Contents

Scope

The Change Management policy covers all services provided by participating HSC IT organizations. The primary functional components covered in the Change Management process are documented in *Appendix A*, *Scope*.

Out of Scope

There are many IT tasks performed at UNM HSC, either by the IT department or by the end users, which do not fall under the policies and procedures of Change Management. Tasks which require an operational process but which are outside the scope of the Change Management policy are also documented in *Appendix A*, *Scope.*

Key Definitions

Change – The addition, modification or removal of an IT service or service component and its associated documentation.

Change Model – The step-by-step process to be followed to record, review and implement a change. A Change Model can be used for any type of change.

Change Record – The record within Help.HSC that contains all of the information relative to a change. This information includes justification, risk and impact analysis, communication, approvals, phases, and tasks associated with accomplishing the change.

Change Schedule (CS) - The CS shows when all changes are to take place within the entire IT infrastructure. This at-a-glance change schedule makes it possible to see available change windows and possible conflicts.

Configuration Item (CI) - An IT component that is significant enough to be under Configuration Management control. Each CI can be composed of other CIs. CIs may vary widely in complexity, size, and type from an entire system (including all hardware and documentation) to a single software module or a minor hardware component.

Request for Change (RFC) - This is the formal change request, including a description of the change, components affected, business need, cost estimates, risk assessment, resource requirements, and approval status.

Roles and Responsibilities

Roles associated with the Change Management process are defined in the context of the management function and are not intended to correspond with organizational job titles.

Role	Responsibilities
Change Initiator	Business or IT representative who initiates a request for change. This person is responsible for filling out the Request for Change (RFC) form ensuring that all required information is included, submitting it according to this procedure, and notifying change manager.
Change Process Owner	Senior manager who provides management control and guidance for the process in the IT department. Accountable for process design, operation, and improvement. Approves process rollout and changes to the process. Coordinates with Change Process Owners in other IT departments to ensure common practices where appropriate.
Change Manager	This person has overall operational responsibility for the change management process in the IT department or designated sub-department. Accountable for vetting that the change request is accurate and complete and includes enough information for the CAB to approve or reject the proposal. May make the determination regarding categorization and classification of the request. Publishes metrics and the Change Schedule.
Change Advisory Board (CAB)	The CAB is a cross-functional team responsible for assessing change requests in terms of business need, cost/benefit, viability, and potential impacts to existing systems or processes. The CAB instructs the Change Manager to approve, defer, return, reject or cancel changes. Also, the CAB makes recommendations related to change implementation. Each organization will define their CAB or CABs depending on their own change management process. After changes are complete, the CAB reviews them for success/failure and lessons learned. See *Appendix B – CAB Logistics* for recommendations regarding membership and agenda.

Emergency Change Advisory Board (ECAB)	This team (or individual) is a subset of the CAB that is responsible for dealing with Emergency changes. The ECAB must be able to respond on very short notice and authorize or reject Emergency changes.
Technical Review Board (TRB)	An ad-hoc group of subject manner experts (SME), and technical experts who are convened by a CAB to do an in-depth technical review of a change.
Service Owner	Represents one or more services in IT leadership and CAB meetings. Understand customer service requirements. Authorizes changes to the service.
Component Manager	Represents one or more service components in the CAB. Understands the technical structure of the component and sub-components, and how they support the service.
Stakeholder	Any individual with an interest in types of changes or in a particular change.

Metrics and Reporting

The Change Manager will work with the Change Process Owner to establish appropriate metrics to monitor the success and continual improvement of the change management process. Reports containing the above metrics will be generated by the Change Manager and published to CAB member dashboards prior to the meeting.

Activities, tasks, workflows, and work instructions

Each organization will develop their detail procedures to include processes for how each change type is entered, reviewed, approved, and completed. These detail procedures should give clear guidance to all parties involved in the change process regarding their work instructions and tasks.

These detail procedures are found in *Appendix C – Detail Procedures*.

Communications

The change initiator is responsible for communicating the change to the proper audiences. Once the initiator is notified of the change approval, they should initiate necessary communications about the change prior to the change being made. Appendix E contains guidelines for when change notifications should be sent and to whom they should be sent.

