Information Technology Security Plan
Change Management Policy (10.16)

Responsible executive: CIO	Approval date: 7/01/2016
Responsible office: ITS	Effective date: 7/01/2016

Related policies: IT Security Plan

1.0 Policy Statement

Change management requires that all changes to information systems be approved through a documented change management process. A repeatable and auditable change management process will define key roles, responsibilities, escalation procedures, and outline the process for requesting and executing changes to information systems.

2.0 Reason for Policy

The purpose of this policy is to provide guidelines to manage changes to information systems in a predictable manner to ensure service availability is maximized and university business processes are not adversely disrupted by undesirable changes.

3.0 Applicability

This policy applies to all production services and service components, including but not limited to server applications, databases and network components.

4.0 Policy
4.1 Change Management

A change management system should be implemented to manage changes for the following events:

- Introduction or discontinuance of a system or service
- A planned production outage of a significant operation or service
- Significant business or operational changes that would affect business continuity
- Changes affecting computing environmental facilities (e.g., HVAC, electrical)

A Change Management committee should be established, as needed, to review and approve change requests and ensure that change reviews and communications are performed.

Change Management procedures for managing service changes should address the following areas:

- Planning and controlling changes

- Change decision-making and authorization
- Risk assessment and impact analysis
- Remediation planning
- User acceptance testing
- Communications

4.2 Maintenance Management

Maintenance management, for handling routine maintenance and updates to existing architecture, is not required to follow change management procedures it they meet the following criteria:

- Do not add new functionality
- Have standardized and repeatable maintenance procedures
- A roll-back and recovery plan has been developed and is in place
- Do not require a communication plan to be implemented
- Are usually implemented during standard maintenance windows