IT@UC Information Technology at the University of Cincinnati

Change Management Process

Preface

Changes in and/or to a production environment are the largest single cause of service interruptions and unpredicted results. In order to be effective, the change management process must be inclusive of all events affecting the UC production environment and must be used consistently by all operational areas of IT@UC with the support of upper management. In addition to providing a common approach to implementing changes, it will aid in ensuring all staff that could potentially be impacted by a change will have advance knowledge and allow them the opportunity for proactive response rather than reacting to unforeseen circumstances. At the same time, it will enable changes to be scheduled more effectively thereby reducing the effect of multiple, and apparently unrelated, changes causing a disruption in service. This will reduce the effort of identifying and correcting problems caused by a given change to the environment and allow us to be more responsive to potential problems and provide greater availability of services to the University community.

The purpose of this document is to outline the processes that govern the Change Management Process in the University of Cincinnati's Information Technology department. This document describes how to use the procedures and provides a definition of the management controls required and some rationale for instituting those controls.

Table of Contents

Objectives/Purpose

Change Management is the process of planning, coordinating, implementing, and monitoring changes affecting any production platform within Information Technology's control. The purpose of Change Management is to ensure that potential changes to IT service components are reviewed in terms of their efficacy to meet business requirements, and that their impact is evaluated. The objectives of the Change Management process are to:

- Ensure that changes are made with minimum disruption to the services IT has committed to its users.
- Support the efficient and prompt handling of all changes.
- Provide accurate and timely information about all changes.
- Ensure all changes are consistent with business and technical plans and strategies.
- Ensure that a consistent approach is used for all groups who request changes.
- Provide additional functionality and performance enhancements to systems while maintaining an acceptable level of user services.
- Reduce the ratio of changes that need to be backed out of the system due to inadequate preparation.
- Minimize the total number of unplanned changes.
- Ensure that the required level of technical and management accountability is maintained for every change.
- Monitor the number, reason, type, and associated risk of the changes.

The Change Management procedure for IT@UC defines how the change process is implemented in all of the IT platform environments. The objectives of the operating procedures, in addition to those detailed above, are to:

- Provide documentation that allows IT@UC management to understand, at any point in time, the overall impact of the planned change.
- Minimize the bureaucratic impact on the development community while still maintaining control of the environment.

Activities of the Change Management Process at IT@UC include:

- Receiving change requests from the Request for Change process
- Determining rather or not the change is in the best interests of IT@UC.

- Determining the risk of the change
- Accepting or rejecting the requested change
- Scheduling the change
- Communicating change status as required to all interested parties
- Closing the change

Scope of Changes

Scope Inclusion

The addition, modification, or removal of items that could have a negative effect on production services. Examples:

- Hardware changes
    - New installations
    - Upgrades/Moves
- System software changes (operating level)
    - Approved Operating System updates
- Application changes
    - Functionality updates
    - Web page additions/deletions
    - New releases
- Network changes
    - New installations
    - Upgrades of equipment/software
    - Equipment replacement
- Database changes
    - New installations/Change
    - Decommissioning
    - Security Patches
- Software Changes
    - Version upgrades, enhancements, and patches
- Planned/scheduled outages

Change Management Standards

- All requested changes to IT@UC's environment must adhere to the IT@UC Change Management process. A substantive change has the potential to affect the ability of users and systems to interact with each other.
- All changes to the production systems within IT@UC must have a corresponding set of

documentation that describes the change, the business reason for the change, and the disposition of the change. This includes emergency changes. This set of documentation is in the form of a **Request for Change (RFC)**.

Roles and Responsibilities

Change Advisory Board (CAB)

The Change Advisory Board (CAB) is a team of people made up of IT management and subject matter experts, chaired by the Change Manager. This team is made up of resources from a broad range of IT departments so that they can also assess whether a change will have a potential down or upstream impact to systems within their departments. (example: a router change may impact a Web Server and would therefore be of a concern to the Web Server Administration team).