Approved changes that have a board impact, such as the entire HSC, may require additional communications such as notification in the HSC or Hospital daily communication e-mail, signage, or

other communication methods. On these changes, the change initiator should work with their management to ensure the necessary notifications are being completed.

Classification and Categorization of Changes

Following ITIL guidelines, there are three different types of service change:

- Normal Change – Any service change that is not a standard change or an emergency change.
- Emergency Change – A change that must be implemented as soon as possible, for example to resolve a major incident or implement a security patch
- Standard Change – A pre-authorized change that is low risk, relatively common and follows a procedure or work instruction.

In addition to the change types, changes can be categorized as major, significant or minor, depending on the level of cost and risk involved, and on the scope and relationship to other changes. The detail procedures for each group should address this categorization.

Normal Changes

A Normal Change is one which will affect services in the production environment, either by:

- Causing a service outage; or
- Running a significant risk of causing an outage; or
- Creating a significant change in the end user experience,

regardless of whether the change is made during a normal maintenance window or not. All Normal Changes must be approved by the appropriate CAB, and communicated to the appropriate stakeholders prior to implementation.

The appropriate Change Manager or CAB may decide that the scope or risk of a particular change requires senior leadership approval, and escalate it to the appropriate leadership group.

Normal Changes Categories: Expedited Changes

An Expedited Change is a Normal Change that must be expedited for approval more quickly than the normal CAB process allows, due to critical business requirements or risk.

Expedited Changes must be approved by the appropriate Change Advisory Board (CAB).

The CAB will review and approve the Expedited Change via email or other collaborative tools.

The Change Manager will ensure that all RFCs processed by the CAB are properly documented in Help.HSC as soon as possible.

Emergency Changes (approved after the fact)

A change that must be made before a CAB can be convened to review and approve it due to a repair or error in an IT service that is causing a negative impact. Incident resolution may sometimes require Emergency Changes. Examples include a critical service-down that requires a quick hardware swap-out, or a late-night system emergency when the Change Manager or others may not be available.

An Emergency Change must follow these steps:

- If time allows, the Change Initiator must make a good-faith effort to contact their manager or the appropriate Change Manager to give them the opportunity to approve the change prior to making it.
- Once the change is deployed and the incident is resolved, the Change Initiator must document the change in Help.HSC as an Emergency Change.
- The Change Manager and the CAB will review all Emergency Changes at their next scheduled meeting.

Standard Changes

A type of change that follows an established procedure or work instruction and is relatively common. Their risk profile is the inverse of the Normal Change, meaning they do not:

- Cause a service outage,
- Run a significant risk of causing an outage, or
- Create a significant change in the end user experience.

Change Models for Standard Changes will be defined by each IT group making production changes. IT personnel may submit a Change Model for each proposed Standard Change for review by the appropriate CAB, using a Normal RFC.

Once a Change Model is approved by the CAB, subsequent changes of that type may be done without bringing an RFC to the CAB.

If a Standard Change results in a production outage or service disruption, the Change Manager may call the Change Model back to the CAB for review.

Service Requests which trigger changes to configuration items in the production environment will also be authorized via Change Management. Normally these are Standard Changes using a Change Model, and only the Change Model requires approval, not each individual change.

Standard Change Categories:

Local Review Changes

- A Local Review change is a Standard Change which requires some form of approval. The team manager will determine whether a team member or the manager must review the Standard Change prior to implementation.

Log-Only Changes

- A Standard Change Model which has been reviewed and approved by the CAB, and which the team manager agrees can be made without further review

Unauthorized Changes

Any change in the scope of this policy which does not follow an approved process is an Unauthorized Change.

IT Directors and Managers are accountable for any unauthorized changes implemented by staff in their units.

Risk and Impact Analysis

The Change Initiator must complete a risk and impact analysis form for all standard changes. See Appendix D for the Risk and Impact Analysis template.

Scheduling of changes

The Change Initiator will review the HSC Global Change Calendar in HelpHSC in order avoid change conflicts and establish a preliminary schedule for the change to be submitted to the CAB. The CAB may require changes to the proposed schedule.

