

# UNIVERSITY OF UTAH OIT AND ITS OPERATIONS POLICY

---

## OIT and ITS – CHANGE MANAGEMENT

**Revision Date:** 10/15/2008

**Chapter or Section:** Information Technology

---

### **I. PURPOSE**

The purpose of this policy is to define standard Change Management principles, roles and processes for use across OIT and ITS.

### **II. DEFINITIONS**

Change Management is an important piece of the ITIL framework. The ITIL Change Management process depends on effectively managing risk and maintaining accurate configuration data, which will assist in better understanding the impact of IT changes. There is a very close relationship between Change Management and other ITIL disciplines such as Configuration Management and Release Management.

Change Management is the process of planning and coordinating the implementation of all changes into the production environment in a logical and risk mitigated process.

### **III. POLICY**

- A. The Information Technology Service Management team will facilitate definition of procedures, metrics, and documentation necessary to implement change management for OIT and ITS.
- B. The procedures, metrics, documentation, etc. will be submitted to the Change Management Board (CMB) for approval.
- C. The CMB, chaired by the Director of IT Infrastructure and Operations, will be the governing authority for change management policy, procedures and metrics. The CMB will also serve as the final authority for appeals from the Change Advisory Board (CAB). OIT and ITS Leadership will serve on this board, or appoint delegates.
- D. The CAB reviews requested changes, risk level, their disposition, and coordinates scheduling. OIT and ITS Leadership will identify members of this board.

### **IV. SCOPE**

- A. The Change Management Policy applies to all providers of IT services and all requesters of changes to those services provided by OIT and ITS.

#### **PROJECTS**

The definition, creation and management of projects ARE NOT within the scope of change management. However, where project delivery will affect the production environment, the onus is on project managers to follow this change management process.

## **ROLES, RESPONSIBILITIES and GOVERNANCE**

**Change Requestor:** The person or business requesting or filing the Downtime Event Management Notification/Request For Change (DEMNRFC) notice.

**IT Operations Change Managers:** The stewards of the Change Management Process. Acts as liaison between implementers, requestors and approvers (CAB / CMB). Accountable to the CAB and CMB. The roles and responsibilities include:

- Review and filtering of changes
- Establishment of priority & impact in conjunction with the change requestor
- Review of benefits, justifications, risks & issues.
- Convener of the CAB
- Escalation to the CMB
- Management reporting, metrics etc...
- Review change(s) after implementation
- Maintenance of the change calendar

The IT Operations Change Managers are the ITSM Team.

**IT Operations Change Advisory Board (CAB):** The role of the CAB is to review all requested changes, approve or reject them and schedule them appropriately. The CAB will have broad representation from OIT and ITS. The CAB will meet weekly to review all DEMNRFC's and approve or reject them and schedule them appropriately.

The IT Operations CAB consists of: The Associate Director of Service Management, the Associate Director of Networks, the Associate Director of Enterprise Systems, Campus Help Desk Manager, ITS Help Desk Manager, Associate Director of OIT Services, Campus Network and Operations Services Manager, OIT Customer Account Manager, Info Security Operations Manager, Field Operations Manager, Data Center Manager, OIT Communications Manager, CIS Representative or assigned proxies.

**CAB/ Emergency Change Committee (CAB/EC):** Subset of full CAB.

The IT Operations CAB/EC is any two out of the three -- The Associate Director of Service Management, the Associate Director of Networks, the Associate Director of Enterprise Systems or assigned proxies. The CAB/EC can be convened with short notice to assess an Emergency change.

**Change Management Board (CMB):** The Change Management Board will be the governance authority for policy/procedures approval, metrics review, change appeal approval, conflict resolution, and approval for go-live procedures for major initiatives.

The IT CMB membership consists of the following: Campus CIO, University Hospital & Clinics CIO, Director of IT Infrastructure and Operations, Campus Enterprise Architect. The CMB is chaired by the Director of IT Infrastructure and Operations.

**Change Implementer:** Individual(s) actually making the changes in the environment

**Change Notification Group:** The affected business unit and IT staff who benefit from knowing what changes are approved and when they are scheduled to be implemented. Users will receive notification about any possible service interruption caused by the change in a timely manner.

### **Change Windows**

- Change Windows are pre-determined time frames in which changes are explicitly declared to be allowed or not allowed. These time frames are generally after business hours, and may be determined by risk or business impact. Weekdays are from 7 p.m. to 7 a.m. Weekends are from 4 p.m. to 8 a.m. Preventative maintenance changes should be planned and scheduled when most feasible.
- Change Moratoriums are time frames when changes are not allowed. The CAB will propose Change Moratoriums. Change moratoriums will be approved by the CMB and advertised monthly by the Change Manager. Examples of possible change moratorium windows would be end-of-month (due to data financial processing), major holidays when staffing will be lower than usual, or time frames surrounding major business events.

### **Change Lead Times**

- Routine changes will be submitted for approval to the Change Manager at least 10 days prior to the planned change date/time.
- Any changes submitted less than 10 days prior to the proposed change date/time will be considered 'Emergency' changes and subject to the 'Emergency' Change Approval process. The Emergency process has all the same procedural requirements as routine changes. Emergency changes need only be approved by the CAB/EC.
- Changes in the RFC process which were previously classified as "High Priority" changes will now be categorized as Emergency.