The Mission of the Change Advisory Board is to plan and monitor all changes introduced into the IT environment. Responsibilities include ensuring the following things are present for every change.

- The Change Request has been submitted with the required information.
- There is a business/technical reason for the change.
- A user has been identified who is responsible for the change.
- A viable Change Plan exists.
- A pre-test plan exists if test environment is available, if not a test plan after implementation is provided.
- A viable Back-out Plan exists.
- If applicable, verifies that the change has been tested prior to implementation.
- If applicable, verifies that a security scan has been performed.
- A technical impact assessment has been completed.
- If applicable, verifies that the security review has been completed.
- If applicable, verifies that the architecture has been reviewed.
- Verifies that the disaster recovery plans have been updated accordingly to address the change.
- A business impact assessment has been completed.
- A Communications Plan has been developed ensuring communication to the IT and user communities of the intended change and potential impact to them in case of failure of the implementation.
- Appropriate business/management approval has been obtained based on the risk assessment.
- A post-installation review of the completed change to ensure proper and successful implementation.

Change Manager

The Change Manager oversees the entire Change Management process and ensures that all guidelines

laid out in the process document are being followed for every change. The Change Manager's responsibilities for all changes include:

- Is responsible for and owns the Change Management service
- Has nominated a designee to cover Change Management in the event of absence
- Coordinates, sets, and finalizes service requirements, objectives, and targets for the Change Management service in conjunction with other IT@UC process owners
- Involved in development and subsequent agreement on process improvements related to the Change Management service
- Develops requirements for Change Management standards, procedures, measurement, tools, and technology in conjunction with other IT@UC process owners
- Owns, maintains, and ensures accuracy and timeliness of the Change Management Calendar
- Reviews change requests for procedural compliance, information quality, and completeness.
- Verifies that accurate priority and impact are assigned to change requests
- Coordinates and owns the change approval and rejection process which incorporates routing to reviewers, receiving reviewer responses, and relaying appropriate information to requesters. This also includes negotiation with both parties and final ruling
- Facilitates the weekly Change Management Meetings
- Notifying affected parties that changes are scheduled and ready for implementation
- Ensures post-change outcomes and required documentation is attached and complete.
- Schedules and attends all meetings concerning the Change Management process
- Complies with Change Management service standards, process, and procedures as required
- Provides a technical resource to project requests where Change Management service expertise is required
- Captures and reports appropriate Change Management service measurement data
- Attends appropriate problem escalation/resolution, project development, and service support reviews where Change Management service expertise is required
- Adds notification to the planned maintenance page for changes that will degrade or cause an outage to the current core systems and core applications.

Change Requester

The Change Requester initiates and completes the Change Management process and has overall responsibility for accepting changes. The Change Requester can be the same person as the change Implementer (see the Change Implementer section below) or may be the manager of the department requesting the change. Change Requester responsibilities for given changes include:

- Reviews change request with departmental manager for efficient approval

- Assesses the change for risk/impact and ensures the appropriate risk category has been applied
- Ensures that the change request contains accurate information at a sufficient level of detail to implement the change without intervention
- Ensures proper lead-time for changes is allowed (see the Lead Time for Changes section of this document)
- Ensures that a representative for the change is present at the weekly Change Management Meeting (see the Change Management Meeting section of this document)
- Communicate intention of change to all potentially affected parties
- When target date or time of implementation needs to be changed after approval, the change will be resubmitted.
- Responsible for obtaining appropriate resources for all change tasks requiring completion for change success
- Coordinates task documentation within a change request with other participating staff as appropriate
- Attends change assessment and review meetings as appropriate (i.e. post-mortem reviews for major interruptions in service caused by a change)
- Ensures all rejected changes are reevaluated for completeness and correctness prior to resubmission
- Updates change requests as required and requested
- Attaches the following documentation to Requests for Change
    - Backout Plan (required for all changes. If there isn't a detailed backout plan documented, note in the details of the change what you will do if the change should fail)
    - Test Plan (required for all changes. If you don't have a testing environment, note that and how you will verify that it works in the description of the change)
    - Attach affirmation that testing is complete (if the tester is not the requester, the requester will attach the affirmation to the change (this can be copy and pasted from chat or email, including the tester's name from chat or email header))
    - Any scans necessary for approval of the change
    - Any added documentation that will add detail to the description (lists etc. of what systems and applications will be affected)

