S&T IT Change Management
Policy and Procedure

5/1/2016

Executive Summary – S&T IT Change Management

All IT & Ed Tech staff are responsible to follow the Change Management Process when introducing changes into the IT environment of Missouri University of Science & Technology.

The CIO is responsible for enforcing the change management policy as well as updating the policy and process.

Change management is a process meant to ensure that any changes to existing, or introduction of new, software or hardware within the Missouri University of Science and Technology's (S&T) Information Technology (IT) production environment is done is an orderly and controlled manner. Ensuring effective change management within the S&T IT production environment is extremely important in ensuring the efficient delivery of IT services while reducing risk.

Objective

This document provides policy and procedures for S&T IT change management. The details in this document are intended to meet the foundation requirements for industry best practices as detailed within the Information Technology Infrastructure Library (ITIL) directly relating to IT change management. It is important to note that not all of the ITIL best practices for IT change management are included in this document. These operations also are intended to satisfy the Control Objectives for Information and Related Technologies (COBIT□) elements related to IT change management. In addition to meeting all of the ITIL and COBIT requirements, these guidelines provide for the efficient and effective handling of S&T IT changes completed by the IT organization.

IT Change Management (in general)

All IT & Ed Tech staff are responsible to follow the Change Management Process when introducing changes into the IT environment of Missouri University of Science & Technology.

The CIO is responsible for enforcing the change management policy as well as updating the policy and process.

S&T IT Change Management (CM) is the process of requesting, analyzing, approving, developing, implementing, and reviewing a planned or unplanned change within the IT infrastructure. The Change Management Process begins with the creation of a Change Request within the S&T IT's technology platform and ends with the most appropriate implementation of the change and the communication of the result of that change to all interested parties. The change management (CM) process is used to control, document, determine risk and impact of changes and communicate information about changes made to production services. S&T IT utilizes an online web application to document and track changes as they proceed through the S&T IT CM process. All changes to production systems and applications are required to be entered into the application. The application can be accessed at https://itweb.mst.edu/auth-cgi-bin/cgiwrap/cmweb/main.pl.

All change requests are reviewed during the weekly CM meetings. The normal process for a change request is to be reviewed at least 1 week prior to being implemented in production. Any CM request with less than 1 week of lead time to review is considered an emergency change and requires management approval and a post review audit. All areas of IT and select other campus groups are encouraged to attend the CM meeting each week as this is the forum to debate what changes are being proposed and approved. Any change owner with requests scheduled for review is required to attend or send a proxy, otherwise the request is denied.

CM steps *(All of the following are described "in detail: within the sections that follow)*

1. Initiating a change request
2. Analysis, Initial Approval and Planned
3. Completing the CM entry. The following fields are required to enter a CM entry request:
    - Status
    - Owner
    - Participants
    - Summary
    - Impacted Services
    - Change length
    - Outage Length
    - Risk level
    - Impact level
    - Review date
    - Change date
    - Change Time
    - Purpose
    - Procedure
    - Risk Analysis
    - Communication Type
    - User Impact
4. Risk Levels and Analysis assessments
5. User Impact Levels and Analysis assessments
6. Change Date and Lead time determinations
7. Developing the Backout Plan
8. Testing
9. Peer, Code and Security Reviews and Approvals
10. Change Scheduling - Reviewing the request during the weekly change management meeting.
    - Post reviews (Audits) of any emergency request or other requests are reviewed.
    - New requests scheduled for review are presented by the owner and reviewed for approval or denial
        - If approved update the status of the request to scheduled.
        - If declined update the status of the request to declined.
    - Previously reviewed requests scheduled for implementation at the next window are listed
    - Other CM items not yet entered into the system are discussed
11. Implementation and Promotion - Change is implemented during scheduled CM window.
12. Testing, Validation and Acceptance - Update the status of the request to completed.
13. Post review is done if necessary.

In Scope

The intended scope of S&T IT's Change Management is to cover all of the S&T's computing systems and platforms. The primary IT functional and operational components include:

- **Hardware** – Installation, modification, removal or relocation of computing equipment.
- **Software –** Installation, patching, upgrade or removal of software products including operating systems, access methods, commercial off-the-shelf (COTS) packages, internally developed packages and utilities.
- **Database –** Changes to databases or files such as additions, reorganizations and major maintenance.
- **SDLC/Application –** Software development life cycle and application changes to be promoted to production as well as the integration of new application systems and the removal and decommission of obsolete elements.

