

# Change Management Guidelines

---

1. Purpose .....	1
2. Scope.....	1
3. Guidelines .....	1
4. Documenting Change Requests .....	4
5. Revision History .....	6
6. Approvals .....	6

## 1. Purpose

These guidelines serve as a supplement to [Information Resources Use and Security Policy](#), the University of Texas at Austin’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 can plan accordingly.

## 2. 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](#)).

## 3. Guidelines

Each department, unit, 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.

### 3.1. 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.

## **Change Management Guidelines**

**Document Version:** Approved

- Some suggested communications are provided at each step of the change management process described below.

### **3.2. Maintenance Window**

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

### **3.3. Change Committee**

The change committee reviews change requests and determines whether or not they should be made. 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. Each area must determine the membership depending on their needs and the specific resources in question.

### **3.4. 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 business unit.

### **3.5. Plan the Change**

Determine the following information during the planning process:

- Who is responsible for the change
- What effect the change will have
- When the change should occur, based on the following factors:
  - When will the change have the least chance of interfering with operations?
  - Will appropriate support staff be available?
  - Can the change be made within the standard maintenance window?
  - Will there be enough time to review and test the proposed change?
- Why making the change is important
- How the change will be made

- If the change will result in any additional security issues or increase the risk to the system
- Back-out procedures in case the change is not successful.
- What additional training and documentation will be necessary for both support staff and end users

Let others know about the proposed changes. This can be as formal as a change request form, or as simple as e-mail message to concerned parties.

### 3.6. 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 can be given.

### 3.7. Obtain Approval to Move Forward with the Change

- The change request form 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.

### 3.8. 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 made, 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.

### 3.9. Keep a Record of the Change

## Change Management Guidelines

Document Version: Approved

- Keeping a record of the change management process can 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](#) to help you decide how to document your changes.
- Archive the change management documents that were completed during the process. This does not mean to imply that actual paper copies of the associated documents must be kept.

## 4. Documenting Change Requests

Different systems require different levels of documentation for change requests.

### 4.1. Full Change Request Form

A full change 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 kept. The sample change log below could be used to do this.

<b>Change Requested By:</b> <i>Enter requester name and e-mail address. If request came from external source then enter your name and external source name.</i>
<b>Date of Change Request:</b> <i>Enter date/time of request here.</i>
<b>Change Description:</b> <i>Enter a summary of the change required and a reason for the change.</i>
<b>Change Priority:</b> <i>Please give 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.</i>
<b>Impact Assessment:</b> <i>Enter a summary of the business and technical functions that could be affected by these changes. This section should specify known risks and concerns.</i>
<b>Pre-Deployment Test Plan:</b> <i>Describe how you will test the change before deployment. Note: Testing changes will greatly reduce possibility of failures and unwanted surprises.</i>
<b>Back Out Plan:</b> <i>Describe how a failed change could be backed out or how the resource could be restored to its previous state.</i>
<b>Post Deployment Test Plan:</b> <i>Describe how the change is tested to determine whether it was successful.</i>

**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.*

#### 4.2. Abbreviated Change Request Form

An abbreviated change request form should be used for changes affecting data classified as Category II (moderate level of sensitivity) where UT Austin 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 request form and the change log into a single form.

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

#### 4.3. 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

## Change Management Guidelines

Document Version: Approved

### 5. Revision History

Version	Date	New	Original
	2/25/2011	Converted web page to PDF	No changes
	4/1/2010	Updated text on the University Identification Card Guidelines to read: "Broken ID Cards: ID Cards must be replaced if they are broken or mutilated. The remaining pieces of the card must be returned to the ID Center. ID Cards that break or become unreadable will be replaced at no cost. The ID Center will reserve the right to apply a replacement card charge in the event the cardholder requests an inordinate number of card replacements over the course of their possession of the ID card (e.g., due to negligent care of the ID Card)."	"Broken ID Cards: ID Cards must be replaced if they are broken or mutilated. The remaining pieces of the card must be returned to the ID Center. ID Cards that break or become unreadable solely due to normal wear will be replaced at no cost. Replacement costs for mutilated cards (holes punched, other abnormal use) are the responsibility of the individual." "
	10/1/2009	Updated visual appearance to new template. Corrected any out of date links to ensure they are pointing to the most current policy documents.	
	9/14/2007	Changed references from BPM 53 to UTS 165.	"BPM 53"
	6/27/2007	Removed from section III, "Planning the Change" the list item "Can the maintenance be performed within the standard maintenance window?" because of redundancy. Changed "a" to "the" in "Can the change be made within the standard maintenance window?"	"Can the maintenance be performed within the standard maintenance window? " "Can the change be made within a standard maintenance window?"

### 6. Approvals

Name	Role	Members	Date
Chief Information Security Officer	Approval	Cam Beasley	March 3, 2011