Change Approver

The change approver may be an AVP, Director, Manager, or a designee that they have appointed. The Change Approver responsibilities include:

- Review the changes submitted by their technicians
- Approve/deny the changes via the Change Management application. Approvers should complete their approvals quickly to allow time for additional approvals such as OIS and Change Manager approvals.

Change Implementer

The Change Implementer has overall responsibility for understanding the requested change and carrying out the tasks associated with the RFC. They are responsible for creating, with other resources as required, the coding, system, procedure, and/or process modifications required to implement the change. With the change requester, they are responsible for representing the change to the Change Advisory Board, monitoring and/or testing the code prior to final promotion into production, and requesting change closure. Specific Change Implementer responsibilities include:

- Meeting with the Change Requester to understand the requested change and to complete the Change Request documentation as necessary
- With the Change Requester, presenting the change to the Change Advisory Board from a technology and IT architecture perspective for approval to proceed
- Developing backup and/or back-out plans
- Designing and creating the code, procedures, or process modifications required to ensure change success
- Designing and developing tests required to demonstrate the quality and usefulness of the change
- Monitoring the promotion (on site or remotely) of the change into production
- Resolving issues associated with promoting the change into production, when necessary
- With the Change Requester (as appropriate), participating in the review of the promotion of the change
- Requesting closure of successful changes or documents outcome of failed change

Change Types

The Change Management procedure applies to all changes that could potentially impact the IT@UC environment. Any upgrade, move, replacement, reconfiguration, modification, or removal of a system which has associated risk, may require an Information Security Review per the Information Security Design & Architecture Review Policy.

Changes typically fall under, but are not limited to, the following categories:

- **Configuration Changes**
    - Examples – Updates to the Access Control List, changes to routers, switches, firewalls, cabling infrastructure
- **Database Changes**
    - Examples – decommissioning an SQL database, rebooting database outside of pre-defined time frame
- **Environmental Changes**

- Examples – Installing a new UPS, facility maintenance which may cause downtime

- **Hardware Changes**
  - Examples – installing memory on a server, installing more storage on a server
- **Software Changes**
  - Examples – vulnerability updates to software packages, upgrades/updates to enterprise server operating systems

Change Management Risk & Security Level Assessment

Summary

Change Management Risk & Security Level Assessments are used to determine the levels of risk involved with changes. The technician that submits the Request for Change is responsible for determining the risk level of the change.

Final risk determination in the Change Management system is broken up into three categories:

Low Risk

These changes have little or no impact on the environment and reversing the change is relatively easy and straight-forward. Low risk changes rarely require more than minimal documentation and user notification is often unnecessary.

Moderate Risk

These changes can affect departments, user groups, or an entire site, but reversing the change is reasonably attainable. All affected users should be notified of these types of changes.

High Risk

These changes have the greatest degree of impact on departments, user groups, or may even affect the entire environment. Reversing these changes is a time-consuming and difficult endeavor. Upper management should be aware of the potential impact of these changes and all affected users should be notified in advance.

Risk Assessment

Assessing Risk Level for a Change involves calculating Dependencies, Impact, Priority, and the Users Affected by the Change. To more accurately determine the Risk involved with a Change, utilize the table listed below.

*Redundancy factors in the determination of risk. Redundancy means there is a full failover of services that provides no impact to end-users.