- Moves, Adds, Changes and Deletes – Changes to system configuration.
- **Schedule Changes** - Requests for creation, deletion, or revision to job schedules, back-up schedules or other regularly scheduled jobs managed by the S&T's IT organization.
- **VOIP** – Installation, modification, de-installation, or relocation of PBX equipment and services.
- **Desktop** – Any modification or relocation of desktop equipment and services.
- **Generic and Miscellaneous Changes** – Any changes that are required to complete tasks associated with normal job requirements.

Out of Scope

There are many IT services and tasks performed at S&T, either by the IT department or by the end users that do not fall under the policies and procedures of Change Management. Services and tasks that require an operational process, but are outside the initial scope of the S&T's Change Management process include:

- Contingency/Continuity/Disaster Recovery
- Changes to non-production elements or resources
- Changes made within the daily administrative process. Examples of daily administrative tasks are:
  - Password resets
  - User adds/deletes
  - User modifications
  - Adding, deleting or revising security groups
  - Rebooting machines when there is no change to the configuration of the system
  - File permission changes

The S&T IT Directors/Management may modify the scope periodically to include items in the scope of S&T IT's overall Change Management process.

Change Management (in detail)

This section describes the basic tasks associated with Change Management for S&T IT in more detail.

Initiating a Change Request

It is critical that the Change Management Process is consistent in quality and completeness and discards irrelevant requests. Change requests can be submitted by anyone within an S&T business unit via the self-service Help Desk Ticket System (help.mst.edu) or by contacting the IT Help Desk (http://it.mst.edu/help-desk/), upon review of the created ticket at IT's tier 1 support level for completeness, the ticket will typically be assigned to a tier 2/3 level IT resource group (Network, Systems, PIMS/Applications, Desktop, Ed Tech, IT RSS). Requesters can make changes to the request or check the status via the self-service Help Desk Ticket System (help.mst.edu), by contacting the IT Help Desk (http://it.mst.edu/help-desk/) or directly contacting the assigned IT resource. Requestors will likewise be contacted if additional information is required.

Analysis, Initial Approval and Planned

The assigned tier 2/3 level IT resource group collects additional information to define the change parameters, identify coding and/or technical requirements as well as establishes the initial priority and approval from management. At this point a new Change Management entry is made within the S&T IT Change Management (CM) system (https://itweb.mst.edu/auth-cgi-bin/cgiwrap/cmweb/main.pl?) with a status of planned if the request is to be routine and/or scheduled maintenance.

- Routine and scheduled maintenance prioritized changes occur within the S&T IT's

scheduled maintenance windows (http://it.mst.edu/help-desk/campus-maintenance-windows/) based on the IT resource group it is assigned.

Emergency prioritized requests occur as needed (with emphasis on implementing/promoting the change within a scheduled maintenance window if possible) to prevent any catastrophic events that are likely to occur and/or to recover services from such an event and may result in interruptions of campus computing services lasting several hours or longer. These are changes that, if not implemented immediately, will leave the organization open to significant risk (for example, applying a security patch) or a change that is important for the S&T and must be implemented soon to prevent a significant negative impact to S&T's ability to conduct business. IT communications will be as needed based on the emergency.

- Emergency change requests require 2 Director's to approval, all CM requirements to be completed after implemented, is identified in the CM system as an Audit and a review of why it was an emergency is reviewed after implementation for avoidance of reoccurring. As an example, the PIMS emergency promotion process is detailed below…
    - Developer notifies director of PIMS that an issue has been discovered in an application and that an urgent fix needs to be put into place. The developer will give an approximate amount of effort needed to fix the issue to the PIMS director.
    - Developer makes necessary changes in development and tests the changes themselves to see if they solve the issue.
    - The developer requests a PIMS promotion manager to promote the account to test (all appropriate servers) and let them know that an emergency promotion will most likely be occurring on this account soon.
    - Developer contacts customer to have them verify the change fixes the issue.
    - Developer ensures that only the changes that need to be committed to fix the issue are committed to the repository and a code review is submitted with those changes.
    - While the developer is completing steps 2 – 4, the PIMS director needs to get written (email is acceptable) approval from at least one other IT director to approve the emergency promotion of the application.
    - Once the PIMS director has gotten approval from a second IT director, that approval needs to be forwarded to PIMS promotion managers so they have record of the approval and know it is OK to proceed with it.
    - Once the code review and any associated audits on the account is closed, the developer notifies the PIMS promotion managers that the CR is closed and that the emergency promotion can be completed.
    - PIMS promotion manager promotes account to all appropriate servers in production and then notifies the developer and PIMS director that the emergency promotion is complete.
    - An entry needs to be placed in Change Management as an Audit to be reviewed at the next meeting.

