I. 5.8.24 Change Management Security Policy

Chapter 5 - Information Technology	Original Effective Date: October 2004
Section: Section 5.8 Information Security	Date Last Reviewed: October 2025
Responsible Entity: Chief Information Security Officer	Date Last Revised: October 2025

II. Purpose

A structured Change Management process can minimize vulnerabilities of information resources, limit their exposure to exploitation and attack, and maximize the protection available to prevent damage to the University.

III. Scope

This policy applies to all current and former faculty, staff, students, residents, healthcare providers, researchers, contractors, or any other third-party entities who have direct or indirect access to Information Resources created, held or maintained by UT Health San Antonio or any controlled affiliate, including, but not limited to its clinics, hospitals, and research operations.

IV. Policy

A. UT Health San Antonio shall adopt Change Management processes to ensure secure, reliable and stable operations to which all Information Resource Custodians and/or Data Owners that support Mission Critical Information Resources or Network Infrastructure are required to adhere. The Change Management process must incorporate procedures for:

1. Formal identification, classification, prioritization and request of scheduled changes;

2. Identification and deployment of emergency changes;

3. Assessment of potential impacts of changes, including the impact on data classification, risk assessment, other security requirements and the institution's operations;

4. Authorization of changes and exceptions by the Data Owner, Information Resource Custodian or System Administrator as deemed appropriate by the risk;

5. Testing changes;

6. Communication plan;

7. Change implementation and back-out planning; and

8. Documentation and tracking of changes.

V. Definitions

There are no defined terms used in this Policy.

VI. Related References

UT System (UTS) Policy
UTS 165.2.3 System Development & Maintenance Standard

VII. Review and Approval History

The approving authority of this policy is the University Executive Committee.

Effective Date	Action Taken	Approved By	Approved Date
10/2004	Policy Origination		
10/2016	Policy Revision		
02/2023	Policy Review/Discretionary Edits		
10/2025	Policy Review/Discretionary Edits	ICPO/CISO	10/2025