Change Risk Assessment Matrix

RLA Attributes	4	3	2	1	S
Dependencies	Irreversible - Change cannot be reversed or validation is based on usage	Complex implementation and/or validation – or – Requires extended change window – or Change exceeds 1.5 hours to implement	Moderate implementation and/or validation	Typical- Easily validated and reversed.	
Impact to System	Affects All Platforms/Servers – or affects all sites. University-wide impact or a major hardware (system or network) replacement requiring extended setup and implementation time to restore service	Platform or network – or - Affects multiple platforms, systems or business/departments. Affects multiple network nodes or buildings or requires a reboot following a software upgrade, configuration change or a physical change. (coordination with end-user group(s) required).	Affects single platform or server. Exclusive use of major component or major sub-system. One user or a small group of users will experience network outage **– or–** external users will be unable to access a single resource	by users during implementation No network outage or loss of functionality for any user is expected	
Urgency (to restore service)	Major System(s)	Critical Component(s)	Non-critical components	None	
Users Affected by Change	Entire Organization	One or More Colleges	Select departments, units and/or groups	Individual or Small Group	

Risk Level Total	Risk
13-16	High
9-12	Moderate
4-8	Low

Total:

Example:
Dependencies = 2, Impact to System = 3, Urgency = 1, Users Affected by Change = 2 Total = 8 = Low Risk

Security Assessment

Assessing the Security Risk Level for a Change involves calculating the Data Type, System/Service Type, Change Type, and the Users Affected by the Change. To accurately determine the Security Risk involved with a Change, utilize the table below.

Security Risk Level Assessment

SRLA Attributes	4	3	2	1	S
Data Type (uc.edu/infosec/policies)	* Restricted/ * * Export Controlled	Controlled	N/A	Public	
System/Service Type	Publicly accessible with **no** authentication	Publicly accessible with authentication	Only accessible via internal network	Only accessible via internal network by system or application administrator(s)	
Change Type	Major Modification to core components – includes patches and upgrades	Moderate modifications to core components	Modifications to core components including executable code; database changes affecting data (inserts, updates, deletes)	UI / cosmetic changes (CSS, HTML) modifications restricted to CSS and HTML changes. Database changes not affecting data (stored procedures, queries that export or produce data)	
Users Affected by Change	Entire Organization	One or More Colleges	Select departments,	Individual or Small Group	

* Applications that contain or access **Restricted Data** with **Change Types** that involve modifying code or moderate to major modifications to core components must have a **Data Type** risk level of **4** and be documented accordingly.

** If there is **Export Control Data**, contact the Office of Information Security (OIS).

Risk Level Total	Risk
13-16	High
9-12	Moderate
4-8	Low

Total: ☐

Example:
Data Type = 2, System/Service Type = 3, Change Type = 1, Users Affected by Change = 2 Total = 8 = Low Risk

Notifications and Vulnerability Scans

Application changes often require a vulnerability scan to be reviewed by Information Security to ensure the change will not have any adverse effects. The Risk Level Assessment and Security Level Assessment scores will determine when a scan is needed.

* Systems participating in scheduled vulnerability scans under the Vulnerable Systems Policy do not need to attach a separate scan.

** Emergency Changes must submit a passing scan within 10 business days of the change being made. If the change will take longer than the 10 business days, OIS must be notified. Refer to the Decision Matrix below for guidance as to when a scan must be provided.

Decision Matrix

Security Level Assessment					
High Risk System	Does not require CM approval	**Requires Approval & Scan**	**Requires Approval & Scan**	**Requires Approval & Scan**
Moderate Risk System	Does not require CM approval	Requires Approval / No Scan Required	**Requires Approval & Scan**	**Requires Approval & Scan**
Low Risk System	Does not require CM approval	Requires Approval / No Scan Required	Requires Approval / No Scan Required	**Requires Approval & Scan**
	Standard Change (requires Standard Change template)	Low Risk Change (> 48 Hours) (Risk Score 4-8)	Moderate Risk Change (> 4 Days) (Risk Score 9-12)	High Risk Change (> 7 Days) (Risk Score 13-16)

Risk Level Assessment

The y axis represents the Risk calculated for the Security Level Assessment. The x axis represents the Risk calculated for the Risk Level Assessment.

** Should the Risk or Security Assessment calculate to 2 different risk levels i.e. RLA = Low Risk and SRLA = Moderate Risk, then the assessed risk level should be the higher value.