NOTE: Emergency changes are to be kept to an absolute minimum due to the increased risk involved in implementing them.

Completing the CM entry

For all changes, the assigned tier 2/3 level IT resource must complete the S&T IT CM entry. The following are the fields for completing a CM entry (mandatory fields with * must be filled in before the CM entry can be updated from Planned status):

- Status*: *Planned/ Audit/ Review/ Scheduled/ Declined/ Delete*
- Owner*: *List single userid responsible for the change (typically this is the person assigned to the change and creating the CM entry)*

- Participants*: *List all userids involved in change (ie security, database, server, applications)*
- Ticket: *Related ITSM ticket number*
- Application User: *IT app userid*
- Summary*: *high level description of the change*
- Impacted Services*: *See the following section "Risk Levels and Analysis"*
- Change Length*: *See the following section "User Impact Levels and Analysis"*
- Outage Length*: *See the following section "User Impact Levels and Analysis"*
- Risk Level*: *(Low/Medium/High) and see the following section "Risk Levels and Analysis"*
- Impact Level*: (Low/Medium/High) and see the *following section "User Impact Levels and Analysis"*
- Review Date*: *See the following section "Change Date and Lead Time"*
- Change Date*: *See the following section "Change Date and Lead Time"*
- Change Time*: *select the appropriate scheduled maintenance window (http://it.mst.edu/help-desk/campus-maintenance-windows/)*
- Purpose*: *Define the requirements and description of the change. Estimate the IT, business and other resources required to implement the Change, covering the likely costs, the number and availability of people required, the elapsed time, and any new infrastructure elements or additional ongoing resources required based on the change.*
- Procedure*: *Instructions and back out for the implementation and promotion (See the following section "Developing the Backout Plan"*
- Risk Analysis: *See the following section "Risk Levels and Analysis"*
- Communication Type: *select from "Change Owner Handling Communications" or "IT Comms Assistance Required"*
- User Impact*: *See the following section "User Impact Levels and Analysis"*

Risk Levels and Analysis

This section describes the criteria to consider when evaluating the risk and impact of a change. This process is intended to evaluate and validate the technical feasibility, risk and effect a change will have on the production environment and end user productivity. Consider the following risk criteria while reviewing any change:

- Evaluate the change to gauge the risk, impact and effect of the change during and immediately following the change implementation.
- Review the completeness of the change, including anticipated assets changed, impact on start-up or shut down of systems, impact on disaster recovery plans, back-up requirements, storage requirements, and operating system requirements.
- Evaluate the technical feasibility of the change and the whole impact of the change in terms of:
  - Performance
  - Capacity
  - Security
  - Operability
- Validate technical aspects, feasibility, and plan.

After the above risk assessment is complete, the reviewer must assign a Risk level to the change in the CM entry based on the below.

- Low – For routine categories, the risk default is low. If the evaluation of the risk corresponds with the criteria below, the risk will be designated as "low." The risk criteria include:
  - Involves IT resources from one workgroup within same IT division
  - Low complexity – no technical coordination required
  - Low risk to system availability (system/service outage affecting clients during

Non-Prime Time)
  - Easy implementation and back-out
  - No impacts to service level agreements
  - The change is well understood and has been tested
  - Backout is defined and tested
- Medium – The components of a medium risk include:
  - Involves IT resources from more than one workgroup within same IT division
  - Significant complexity – technical coordination required from one or more functional groups
  - Moderate risk to system availability (system/service outage exposure during Prime/Peak Times, outage primarily expected during Non-Prime Time)
  - Some complexity to implementation and back-out plans, back-out not expected to extend the window timeframe
  - Affects application, data or server security
  - Impacts service level agreements (e.g. Business Non-Prime Time) and internal support required
  - The change is less understood
  - Has been partially tested including backout or cannot be tested but backout is well defined
- High – A risk is considered to be classified as high if the following criteria apply to the change:
  - Involves IT resources from more than two workgroups, crosses IT divisions
  - High complexity – complex technical coordination required with one or more functional groups
  - High risk to system availability (system/service outage expected during Prime/Peak Times)
  - Complex implementation and back-out plans, back-out likely to extend the window timeframe
  - Affects security of data on infrastructure
  - Impacts service level agreements (e.g. Business Prime/Peak Time)
  - Outside vendor support is typically required
  - The change is not understood
  - Backout is difficult or does not exist

