The customer may be an internal YCCD employee or contractor, or an external entity.

- **Product Owner**: the role that qualifies and prioritizes Change Requests from the Customer. The Product Owner may represent interests within a specific entity.
- **Change Implementation Team**: the internal YCCD group responsible for design and implementation of the Change Requests. The Change Implementation Team may consist of the of the following roles.
  - **Designer** – analyzes request needs and determines change requirements.
  - **Developer** – implements the requirements and creates a solution to implement the request.
  - **Tester** – tests the solution for functionality and fit for the request.
  - **Installer** – installs the solution into the production environment.

2.2 Process Tools

The primary tools used to manage Change Requests are the District-wide Help Desk system and an Application Lifecycle Management tool. YCCD currently uses SysAid Help Desk software.

2.3 Change Requirements

The basic requirements for Change Management are:

1. Customers requesting changes that are part of a production environment must follow defined procedures by submitting a Change Request through the SysAid Help Desk system.
   a. The Change Request is authorized by the appropriate administrator.
   b. The Customer submits the Request
   c. The Request is reviewed by YCCD ITS, and the relevant Product Owner.
   d. Once the change has been approved by YCCD ITS, the Change Implementation team schedules and implements the change.
2. All changes to production software must be completely and comprehensively tested.
3. All 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 Change Management team who have a need-to-know.
   a. Segregation of duties must be maintained. Segregation of duties ensures that the individual(s) who develop the solution are not the individual(s) who test and or install the solution into the production environment. This separation helps reduce or eliminate the potential of erroneous or unwanted modification to a production environment.
5. Version controls for source code must be in place to maintain application integrity.
6. All changes implemented 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 to remove personally Identifying Information (PII).

2.4 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 parties with interests in the Request solution.

2.5 Payment Card Industry Considerations

YCCD adheres to the requirements of the Payment Card Industry Data Security Standard (PCI-DSS) for its systems that store, process, or transmit cardholder data. PCI-DSS contains significant security provisions in addition to those required by this Administrative Regulation. PCI-DSS is subject to change without notice. The current Payment Card Industry Data Security Standard may be found here: PCI Security Standards Document library YCCD complies with SAQ-C.