Change Priorities

The following guidelines for definition of Change priorities are provided for consideration during the planning cycle. It must be clearly understood that these requirements are the minimum for each of the defined levels. The requester may wish to plan additional lead times, documentation, or reviews to ensure that targets can be met and planned implementation schedules can be achieved.

Scheduled Changes – Required Lead Times

To allow time for the changes to be presented in CAB meetings, all Lead Times exclude weekends, holidays, and days that the university is closed.

Lead Times for Scheduled changes based on Risk are as follows:

Low Risk: The lead time for implementation is 48 hours from submission (business days only in the 48-hour count) i.e., a Scheduled **Low Risk** change submitted on Friday at 4:00 pm must be scheduled for implementation no earlier than Tuesday 4:00 pm the following week. A Scheduled **Low Risk** change submission, i.e. Friday at 4:00 pm prior to Memorial Day Holiday earliest possible implementation no earlier than Wednesday 4:00 pm following the holiday.

Moderate Risk:

Minimum 4 days' lead-time prior to implementation. This excludes holidays, weekends and scheduled university closed days such as winter season days. The time (hours & minutes) of submission and implementation is not considered, only the day of submission and the day of implementation are considered, i.e. A Moderate Risk change submitted at 3:00 PM on a Thursday can be implemented anytime on the following Tuesday.

High Risk: Minimum 7 days' lead-time prior to implementation. Recommended 14-21 days' lead-time, depending on the impact and communications necessary. The Change Advisory Board will determine if there is enough lead-time and will push back the date to accommodate, if necessary. The lead time excludes holidays, weekends and scheduled university closed days such as winter season days. The time (hours & minutes) of submission and implementation is not considered, only the day of submission and the day of implementation are considered, i.e. A High Risk change submitted at 3:00 PM on a Monday can be implemented anytime on the Tuesday of the following week.

NOTE: Changes outside of lead time will be rejected and need to be rescheduled.

Scheduled Changes
Recommended Implementation Times

Change Management Scheduling Policy

**** While Changes may be implemented on weekends and holidays, the lead times do not include weekends, holidays, and days that the university is closed. ****

Weekly Maintenance Windows – Where possible, IT@UC will attempt to schedule Low Risk changes on Tuesdays & Thursdays after 6pm to 6AM the following morning and be fully completed by 7AM (can be done on weekends between 12:01AM on Saturday to 6AM Monday with enough lead time and fully completed by 7AM Monday)

Instructional System Window

- Should be Scheduled between 10Pm and 6AM any day. If not, requires a 3rd level approval (AVP) attached to the change prior to implementation, and it is required that the reason it is outside the window to be stated.
- Should be fully completed by 7AM

Scheduled Changes - Scheduled changes are any planned changes to UC's environment. To ensure that the appropriate level of planning is involved for each change, the required Lead Time based on risk must be followed

Scheduled Low Risk

- Should be implemented on Tuesdays or Thursdays after 6PM to 6AM the following morning (can be done on weekends between 12:01AM on Saturday to 6AM Monday with enough lead time and fully completed by 7AM Monday)
- If outside of the window stated above, it is required that the reason it is outside the window to be stated.
- Must be fully completed by 7AM
- Must have 48 hours lead time from submission to implementation time
- If it doesn't have 48 hours lead time, excluding weekends, holidays and days the university is closed – the change will be rejected, and technician will need to change the time to meet the required lead time.

Scheduled Moderate Risk

- Should be implemented outside of work hours (after 6PM to 6AM)
- Should be fully completed by 7AM
- If a Moderate Risk change is Scheduled during the workday (7AM – 6PM Monday – Friday) - Requires a 2nd level approval (Director) the change management application prior to implementation and it is required that the reason it is outside the window to be stated.
- If it doesn't have 4 business days lead time, excluding weekends, holidays and university closed days – the change will be rejected, and technician will need to change the time to meet the required lead time.