User Impact Levels and Analysis

This section details the potential user impacts associated with a change, and the criteria necessary to assign a user impact level to a change. This user impact analysis is completed when a new change record is created. The user impact process evaluates the impact of the change as it relates to the ability of S&T to conduct business. The key objective is to confirm that the change is consistent with S&T's business objectives. The following points should be considered while performing this user impact assessment:

- Evaluate business risk/impact of both doing and not doing the change
- Analyze timing of the change to resolve any conflicts and minimize impact
- Ensure all affected parties are aware of the change and understand its impact
- Determine if the implementation of the change conflicts with the business cycle
- Ensure current business requirements and objectives are met.

User impact levels are established based on the answers to the following questions:

Customer and/or Client Impact

- High (4) – Impacts several internal and/or external customers, major disruption to critical systems or impact to mission critical services.
- Medium (3) – Impacts several internal customers, significant disruption to critical systems or mission critical services.
- Low (2) – Impacts a minimal number of internal customers, minimal impact to a portion of a business unit or non- critical service.
- No Risk (1) – No impact to internal customers, as well as no impact to critical systems or services.

IT Resource Impact

- High (4) – Involves IT resources from more than two workgroups and crosses IT divisions or involves expertise not currently staffed.
- Medium (3) – Involves IT resources from more than two workgroups within the same IT division or involves expertise that has limited staffing.
- Low (2) – Involves IT resources from one workgroup within same IT division.
- No Risk (1) – Involves a single IT resource from a workgroup.

Implementation Complexity

- High (4) – High complexity requiring technical and business coordination.
- Medium (3) – Significant complexity requiring technical coordination only.
- Low (2) – Low complexity requiring no technical coordination.
- No Risk (1) – Maintenance type of change

Duration of Change

- High (4) – Change outage greater than 1 hour and affecting clients during Prime/Peak times. Lengthy install and back-out.
- Medium (3) – Change outage less than 1 hour during Prime/Peak times or greater then 1 hour during Non-Prime times.
- Low (2) – Change outage less than 1 hour during Non-Prime times and affecting clients during Non-Prime times.
- No Risk (1) – No outage expected.

Security

- High (4) – Affects critical data or server security and the back-out would likely extend the window timeframe.
- Medium (3) – Affects non-critical data or server security and has a moderate back-out plan which would not extend window timeframe.
- Low (2) – No security issues and easy back-out plan.
- No Risk (1) – No back-out plan needed.

Service Level Agreement Impact

- High (4) – Impacts SLA during business Prime/Peak times.
- Moderate (3) – Impacts SLA during business Non-Prime times.
- Low (2) – Little measurable affect on SLA times.
- No Risk (1) – No affect on SLA times.

RANGE	User Impact Level
24 – 19	High
18 – 11	Medium
12 – 1	Low

Change Date and Lead times

It is essential that requests for change are submitted and approved in a timely manner. This will allow completion of accurate documentation, change processing and obtaining the approvals in sufficient time prior to the requested implementation date, and also provide for conflict resolution for scheduling of changes.

Lead times are the number of days an action (Initiation or Approval) must be completed prior to the requested change date. The number of days may vary depending on the priority and the

risk level. The Risk Worksheet which is required to be completed for each change will assist Change Initiators to determine risk potential. Preferably, high risk and/or large change requests should have several weeks (or even months) notice prior to the requested implementation date. Lead Times for each change will vary depending on the type of change. Change Initiators should plan lead times to allow sufficient time for planning, review, and approval. In some cases, lead times would also need to be planned to allow for standard implementation times that have been set for certain processes like the SDLC Approval process.

