Change Management Policy (ISP-09)

Document Owner

Executive Owner:	Darrell Morrison
Functional Area:	Information Technology

Authorization

Authorized By:	David J. Hinson
Position:	Interim Chief Information Officer
Signature	
Authorization Date	February 25, 2025

Version History

Issue	Reason For Change	Date
1.0	Initial Release	02/25/2025

Review Period

Information Security Policies are to be reviewed at a minimum annually.

Change Control

Requests for changes to Information Security Policies are to be sent to the document owner providing details of the requested changes and a short justification.

Exceptions

Requests for exceptions to this policy are to be submitted in accordance with the exception policy. Note that all exceptions are time limited to no more than 12 months in duration.

Applicability

This policy applies to all staff and contractors who make changes to IT systems and services.

Table of Contents

Introduction

The process of planning, testing, documenting, and approving changes to system and service configurations enables the maintenance of system availability and compliance with standards and leading practices. This process has been shown to improve system availability and reduce the risk of misconfiguration leading to a compromise.

Objective

The Objective of this policy is to define the roles and responsibilities and high-level procedure for managing change to University IT systems and services.

Policy Statement

General

This policy applies to all IT Systems and services in use by the University regardless of the purchasing and or owning business unit. Changes include but are not limited to the following:

- ✓ Systems (OS Configuration/Patch Management/Code deployment/etc.)
- ✓ Application code and configuration changes (New features requested/etc.)
- ✓ Security changes (Deployment to of new tools, access control lists, and/or firewall rules)
- ✓ Network changes (New devices, configurations)

All changes need to be requested in writing: annotating the target system to facilitate the change. This ensures an audit trail is created for the changes made and when they occurred. The University will implement separation of duties such that change approvers must not be change implementors.

Responsibilities

1. All developers and IT staff members must comply with this policy by raising change requests and ensuring they do not deploy work in production prior to authorization.
2. The IT Director is responsible for implementing and overseeing the change management process to ensure it is enforced, efficient, and effective.

Outline Process for Change Management

1. The change is documented including implementation, backout and implementation test plans.
2. The change is tested in a non-production account.
3. The change has been reviewed and approved for implementation.
4. High risk changes are authorized for execution by the IT Director.
5. Changes are implemented and tested post implementation.
6. The change ticket is closed.
7. The change management process is reviewed quarterly for improvements to enforcement, efficiency, and effectiveness.

Standard Changes

Highly repetitive changes such as creating new user accounts may be designated as standard changes.

These are pre-reviewed and approved to reduce the level of friction and improve efficiency and effectiveness of the process.