Scheduled High Risk

- Should be implemented on Holidays or Weekends
- If not on a Holiday or Weekend – Requires a 3rd level approval (AVP) prior to implementation and the reason it is outside the window must be stated.
- If it doesn't have 7 business days, excluding weekends, holidays and university closed days lead time – the change will be rejected, and technician will need to change the time to meet the required lead time.

Escalated Changes

- Must be initiated by customer, internal (leadership), or vendor
- Must state the reason the change could not wait the normal Scheduled lead time based on risk.
- 3rd level approval (AVP) must be attached to the change prior to implementation.

Emergency Changes

- (An emergency change is a response to a major incident that impacts a service in production (break/fix only) or a required security fix that needs to be implemented immediately. Emergency changes do not fall within the required scheduled risk lead times.)
- Must state the reason the change could not wait the normal Scheduled lead time based on risk.

Standard Changes

Standard Changes are proven, repeatable and verified to be low risk, with little to no impact to services.

Changes classified as Standard must follow defined criteria in the specific change model that has been vetted and approved by the Change Advisory Board (CAB) with final approval by the AVP. The approved models are selectable in the Standard Change Catalog when submitting a change.

Procedure to Request a new Standard Change:

1. Propose a Standard Change: to have a low risk change that is repeatable to be added to the Standard Change Template Catalog.
2. The Standard Change Template request is submitted to the CAB for approval.
3. CAB Recommendation: The technician will demonstrate the steps used to implement such a change during the CAB meeting. The CAB will make a recommendation to approve/deny the change.
4. Change Manager Recommendation: The Change Manager will take into consideration, the recommendation of the CAB and make a recommendation to the AVP of ESS for approval
5. If approved, the Standard Change name and date of creation are recorded in the approved template and will be listed in the Standard Change Catalog. (Any subsequent modifications dates will also be recorded after approval)
6. If a Standard Change is not in compliance with the template or results in an incident, the change will be reviewed and determined if it should have been a scheduled change and/or if the Standard Change is recommended to no longer be a Standard Change.
7. If the CAB or the technician implementing the change needs to add information to a particular Standard RFC, they can modify the standard change and resubmit it for approval. The standard change template will then be reviewed again by the CAB and sent for approval by the Change Manager and then the AVP.
8. When the Submitter saves the RFC, it will automatically send notifications out to the CAB and Approvers.
9. Standard Changes will be reviewed on a yearly basis.

Recurring Maintenance

Procedure to Request a new Recurring Maintenance Change:

1. Purpose of Recurring Maintenance Changes are to schedule a maintenance window for the change to be implemented recurring at the same day and time (daily, weekly, monthly etc.)
2. Submit for approval: Once the draft is ready to be sent to the CAB, the technician will email the drafted Recurring Maintenance Change for the approval process based on risk.
3. If approved, the Recurring Maintenance Change name and date of approval are recorded in the approved document and will be listed as a template in the Recurring Maintenance Change Catalog.
4. Submitters can now utilize Recurring Maintenance changes based on this template and will add their current changes to be implemented in the description and justification.

5. When the Submitter saves the RFC, it will automatically send notifications out to the Change Manager for review and approval.
6. Recurring Maintenance Changes will be reviewed on a yearly basis.

Escalated Changes

Escalated changes are changes that are not a break/fix and do not meet the required lead time to be a Scheduled change.

A typical example is an Escalated Change is one that is identified on Thursday and must be implemented the following day, Friday, prior to next CAB meeting.

UC Escalated Changes meet these criteria:

- AVP approval required prior to implementation
- Time Sensitive Mandate by Leadership, Institutional Mandate, 3rd party vendor, or Compliance Requirement
- They will be reviewed in the CAB (possibly after implementation)

Emergency Changes

Emergency changes are a break/fix where service must be restored as soon as possible. ***An emergency change is a response to an incident that impacts a service in production or a required security fix that needs to be implemented immediately.***

Emergency changes in break-fix situations may be implemented immediately without an RFC, as long as there is a minimum of verbal approval from a director or above. For every emergency, an RFC must be entered, documenting the justification and outcome of the change. These changes will be reviewed at the next CAB Meeting.