Developing the Backout Plan

Development of the back-out plan is essential to ensuring effective recovery in the event of a failed change. The back-out plan is primarily based on the risk and user impact levels and analysis and the implementation and promotion procedures and plan.

Testing

All changes will undergo some level of testing depending on the complexity of the change. Once the change is built, configured and integrated in the development environment, the change is moved to the Test/QA environment. This phase focuses on conducting testing and quality assurance to ensure reliability and performance of all components of the organization's technology infrastructure. The assigned tier 2/3 level IT resource will oversee testing and whether or not to advance the change to the next step.

Peer, code and Security Reviews and Approvals

Peer, code and security reviews are the last step of the Change Development Phase. Peer, code and security reviews are required for all codes changes and optional but recommended for all other S&T IT changes. All peer, code and security reviews and approvals are conducted, documented and completed using S&T IT's collaborative peer code review system (Crucible) from Atlassian (https://www.atlassian.com/software/crucible/overview). The purpose of peer, code and security reviews of code are to improve developer skills, cross knowledge of code and consequently the quality and security of the code. In general the review goes as follows:

- Developer checks code into subversion
- Developer submits a code review (from https://crucible.mst.edu/auth-cgi-bin/cgiwrap/crstatus/main.pl)
- Reviewers are automatically assigned to the review by netgroup which sends an email notification
- Peer review allows comments about code and mapping of defects to standards
- IT Security checks reviews for completeness (two reviewers complete and developer has responded as relevant to comments)

There are two types of closures of the review:

1. good to go: this is used when no further development work is indicated
2. needs audit: this is used when further development work is indicated

There are in general four types of addressable comments that can be produced by a code review:

1. Defects are when the code does not meet the requirements of an approved coding standard
2. Security issues that do not have a matching coding standard
3. Other issues that are not coding standard or security related (for example, group conventions, code does not work as expected, typographical errors)
4. Requests for clarification as to purpose or intent of code

- Identified defects must be addressed in accordance with the approved coding standard.
- Security issues are to be addressed based on the risk and impact of the issue, but generally fall into "fix before promotion" or "fix before next promotion".

- Other issues are addressed as appropriate. For example, the apps team may have requirements levied on their applications that the system team does not use.
- Requests for clarification are addressed by providing the clarification, which may lead to further comments.

In general, the IT Security oversight of the process is ensuring that two reviewers have completed and that raised issues are addressed.

Audit Reviews

The purpose of an "audit" review is to facilitate the processing of changes made pursuant to a previous peer review. By limiting the scope to only previously identified and approved changes, the full peer review is not required.

General Flow (Audit)

- Developer makes changes indicated from peer review
- Developer submits a code review, noting previous review and specifying "audit of CR-####"
- IT Security checks current and previous review to validate that all and only the indicated changes have been made
- On successful completion the review is closed with "good to go"
- If IT Security is the developer then any "audit" requires at least one other reviewer to certify that that changes match.

Change Scheduling

After all previous step are completed, the status within the S&T IT CM system can be changed to reviewed and brought before the weekly CM meeting (every Wednesday 2-2:30) to be approved for the status to be changed to scheduled.

Implementation and Promotion

Once a change is scheduled in the S&T IT CM system, it moves into the Implementation and Promotion Phase. During this step a designated S&T IT Promotion Managers reviews all comments, recommendations, approvals and the procedure for the implementation and promotion of the change to ensure all required tasks have been completed and may contact the assigned IT resource for the change if needed. The Promotion Manager implements the change in accordance with the CM procedures during the scheduled time. Failure of the implementation at this level will normally require the Change Implementer to follow the back-out plan to ensure normal system operations.

Testing, Validation, and Acceptance

Once a change has been implemented, the S&T assigned IT resource for the change and the requestor will test and accept/reject the change. Following a successful change implementation, a change review must be conducted to determine if the change resulted in the desired outcome. In most cases, this review process might be very brief. For a routine change, where the effect has been small and the results relatively predictable, the review process will be limited to checking that the change has provided the user with the desired functionality. After this is conducted the S&T IT CM entry status is changed to completed and any comments gathered are captured as "Post Comments" within the system.

Reporting and Documentation of Changes

Reporting and documentation of changes are within S&T IT are all in the Change Management (CM) system (https://itweb.mst.edu/auth-cgi-bin/cgiwrap/cmweb/main.pl?).