The University of Texas at El Paso
Information Security Office
Change Management Guidelines

Contents

Purpose

These Change Management Guidelines[1] serve as a supplement to The University of Texas at El Paso Information Resources Use and Security Policy, the University of Texas at El Paso's implementation of UT System UTS 165. The purpose of these guidelines is to manage changes in a rational and predictable manner so that staff and clients may plan accordingly.

Scope

These guidelines should be applied in proportion to the respective data classification category, the availability requirements of the data, and the impact of the change on the user community. (See Data Classification Standard).

Roles and Responsibilities

Each department or entity is responsible for defining its own change management process. In addition to the sensitivity and importance of the IT resource being managed, the organizational structure of the entity, as well as its IT and business processes, should be taken into account when designing the change management process.

Communication

Communication before, during and after the change is one of the most important parts of change management.

- Make sure that adequate advance notice is given, especially if a response is expected.
- Make sure that it is clear whom people should respond to, if they have comments or concerns.
- Some suggested communications are provided at each step of the change management process described below.

Maintenance Window

A maintenance window is a defined period of time when maintenance, such as patching software or upgrading hardware components, may be performed. Clearly defining a regular maintenance window can be advantageous as it provides a time when users should expect service disruptions.

Change Committee

The change committee (also known as the Change Control Board) reviews change management requests and determines whether or not they should be implemented. In addition, it may determine that certain changes to the proposed plan for implementing the change must be made in order for it to be acceptable.

The change committee may consist of as little as one person, or it may be a group of people, depending on who should be involved in the process. In addition, the membership of the committee might be formally defined, or it might change depending on the nature of the change, or the systems involved. For the Information Resources and Planning Division, it may consist of one, some, or all of the following: Vice President for Information Resources and Planning; Enterprise Computing Director; Telecommunications Infrastructure Director; Technology Support Director; Chief Information Security Officer; and/or other Vice President. Each area must determine the membership depending on their needs and the specific resources in question.

[1] Adapted from the "Change Management Guidelines" (previously located at http://www.utexas.edu/its/policies/opsmanual/chgmgmt.php; now at https://security.utexas.edu/policies/change_management), with permission from ITS, The University of Texas at Austin, Austin, Texas 78712-1110

Critical Changes (and bypassing the process)

In some cases, events are critical enough that they must be rushed into production, creating an unscheduled change. Each situation is different, and even though some steps might be bypassed, as much consideration as possible should be given to the possible consequences of attempting the change. It is still important to obtain sufficient approval for the change. What constitutes "sufficient approval" will vary, and should be defined by the department or department/business unit.

Test the Change

- If a test environment is available, the change should be tested.
- Detailed discussions and tabletop testing should supplement testing in a test environment. They may also be used as an alternative if test equipment is not available.
- Look for unintended consequences that might result in stability or security issues.
- Communicate the results of the tests to supervisory staff and the change committee, so that final approval may be granted.

Obtain Approval to Move Forward with the Change

- The Change Management Request Form (Full or Abbreviated) and the results of testing should be presented to the change committee.
- The change committee should weigh the risks and benefits of making the change as well as the risks and benefits of not making the change.
- The change committee may alter the plan or send it back for revision, if it determines that certain aspects of the change proposal are unacceptable or need more work.

Execute the Change

- Make sure that support staff is available and prepared to assist in the change process.
- If system availability will be affected while the change is being implemented, notify affected individuals letting them know what to expect and when to expect it. They should also know whom to contact in case they experience difficulty as a result of the change.
- Verify that the change was successful and that the system is stable.
- Notify affected individuals that changes are complete.
- Provide documentation and instruction to users that will be affected by the change.
- Record that the change took place in the change log.

Maintain a Record of the Change

- Maintaining a record of the change management process may help determine the history of an information resource, as well as provide proof that the change was approved.
- After the change has been implemented, record it in the change log. Sample change logs are provided below to help you decide how to document your changes.
- Archive the change management documents that were completed during the process. This does not meant to imply that actual paper copies of the associated documents must be kept.

Documenting Change Management Requests

Different systems require different levels of documentation for change management requests.

Full Change Management Request Form

A full change management request form provides detailed information about the change and is appropriate for changes affecting data classified as Category I (highest, most sensitive) where protection is required by law, the asset risk is high and is information which provides access to resources, physical or virtual. (See Data Classification Standard.) A record of when the change was performed must be maintained. The sample change log below may be used to do this.

The University of Texas at El Paso
(UTEP**)**
PCI Full Change Management Request Form

CHANGE REQUEST TYPE:
☐ Software ☐ Hardware ☐ Interface

INSTRUCTIONS
Completed forms should be submitted to your primary supervisor. Your supervisor will forward this to the IT department.

