UTEP Standard 7: Change Management

The purpose of the Change Management Standard is to manage and document changes in a rational and predictable manner so that staff and clients can plan accordingly. Changes require serious forethought, careful monitoring, and follow-up evaluation to reduce negative impact to the user community and to increase the value of Information Resources. Please refer to The University of Texas at El Paso Change Management Guidelines for additional information and requirements, as warranted by The University of Texas at El Paso Data Classification Standard and commensurate with the risk and value of the system/data.

7.1 Change Management Requirement. All changes to UTEP Information Resource infrastructure such as, but not limited to, operating systems, computing hardware, networks, and applications must follow Change Management Procedures and adopt Change Management processes to ensure secure, reliable, and stable operations to which all offices that support Mission Critical Information Resources or Network Infrastructures are required to adhere.

(a) Colleges, schools, or units responsible for Information Resources will ensure that the change management procedures and processes they have approved are being performed;

(b) identification and deployment of Emergency Changes;

(c) assessment of potential impacts of changes, including the impact on Data classification, Risk assessment, and other security requirements;

(d) authorization of changes and exceptions;

(e) testing changes;

(f) change implementation and back-out planning; and

(g) documentation and tracking of changes.

7.2 All changes affecting computing environmental facilities (e.g., air-conditioning, water, heat, plumbing, electricity, and alarms) must be logged and reported to the appropriate college, school or unit managing the systems in that facility.

7.3 Colleges, schools, or units may object to a scheduled or unscheduled change for reasons including, but not limited to, inadequate planning, inadequate backup plans, the timing of the change will negatively impact a key business process such as year-end accounting, or if adequate resources cannot be readily available. Adequate resources may be a problem on weekends, holidays, or during special events. The responsible party will review all objections. A security exception request may be submitted to the CISO if there are objections to a planned change that is triggered by security requirements;

7.4 A Change Management Log must be maintained for all significant changes, including emergency changes. The log must contain, as a minimum, the:

(a) date of the submission and date of the change

(b) owner and custodian contact information;

(c) system administrator contact information;

(d) nature of the change

7.5 Information Resources Custodians. All Custodians must implement and adhere to approved UTEP Change Management processes to ensure secure, reliable, and stable operations.

7.6 Revision History

First Draft:	April 2, 2002
Revised:	September 19, 2002
Revised:	May 26, 2011
Revised:	May 12, 2017
Approved:	May 12, 2017 Gerard D. Cochrane Jr., Chief Information Security Officer