UNIVERSITY OF UTAH - IT OPERATIONS POLICY

UIT – CHANGE MANAGEMENT POLICY
Chapter or Section: Information Technology

ID	SOP-CNFM.001 – UIT Configuration Management Policy		
Rev	**Date**	**Author**	**Change**
4.4	9/29/11	Joe Bernhard & Brad Petrucci	11/22/2011

PURPOSE

The purpose of this document is to define the Change Management policies for use across UIT.

OBJECTIVE

The objective of change management is to implement changes in the production environment in a logical and methodical way which mitigates risk and maintains a stable environment.
The ITIL Framework for Change Management process depends on effectively managing risk and maintaining accurate configuration data, which will assist in better understanding the impact of IT changes.

SCOPE

This Change Management Policy applies to all changes to UIT provided environments and services.

The definition, creation and management of projects ARE NOT within the scope of the change management policy. Early in the project process interaction with the change management process is encouraged for success. When production services are changed, Project managers are required to follow the Change Management processes. Projects or complex changes are implemented using Release Management.

All data centers are in scope of the change management policy. This includes Komas, Marriot, West Temple and Park Data Centers.

POLICY

A. The UIT Service Management team will facilitate definition of procedures, metrics, and documentation necessary to implement change management for UIT.

B. Policy and Process guide documents will be submitted to the Change Management Board (CMB) for approval. These documents will be reviewed on a regular periodic basis and any modifications will follow the change process.

C. The CAB reviews requested changes, risk level, their disposition, and coordinates scheduling. The Director of IT Infrastructure and Operations will identify members of this board. The CAB is chaired by the change manager.

D. This policy document applies to any and all Data Center environments and services. This includes physical inventories, locations and movement of tracked items within the data centers.

E. All Requests for Change are subject to the Change Management policies. This includes any RFC that is being implemented by a third party vendor or contractor.

F. All changes must be verified after implementation and the verification is included in the change documentation as part of closure and available to the CAB for review.

G. Unapproved changes may lead to disciplinary action.

H. A Change Calendar will be maintained and published.

I. The UIT Service Management team will monitor the implementation of changes through established metrics for changes.

J. The UIT Service Management team is responsible for monitoring this change management policy and associated process and procedures.

GOVERNANCE

Compliance with Governance requirements when applicable are strictly followed, such as:

Sarbanes-Oxley Act (SOX)

Health Insurance Portability and Accountability Act (HIPPA)

Family Educational Rights and Privacy Act (FERPA)

Information Security Office (ISO)

University of Utah disclosure policies

POLICY INFRACTIONS

This is a binding policy document approved by the executive management for change control.

Any infractions of these policies are subject to disciplinary action.

Exceptions to these polices can only be approved by the CMB.

APPROVAL BODY:	CMB (Jim Livingston)
APPROVAL DATE:	11/22/2011
POLICY OWNER:	Associate Director of Service Management
ORIGIN DATE:	9/28/2011

ROLES, RESPONSIBILITIES, PROCEDUREs

Change Submitter: The person or business requesting or filing the Request For Change (RFC) notice.

IT Operations Change Manager: The steward of the Change Management Process. Acts as liaison between submitters 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 submitter
- Review of benefits, justifications, risks & issues.
- Convener of the CAB
- Escalation to the CAB/EC or CMB
- Management reporting, metrics etc.
- Review change(s) after implementation
- Maintenance of the change calendar

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 UIT. The CAB will meet weekly to review all RFC'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, UIT Help Desk (Campus and Hospital) Manager, Associate Director of UIT Services, Campus Network and Operations Services Manager, UIT Customer Account Manager, Info Security Operations Manager, Field Operations Manager, Data Center Manager, UIT Communications Manager, The Assistant Director UIT Application Systems & Infrastructure, CIS Representative or assigned proxies.

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

The UIT Operations CAB/EC is any two out of the five -- The Associate Director of Service Management, the Associate Director of Networks, the Associate Director of Enterprise Systems, the Director of Application Services, The Assistant Director UIT Application Systems & Infrastructure, Associate Director UIT Voice Systems and Business Administration, and Manager-Service Management Process Support 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 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. Change Submitter is responsible to inform the users that they receive notification about any possible service interruption caused by the change in a timely manner.

Change (Maintenance) 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. After-business hours are considered to be: Weekdays from 7 p.m. to 7 a.m. Weekends 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, Major Academic Events or time frames surrounding major business events.

Change Lead Times

- Major changes will be submitted for approval to the Change Manager at least 10 days prior to the planned change date/time.

- Minor changes will be submitted to the Change Manager at least 10 days prior to the planned change date/time. These changes are pre-approved by default

- Urgent changes will be submitted to the Change Manager for those changes less than 10 days prior to the planned change date/time. And subject to the 'Urgent' Change Approval process. The Urgent process has all the same procedural requirements as routine changes. Urgent changes need only be approved by the CAB/EC.