Blackout Dates

Blackout Dates will be implemented for start of the fall semester and winter season days. During blackout dates no scheduled low, moderate, or high risk changes can be implemented without an AVP approval prior to implementation.

While there will be no blackout dates during exam periods, technicians are asked to refrain from implementing changes that will have an impact on students during the exam periods.

Approval Requirements

All changes must go through an approval process in order to ensure that all necessary parties agree to the change.

Scheduled Changes

Instructional Systems

Instructional Systems – (lead time is based on Risk) Any changes to instructional systems should be scheduled (between 10pm and 6am) to avoid interfering with classes. For exceptions, AVP approval must be obtained and filed with the CM request and reason for exception must be stated.

Instructional Systems:
- Canvas
- Echo360
- Kaltura
- WebEx
- Zoom
- CoursEval
- Teams (probably other apps in O365 too - Word, Excel, PPT, Forms)
- Captioning (Cielo24 currently - moving to 3Play Media)
- Honorlock
- Student Portal
- LinkedIn Learning

Depending on the associated risk level, Scheduled changes require different levels of approval:

High Risk
- Change Advisory Board
- Documented Director (or above) authorization
- Change Manager (final approval)
- Information Security (OIS)

Moderate Risk
- Change Advisory Board
- Documented Director (or above) authorization
- Change Manager (final approval)
- Information Security (OIS)

Low Risk
- Documented Manager (or above) authorization
- Change Manager (final approval)
- Information Security (OIS)

Note: ***All Scheduled Changes require final approval before implementation.***

Emergency Changes

- Documented Director (or above) authorization
- Change Manager (final approval)
- Information Security (OIS)

Escalated Changes

- AVP authorization prior to implementation
- Change Manager (final approval)
- Information Security (OIS)

Note*:* Depending on the impact of any change, approval may be required by directors from multiple departments. This will be at the discretion of the Change Advisory Board.

Approval deadlines*:*

All changes must be approved by Directors, Managers or AVP's prior to next Scheduled CAB meeting.

Updating the Implementation Date and time:

Technicians can only update the implementation date and time up until approval has occurred. Once approval has been granted, technicians will have to submit a new change to go thru the approval process.

Documentation

Documentation requirements for changes are as follows:

Contacts

- The name and contact information of the person creating the RFC (Change Requester)
- The name and contact information of the person who will ultimately deploy the change (Change Implementer)
- The name of Change Requester's manager (if different from the Change Requester)
- The name of the Change Requester's director (if different from the Change Requester)
- The name of the person who will test the change (if different from the Change Implementer)

Description

- What specifically is the change? (what specific edits or updates are you doing? If this is a version change, note what version it was and what version the update is)
- Who (how many are affected, what areas or how many users)?
- What is the worst-case scenario of impact to end users?
- What systems/applications are affected? (what is the IP address, URL and/or Hostname)
- List the systems/applications/services impacted as well as Details about whether those systems/applications/services impacted are hosted locally or in the cloud. If the information

regarding items that will be impacted from a network change is too broad, then provide subnets that will be affected. (you can attach a document if necessary)
- Has there been a notification to those affected?

All changes are tracked, correlated, and used for management reporting, statistics, trending, etc. to identify areas for service and Change Management Process improvement.

Change Management Meetings

The Change Advisory Board members or their designees, Change Manager, and a designee for each change will participate in a Change Management Meeting (CAB), which will be facilitated by the Change Manager. These meetings are Scheduled twice per week. The specific agenda for the meeting is as follows:

Change Management Meeting Agenda

- New Scheduled Changes (Moderate/High Risk)
    - Each request formally entered into the Change Management Meeting by the Change Manager will be reviewed and discussed one at a time, and any questions or conflicts will be handled by the designee for the change.
    - If there are no conflicts, the change will be approved.
    - Those with conflicts will either be rescheduled or denied.
- Emergency Changes
    - All implemented and upcoming Emergency changes will be reviewed.
- Escalated Changes
    - All implemented and upcoming Escalated changes will be reviewed.
- Problems encountered during the previous week
    - Any major incidents will be presented by the Service Desk manager.

