UTSA Institutional Compliance
Office of Information Security

OIS 5 - Standard for Change Management (Computing Systems)

I. STANDARD STATEMENT

The Change Management Standard provides an outline for the implementation and management of changes to all UTSA computing systems. Change requires serious forethought, careful monitoring and follow-up evaluation to reduce negative impact on the user community and to increase the reliability of system performance.

II. RATIONALE

This standard supports HOP Policy 8-12 Information Resources Use and Security Policy

III. SCOPE

This standard applies to all UTSA faculty, staff, and students.

IV. CONTACTS

informationsecurity@utsa.edu

V. PROCEDURES

A. Each department is responsible for defining and documenting its own change management processes, covering changes to resources such as operating systems, computer hardware, networks, and applications and applying the practice to all multi-user systems. The changes must be documented commensurate with risk, scaling from simple change logging to the following processes for mission critical systems of those with confidential data:
  1. Planning the change
  2. Testing the change (if suitable test systems exist)
  3. Obtaining formal approval to implement the change in production
  4. Communicating with users of the system before the change occurs, especially if there are interdependencies with other systems.
  5. Implementing the change
  6. Documenting the results of the change.
B. All changes affecting any central computing systems supported by University Technology Solutions (UTS) must be managed through all of the steps above, and must be thoroughly documented.

Title: OIS 5 – Standard for Change Management (Computing Systems)
Effective Date: June 1, 2011
Last Reviewed: August 10, 2020