- Standard changes will be submitted to the Change Manager for approved Standard changes to be completed within the next or future Change Maintenance window for that system.

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. The Change Timeline can be viewed at: http://itsmalt2/demntimeline/. The Change Calendar can be accessed at http://cmsworkflow1.med.utah.edu/RFCviewer/ .

CHANGE SCHEDULING

The CAB will determine when changes will be deployed in conjunction with the Change Submitter. 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 change 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 (Reason for Change)

Created by Change Submitter. 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 include 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. Describe any service disruptions the change might cause.

CHANGE IMPLEMENTATION PLAN

Implementation plan are created by the Change Submitter. 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.

PEER REVIEW

The Change Submitter should have someone on their team review the Change Implementation Plan. This will assist the Change Submitter in allowing someone else to go through the steps in the Implementation Plan.

OTHER TEAMS ASSISTANCE REQUIRED

Some Changes require that other teams do some action before/during/after the change. Change Submitters should indicate on the RFC that other teams are required to assist this change. The Change Submitter should indicate which teams are required and what they need to do to assist the change.

CHANGE TEST PLAN

Test plans are created by the Change Submitter. 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 Submitter 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 submitter will be contacted. Otherwise, the change will be allowed to move forward as scheduled.

STANDARD CHANGES
Standard changes are changes used in the current IT which is not required to conform to the change lead time standards.

A Standard Change:

1. Is well defined (CI is a Configuration Item that is part of the system or service) and impacted service(s) are uniquely identified). Documented (there is a procedure in the form of a checklist or step-by-step narrative on how to make the change and how to back-out of the change), tested (the change has been implemented successfully) and proven (the change procedure has been used before successfully) at least three times in production.

2. The risk is low (the risk of failure is low or the impact to services should the change fail is minimal) and well understood (the types of risk are known and the consequences of failure understood and can be mitigate within 15 minutes.

3. Is transparent to the user (users will not notice a difference in the way they interact with services or need to change local system or software settings or configuration.

4. Requires no additional funding to implement.

5. Is completed within a declared Change maintenance window for that system or application

Standard changes are submitted via the RFC to the Change Manager for review and approval by the CAB. Any changes not submitted as Planned changes, or not contained in the Standard list will be considered Unauthorized Changes.

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 RFC's, regardless of urgency, impact and type are subject to the Change Management policy. This includes any 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 RFC should have the following headings with supporting descriptions and/or documentation:
-Service / Equipment being changed

-Brief Description of the change (Include Service and what is being changed) this needs to be clear and concise and in basic terms

-Reason for the change

-Change Plan Details

Start Date/Time – End Date/Time

-Describe any service disruptions this change might cause

-Impact if not implemented

-Back out plan should the change be unsuccessful

-Worker notes

-Communication

-Display on Help Desk sites for (Select none, Hospital, Campus, both)

-This field is displayed on the support website. Please type in a user friendly description of the impact

-Peer Review (Did you have a peer review this change, which peer)

-Other team's assistance (Do you need the assistance from other teams, which teams, what do they need to do so you can make this change)

-Urgency (Low, Medium, and High) How urgent is it for this change to go into production?

-Impact (<25 users, 25-250, 251-1000) How many users could this affect?

Risk of Failure (Low, Medium, and High) what is the risk of failure for this change?

Category (Minor, Major, Urgent, Break Fix or Emergency, and Standard if selected from approved list of standard changes).

Change Types:

- Submitter to present to Cab
- Reviewed at CAB meeting

- Minor
  - Minor system or impact
  - 10 day lead time
  - Pre-approved
- Standard
  - Minor change (minor system or impact)
  - Next established Change Window (No 10 day lead time)
  - Transparent to users
  - Documented procedure
  - Requires no additional funding

- Testing and validation of success

3. The CAB meets regularly to review all RFC's and approve or reject them and schedule them appropriately. Change Submitters that have Major or Urgent RFCs are encouraged to attend this meeting in case there are any questions from the CAB.

4. The CAB/EC can be convened with short notice to assess an Emergency change.

5. A 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 from the change submitter 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 submitter must complete the RFC when the change is completed.

-Changing status to completed.

-Enter the completed Date/Time

-Enter the completed Status (Successful, Partial, or Failure)

-If the change is Partial or Failure, then the explanation needs to be emailed to the Change Manager.

10. The Change Manager will maintain the Change Calendar and make it available to the institution. Necessary notifications will be delivered via the Service Desk.

II. UNAUTHORIZED CHANGES

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

III. ENFORCEMENT

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. CAB will suggest sanctions for unauthorized changes to Change Management Board to decide. Possible Sanctions include:

- Manager to explain to CAB why this happened
- Manager to attend CAB for 30 days
- Use Above/Below the Bar for Un-Authorized Changes in ITSM Meeting
- Any "Urgent" team RFCs must be printed, manager must have hand signatures from approvers for 30-90 days
- Present to CAB all team RFCs for 30-90 days