- CAB members or their designees will approve each change included on the workbench, as it is reviewed during the CAB meeting.

The CAB's Role in the Change Management Meeting

As explained in the Roles section of this document, the Change Advisory Board (CAB) is the group that advises the Change Manager in:

- Assessment of changes
- Prioritization of changes
- Scheduling of changes

CAB Meeting Attendees:

- Representatives from areas that have submitted changes for approval. (required)

  They are expected to know of any changes being reviewed for their department and may be required to answer any questions.
- CAB members
- Change Manager

How the CAB Approves or Rejects Scheduled Changes

When a Scheduled change is reviewed, after all questions are answered, the Change Manager raises a vote for approval. The Change Manager, CAB members or their designees approve/deny the changes presented.

- For a Scheduled Change Request to be approved, it must be unanimously approved by the CAB.
- For a Scheduled Change Request to be rejected, any present member of the CAB has the right of veto to postpone a change until unanimous approval can be reached

Statuses

The following status codes are used to reflect the status of a change request:

- **Requested** – The RFC has been submitted into the Change Management system.
- **Pending** – The RFC is in review by the Change Requester's manager.
- **CM Review** – The RFC has been approved by the Change Requester's manager and is now in preliminary review and assessment by the Change Manager.
- **CAB Review** (Scheduled requests only) – The requested has been given preliminary approval by the Change Manager and has been entered into the agenda for the next Change Management Meeting for approval or rejection.
- **Director Approval** (Emergency requests only) – The request has been approved by the manager, business user (if necessary), and Change Manager and is now awaiting Director approval.
- **Approved** – The change has been approved by the appropriate approvers.
- **Rejected** – The change has been rejected. The Change Manager will contact the Change Requester with a suggested course of action.
- **Closed** – The change has been completed (either with success or failure), and the results of the change have been fully documented.

Pre-Planning

Not every change will be successful. This is unavoidable, so it is necessary to ensure that any RFC entered has a detailed back-out plan. The goal of any back-out plan is to return the system(s) back to the state they were in before the change occurred. Where there is a testing environment, a Pre-Test plan must be documented. If there is no testing environment, the testing will occur in production after implementation and this post implementation test plan must be documented.

Pre-Planning Requirements

- Documented Pre-test plan (if testing environment is available)
- Documented Post implementation test plan (if no testing environment is available)
- Pre-Testing Affirmation
- Documented Backout Plan

Backing Out of a Change

In the event that a change needs to be backed out, it is expected that the documented back-out plan will be followed. Once the back-out is complete, the person(s) who performed the change are expected to perform tests to ensure that the original state is fully recovered.

Outcomes

After a change has been deployed, it is the duty of the Change Requester to coordinate with the Change Implementer to document the outcome of the installation. There are a number of outcomes that can be entered after implementation, and they are as follows:

Successful Changes

Successful

When a change was successfully implemented without any problems, and all post-implementation testing was successful, the outcome will be entered as Successful Change.

Unsuccessful Changes

There are varying degrees of Unsuccessful changes. The following guidelines will be used to determine if a change has been unsuccessful or caused an outage to service.

- Expected results did not occur.
- Change caused an impact to the user or Operations.
- Change must be backed out.
- Incomplete instructions or inaccurate documentation provided to Operations.
- Change could not be installed in requested time period.
- Problem opened as a direct result of the change.

Canceled

A change that was entered and canceled *prior to implementation* will be closed as Canceled. For these, the Change Requester must enter into the Change Request the reason(s) why the change was canceled

.

Reports/Metrics

A number of reports on all change activity are available from the Change Manager. These reports are available to anyone who has a need for the information. These measurements include:

- Number of changes by service or application
- Number of approved, denied or canceled changes
- Number of changes by risk level and by group
- Number of changes by outcome and group
- Number/ratio of changes by priority

If more specific reports are required, please contact the Change Manager.