End User Information

End User Name:		Service Desk# (if applicable) Phone:	
Department:		Email Address:	

Machine Location

Please list the room of the machine(s) which are affected by this change management request.

Machine Location:	

Software

Platform: ☐ **Windows** ☐ **Macintosh** ☐ **Linux**

Existing Software:	Application Name:		Version:	
Description of Issues:				
New Software:	Application Name:		Version:	

Important Note: A copy of the license and software for each new software request must be submitted with this change management request for non-site licensed software

Hardware (Additional Peripherals)

Type of Machine: ☐ PC ☐ Macintosh ☐ Linux

Type of Peripheral: ☐ Printer ☐ Scanner ☐ Other – please specify:

Description of Issues:

New Hardware: Make/Model: Serial No:

Requestor Signoff

As the end user specified on this form, I certify that the information provided in this document is both true and accurate. I also certify in the case of software changes that my department is in possession of sufficient licenses for the application.

The end user also recognizes they may be called upon to provide further information to complete this request. UTEP will undertake all best efforts to ensure that changes are implemented within the appropriate timeframe. However, the end user recognizes that should the end user fail to provide assistance in a timely manner when asked there will be unavoidable delays to the deployment of the requested changes.

End User Signature **X** Date: / /

End User's Supervisor

Completed By: Signature: **X** Date Received: / /

(print name)

Enterprise Computing Systems Support / Departmental Systems Administrator Use Only

Received By: Signature: **X** Date Received: / /

(print name)

Change Control Board Use Only (EC / TI / CISO / VPIRP)					
Type of change:	☐ Minor/Pre-approved ☐ Major				
CCB Outcome:		☐ Not Approved ☐ Approved			
Approved By:	(print name)	Signature:	**X**	Date Approved:	/ /

Abbreviated Change Management Request Form

An abbreviated change management request form should be used for changes affecting data classified as Category II (moderate level of sensitivity) where the University of Texas at El Paso has a contractual obligation to protect the data, the asset risk is medium and is an institutionally provided service or Category III (very low but still some sensitivity) where there is no legal requirement for data protection, asset risk is low and there are no other institutional risks. (See Data Classification Standard.) Each change should be entered into a change log. In some cases, it may be possible to combine the abbreviated change management request form and the change log into a single form.

Change Management Requested By: *Enter requester name and e-mail address. If request came from external source then enter your name and external source name.*
Date of Change Request: *Enter date/time of request here.*
Change Description: *Enter a summary of the change required and a reason for the change.*
Change Priority: *Please provide a change request of Urgent, High, Medium, or Low. If this change is time/date dependent then please specify this here. Note: The change control committee may amend above priority/schedules dependent on other activities.*
Impact Assessment: *Enter a summary of the business and technical functions that could be affected by these changes. This section should specify known risks and concerns.*
Pre-Deployment Test Plan: *Describe how you will test the change before deployment. Note: Testing changes will greatly reduce possibility of failures and unwanted surprises.*
Back Out Plan: *Describe how a failed change could be backed out or how the resource could be restored to its previous state.*

Post Deployment Test Plan: *Describe how the change is tested to determine whether it was successful.*

Change Approval: *Specify whether request has been accepted or rejected. The change control committee should make this decision. The decision of the change control committee is that this request be:*

Accepted	**Rejected**

If appropriate, a description of the decision should be described here.

Change Assignment: *Specify the person responsible for implementing the change.*

Change #		**Date of Request**	*Creation date*
Request Name:	*A short name that can be used to refer to this specific change*		
Description of Change	*Describe Change Here*		
Priority (U,H,M,L)	*The priority of this specific change. It can be urgent, high, medium, or low.*		
Assigned to	*The person responsible for implementing the change.*		
Approved by	*The person who approved the change.*		
Status			

Logging Changes

Below is an example of fields you might use in a simple change log. (See Data Classification Standard.)

Change #	Request Name	Performed By	Date	Time

Revision History

Version	*Date*	*Author*	*Description of Change*
1.0	October 1, 2007	ISO	Document Created
1.1	October 29, 2007	ISO	Minor Changes; Reviewed and converted to PDF to post on ISO Webpage
2.0	February 24, 2017	ISO	Document revised to reflect current requirements; fix broken links; removed “Planning the Change”.
2.1	March 1, 2017	ISO	Converted to PDF to post on ISO Webpage

Approvals

Name	*Title*	*Role*	*Date*
Gerard D Cochrane Jr	Chief Information Security Officer	Approval	10/01/2007
Gerard D Cochrane Jr	Chief Information Security Officer	Approval	10/29/2010
Gerard D Cochrane Jr	Chief Information Security Officer	Approval	02/24/2017