Chapter 5	Information Management & Services	Effective:	October 2004
Section 5.8	Information Security	Revised:	October 2016
Policy 5.8.24	**Change Management Security Policy**	Responsibility:	Chief Information Security Officer

CHANGE MANAGEMENT SECURITY POLICY

Overview

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.

Policy

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.

Reference

- U.T. System Policy 165 Standard 7