Technical and CAB Approval Requirements

All changes must be submitted through Help.HSC. They must include the following elements for the Change Manager to bring them to the appropriate CAB for approval.

- Title of request
- Description of the change
- Service categorization
- Change category
- Work type
- All configuration items
- Proposed start date and estimated end date
- If an outage is anticipated or required, requested outage dates and times
- CAB assignment
- Major steps to implement and verify
- Risk and impact analysis form
- Backout plan
- Reason for change
- Communication plan

Technical Review Board (TRB)

Generally the CAB review of a change request does not include a detailed review of the technical content of the change. Consequently, the CAB may recommend that an RFC be referred to a technical Review Board (TRB) for review. This review checks the following aspects of the proposed change:

- The working plan associated with the change

- Correctness of all technical information, including preparation, implementation, verification, and back-out procedures

- Completeness of change, testing procedures, and documentation

- Feasibility of the change

- Potential side effects and impact on other services or infrastructure

• Perceived security risk to the HSC

• Worst-case impact (both change and back-out procedure fail)

This review is performed by the technical resources familiar with the area affected by the change as well as other technical resources with general knowledge of the institution, such as systems analysts, security analysts, service managers, service point/helpdesk staff, etc., as assigned by HSC, UNMH, SRMC, or UNMMG managers. TRB members assigned to review a change for one portion of the institution may be requested from other portions of the institution with consent from the TRB member's management. The TRB may be chaired by an assigned CAB member, a project manager, or a change manager as identified by the CAB.

As changes are to be presented to the CAB two weeks before the change implementation, the review by the TRB will be completed within five working days of a change and the change will be referred back to the CAB that has requested the TRB review. If the change is an expedited change, the TRB will have one working day to review the change and the change will be referred back to the CAB that has requested the TRB review. The referral of the change to a TRB, the assigned staff as well as approval or disapproval (along with reasoning) will be recorded as separate journal entries in the change request. TRB's may work by meeting in person and on the phone or via email.

Appendix A - Scope

Defines the types of changes to be handled per this Policy

Item	In/ Out	Description
Software	In	Installation, patching, upgrade or removal of software products including operating systems, commercial off-the-shelf packages, internally developed packages, utilities, and desktop base images
Hardware	In	Installation, modification, removal or relocation of computing equipment such as servers, storage, network printers, and network equipment. Rebooting of production servers.
System configuration	In	Moves, adds, changes and deletes such as firewall changes, access methods, shared system file permission changes, secure FTP keys, etc.
Databases	In	Changes to databases or files such as additions, reorganizations, and major maintenance
Facilities	In	Installation, modification, removal or relocation of equipment in wiring closets, telecommunications rooms, data centers including power conditioning, cooling, fire suppression, and environmental monitoring/alarming systems
Applications	In	Application changes being promoted to production, new application systems being introduced, and obsolete application systems being removed
Applications under construction	Out	Applications that are in the process of being implemented are controlled by the change control process established for the particular project that is underway. (If out of scope, application teams have the responsibility to communicate changes to any affected customers.)

Production Schedules	In	Requests for creation, deletion, or revision to batch job schedules, back-up schedules, maintenance windows or other production schedules managed by IT
Services	In	Services being moved into production, service changes with significant user impact, and services being retired
Services under construction	Out	Decision to commit resources and provide a new service to customers, up to the time a service goes into production.
Telephony System	In	Installation, modification, de-installation, or relocation of PBX equipment and services
Telephony Units	Out	Any modification or relocation of individual phone lines and desk phones (maintained in Pinnacle)
Business Continuity / Disaster Recovery Plans	In	Planning and architecture documents
Desktop	Out	Any modification or relocation of individual desktop equipment
Desktop Owner	Out	Assigning desktop equipment to a new individual or system.
Production Documentation	In	Any changes to standards, procedures, and guidelines
Non-production	Out	Changes to non-production configuration items (CIs) or resources
Daily administrative tasks	Out	Examples include: ▪ End User password resets ▪ User adds/deletes/modifications ▪ Adding, deleting or revising end-user security groups and roles

Appendix B – CAB Logistics

Recommended Agenda:

- Successful and failed changes, backed-out changes, unauthorized changes or emergency changes applied since the last CAB meeting
- RFCs to be assessed and scheduled by CAB members
- Review and update of the Change Schedule, including Changes in progress
- Advance notice of RFCs expected for review at next CAB

Recommended membership:

- Change Manager (chair)
- Applications managers
- Networks managers
- Platforms managers
- Customer Service
- User representatives

Membership notes:

- CAB will be composed according to the changes being considered
- Membership may vary considerably between meetings.

