OFFICE OF INFORMATION TECHNOLOGY
CHANGE MANAGEMENT

I. PURPOSE AND SCOPE

This rule lays out Office of Information Technology's (OIT) required steps for any change to an IT resource or information systems.

II. DEFINITIONS

A. **Change**: an event or action which modifies the configuration of any component, Application, Information System, or Service.

B. **Emergency Change**: an event or action which modifies the configuration of any component, Application, Information System, or Service that is made outside the Change Management process with CISO approval.

C. **Information Asset:** data or knowledge stored in any electronic manner and recognized as having value for the purpose of enabling the college to perform its business functions.

D. **Information System:** an application or group of servers used for electronic storing, processing, or transmitting any college data or information asset.

E. **IT Technician**: a college employee who uses industry best practices to develop, administer, manage, and monitor computer resources and assets that support the college's IT infrastructure and ensure compliant IT system security.

III. PROCEDURES

A. Change Execution

1. Prior to executing a change in the production environment, IT Technicians must:

   a. capture the business requirement for the change;

   b. identify the change activity via a unique identifier that will be logged and recorded;

   c. plan and test the change as appropriate;

   d. assess the potential impacts to the confidentiality, integrity, and availability of the information system and information assets;

e. communicate the change details to key stakeholders and other appropriate personnel;

f. capture change rollback requirements to recover from an unsuccessful change;

g. receive approval from the Change Management Board as appropriate; and

h. make change during approved outage window.

B. Post Change Execution

1. After executing a change, IT Technicians must:

a. log the successful or unsuccessful change status; and

b. in the event of an unsuccessful change, document the issue and the lessons learned.

C. Segregation of Duties

1. The college must ensure users cannot access, modify, or use information systems without authorization or detection.

2. OIT must physically, logically, or virtually separate test, development, and production environments.

D. Resources

1. Requesting Changes

a. Users may submit change requests through the Change Management SharePoint Site.

b. The Change Management Committee will consider requests added at least 24 hours prior to the scheduled change control meeting.

2. Change Control Meeting

a. The Change Control Meeting is scheduled weekly and the schedule is accessible on the Change Management SharePoint Site.

b. The Director of Technology is responsible for managing meetings and the importable meeting invitation. Users may attend by invitation only.

3. The Director of Technology will invite users responsible for changes attend scheduled meetings to describe purpose, duration, and planned change schedule.

E. Users responsible for changes must notify their supervisor or CISO once a change has been implemented.

F. Emergency Changes

1. Emergency Change items are logged when approved by the CISO or post execution if time to execute is a consideration.

2. IT Technician or representative responsible for making the Change will attend the next scheduled Change Management meeting to describe purpose, duration, and details of the unplanned Change.