TEXAS TECH UNIVERSITY HEALTH SCIENCES CENTER EL PASO

Operating Policy and Procedure

HSCEP OP: 56.01, 1.4.5 CHANGE MANAGEMENT

PURPOSE: The following change management protocols apply to the Institutional IT units as well as the regional campuses' IT departments. The I.T. Division highly recommends that all departments adopt these industry best practices related to IT change management in their respective areas. A change is defined as a modification to the hardware, software, and documentation managed by Information Technology that has a reasonable possibility of impacting normal operations of those resources

REVIEW:

POLICY/PROCEDURE:

1. **Change Definition**

Items that are considered changes include, but are not limited to:

- Installation or upgrades of server, networking, or security hardware or software, including patches and interim fixes,
- Modification of hardware or software that affects the operation of desktop computers connected to the TTUHSC El Paso network,
- Modification of server, network, or security settings that affect access to I.T. resources, and
- Modification or enhancements to the physical environment that supports I.T. resources.

Specific tasks that should not be considered changes include:

- Creation of new file shares, or modification to permissions of existing shares,
- Installation, activation, or removal of network cable drops, or
- Creation, modification, or deletion of accounts and mailboxes.

2. **Change Categories**

Changes will be classified into three categories:

- Category 1 - This category includes changes to resources that provide service to a large number of internal or external I.T. customers, or customers at multiple regional locations.

- Category 2 - This category includes changes to resources that provide service to a moderate number of I.T. customers within a specific location.
- Category 3 - This category includes changes for a single department or smaller group of users at a specific location.

3. **Procedures**

All changes must be documented, and submitted for approval prior to implementation. The following defines the procedure for documentation and approval.

4. **Documentation**

The requester initiating the change must initiate a Request Creator process via the STARS system (http://www.ttuhsc.edu/IT/STARS/roles/default.aspx). The following information must be provided on this form:

- Submission date - Date the change form is submitted for approval,
- Change date and time - Proposed date and time the change will be performed,
- Change duration - Estimated length of time for the change to be completed,
- Control Number - Change Identification number which uses the date of the request and a sequential number for multiple requests originated on the same date starting with 001 in the following format: YYYYMMDD-NNN,
- Change category - See prior section for definition,
- Change Purpose - Fifty character summary of the Change Description,
- Change description - Explanation of the change,
- Impact description - Campus and departments or groups of customers that will be affected by the change,
- Test procedure - Description of the testing performed for the change, if applicable,
- Back-out procedure - Procedure for backing out the change if the implementation is not successful, and
- Back-out duration - Estimated time to back out the change.

The technician's manager will record the change request in a common Change Request Log maintained by the Managing Director of Network, Security, and Systems.

5. **Processing**

After the requester completes the Change Approval Form, it will be submitted to their supervisor or manager for review/approval. The approver will ensure the form is completed and information provided is adequate for decision making. The managers will meet with the authorized approver for Network Services, Information Security, Systems, or schools as needed to review and document recommendations. Change forms must be submitted to the approver of the applicable areas a minimum of one full business day prior to the review date.

If the authorized approver is unavailable for the weekly meeting, the managers will meet to discuss and make recommendations for the change requests. The authorized approver must be notified of all category 1 and 2 changes before implementation.

All changes will be forwarded to I.T. Executive Management (consisting of the CIO, AVP of Information Services, AVP of Security and Infrastructure Assurance, and Managing Director of Technology Services) for final disposition of the request.

Category 1 and 2 changes can be implemented no sooner than two full business days after approval. Category 3 changes can be implemented immediately after approval, according to the change date and time on the approval form.

Announcement messages must be distributed prior to all category 1 and 2 changes. Message content should include impact to user and training provided if applicable. The supervisor or manager should prepare this announcement prior to the change review meeting. The authorized approver will be responsible for posting the announcement.

Changes that are backed out during or immediately after implementation must be resubmitted for approval.

6. **Emergency Changes**

Occasionally, it may be necessary to implement changes before the next weekly change approval meeting. These changes will be designated as emergency changes, and will be documented as Emergency (E) Category, a category E1, E2, or E3.

All of the above documentation and approval procedures still apply for emergency changes, except these changes can be immediately submitted to the supervisor, and subsequently the CIO, for approval and implementation.

Emergency change requests should only be submitted when I.T. operations or security will be negatively impacted or compromised if the change is not implemented immediately.