### **CHANGE CALENDAR**

The Change Calendar contains all scheduled changes (including outages, maintenance etc.) and moratoriums, which will help identify major conflicts in the schedule and provide updated information to stakeholders. The Change Manager is the owner of the Change Calendar. Change notifications to stakeholders for calendar changes will be delivered through the Service Desk. The Change Calendar can be viewed at: <http://itsmalt2/demntimeline/>

### **CHANGE SCHEDULING**

The CAB will determine when changes will be deployed in conjunction with the Change Requester. The CAB will consider the urgency and impact of the change, the existence of any dependant changes and resource availability.

In addition, some systems may have scheduled maintenance windows. The Change Manager and CAB will take these into account when determining a timeframe for a specific Change. Such scheduled maintenance windows will be represented in the Change Calendar.

### **CHANGE REQUEST and/or JUSTIFICATION**

Created by Change Implementer and Change Requester (if needed). The request simply describes the business or technical effort driving the change and the risk associated with the change.

### **CHANGE RISK ASSESSMENT**

Change Risk Assessments describe the risk to the business if the change is not done; the risks involved with doing the change and includes steps that can be taken to mitigate risk associated with the change. Also, considering if the requested change deviates from published or implied technical or operational standards in place at the University of Utah.

### **CHANGE IMPLEMENTATION PLAN**

Created by the Change Implementer and Change Requester (if needed). Change implementation plans describe, in detail, how a change is to be successfully done. Change implementation plans will be followed to achieve the desired outcome. The detail and specifics required in the plan are driven by the change's risk level.

#### **CHANGE TEST PLAN**

Created by the Change Implementer and Change Requester. Testing plans are followed to verify that the change can accomplish the desired outcome. The detail and specifics required in the plan are driven by the change's risk level and complexity.

#### **CHANGE BACKOUT PLAN**

Is created by the Change Implementer and Change Requester and describes how a change will be reversed, or the affected system be placed back into original state should a change action fail. The detail and specifics required in the plan are driven by the change's risk level and complexity.

#### **POST IMPLEMENTATION TESTING AND VALIDATION REVIEW (PIR)**

All changes must be verified and tested after deployment and noted in the change documentation. The review will note the success/failure of the change. The review will also note how well the actual change action conformed to the original change request in terms of fitting within the Change Window, Implementation steps and Testing steps. The detail and specifics required in the PIR are driven by the change's risk level and complexity.

#### **CHANGE APPROVAL or DISAPPROVAL**

All changes submitted and meeting the standards set within this policy will be considered approved pending review of the Change Manager and CAB. If there are questions or issues with any part of the change, the change requestor will be contacted. Otherwise, the change will be allowed to move forward as scheduled.

#### **INFORMATIONAL and/or STANDARD CHANGES**

Informational and Standard changes are changes used in the current ITS and OIT organizations which are not required to conform to the change lead time standards. However, each team must maintain a list of what they consider to be their approved Informational and/or Standard changes. This list, as well as any on-going revisions to this list must be submitted to the Change Manager(s) for review and approval by the CAB. Each change on the Informational and/or Standard change list must be documented in compliance with all other aspects of Planned Changes contained in this policy. Any changes not submitted as Planned changes, or not contained in the Informational or Standard list will be considered Unauthorized Changes.

#### **UNAUTHORIZED CHANGES**

Changes deployed to the production environment that do not follow this change management policy may lead to disciplinary action up to, and including, termination.

#### **PROCESS OWNERSHIP:**

The IT Operations Change Management Process Owner (CMPO) is the Associate Director of Service Management.

The CMPO owns the process and the supporting documentation for the process. The CMPO provides process leadership to the IT organization by overseeing the process and ensuring it is followed. When the process isn't being followed or working well, the CMPO is responsible for identifying why and ensuring actions are taken to correct the situation. In addition, the CMPO is responsible for all changes to the process, and development of process improvement plans.

## ***Change Management Policy - Quick Reference Guide***

The following statements define the Change Management Policy:

1. All Planned DEMN's/RFC's, regardless of urgency, impact and type are subject to the Change Management policy. This includes any DEMN/RFC that is being implemented by a third party vendor or contractor.
2. For a change to be considered by the CAB, the required documentation, such as technical specifications, implementation plan, test plan, a back-out plan and risk assessment must be attached to the change. The quantity of documentation required will be dependent on the type of change as well as the risk and complexity associated with the change.  
For example, each Planned DEMN/RFC should have the following headings with supporting descriptions and/or documentation:
  - Request or justification
  - Assessment of possible impacts, and steps taken to limit negative impacts (risk assessment)
  - Planning and testing
  - Communication
  - Back out procedures should the change be unsuccessful
  - Testing and validation of success
3. The CAB will meet weekly to review all DEMNs/RFC's and approve or reject them and schedule them appropriately.
4. The CAB/EC can be convened with short notice to assess an Emergency change.
5. A DEMN/RFC can be rejected by the CAB for a number of reasons, such as (but not limited to):
  - a. Resources are unavailable to execute the change
  - b. Insufficient planning and documentation
  - c. Insufficient testing authorization and documentation
  - d. Scheduling considerations
  - e. Risk too high
6. Users will receive notification about any possible service interruption caused by the change in a timely manner.
7. As part of the implementation procedure, all changes must follow the test plan, be fully tested with test sign-offs and documentation complete.
8. All changes must be verified after deployment and the verification is included in the change documentation.
9. The Change Managers will maintain the Change Calendar and make it available to the institution. Necessary notifications will be delivered via the Service Desk.

### **V. ENFORCEMENT**

- A. The Change Management Board is responsible for monitoring and enforcement of this policy and approved procedures. A violation of this policy may lead to disciplinary action up to, and including, termination.

APPROVAL BODY:	CMB
APPROVAL DATE:	pending
POLICY OWNER:	Associate Director of Service Management
ORIGIN DATE:	pending