Appendix C – Change Processes

The change management process involves:

- Logging change requests.
- Assessing the impact, cost, benefits, and risk of requested Changes.
- Providing approval or rejection.
- Overseeing the Change implementation.
- Monitoring and reporting the status of Changes.
- Closing Change Requests and conducting post-implementation reviews.

Process Workflow

Figure 1. High-Level Workflow of the Change Management Process
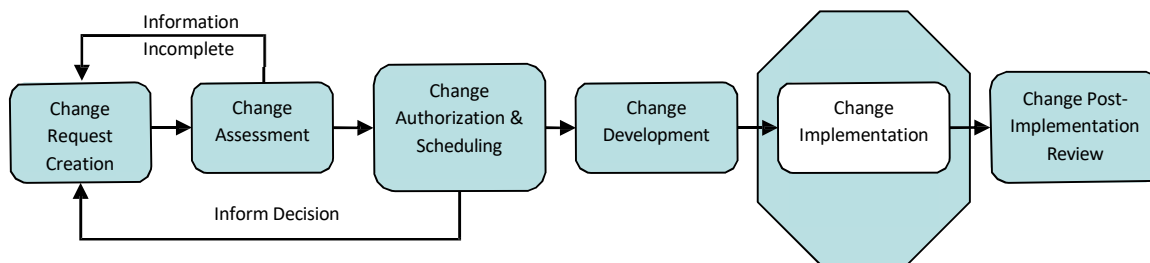
The following pages contain the specific procedures that have been adopted by the organizations using this procedure.

Detail Change Procedures

<u>Normal Changes</u>

1. Change initiator (system analyst, web analyst, DBA, etc.) initiating request for change (RFC) will enter RFC in the Help.HSC system. Change type is *Major*. Changes should be entered into the system **at least two weeks in advance of the actual change date**. If change date is sooner than this, an explanation must be entered. The status of the initial RFC is *recorded.*
2. Change manager will review all changes entered for completeness (all necessary sections have been filled out and are clear). Change manager may request change initiator to clarify or add information if needed. If the RFC is complete the change manager will change the status to *Proposed*. This will populate the change with the approvers based on the selected CAB. The approvers will receive an e-mail notifying them of the waiting approval. HOWEVER, they should not approve until the CAB has met (see steps 4 and 5).
3. The change manger will regularly review the list of changes and prepare that list for the appropriate CAB. The change manager should be responsible for verifying that the proper people are invited to the CAB meeting. This may require working with the change initiator to verify who needs to be included.
4. The CAB will review the following items (via the CAB dashboard in Help.HSC):
   - Completed changes (review successful or not, any issues arising from change)
   - Proposed changes – make recommendation to change manager on approval or rejection
   - Upcoming changes – any slippage of dates will require that RFC status is changed to *Recorded* and change process starts over.
   - Any issues (changes made with no RFC, or any RFC's that caused incidents)
5. Change manager has one of the approvers approve the RFC's per CAB's direction - this will then change status to *Approved* automatically (may take a few minutes for the automatic change to happen in the Help.HSC system). The initiator will be notified via e-mail of the approval (from the Help.HSC system).
6. Change manager closes all completed RFC's (change status to *Closed*).
7. Once change initiator is informed of approval, they will follow the change notification matrix (Appendix E) which may involve sending internal Change Control Notification (CCN) (which can be done via a one step in the Help.HSC system), and any external change communications per their communications plan. Communications initiated to external users should conform to a standard e-mail communication template found in Appendix E.
8. Change initiator executes the change.
9. Change initiator completes the RFC by changing the status to *Competed* and selecting the successful or not successful field.

NOTE: If date (or any other significant information – scope of the change, length of the requested outage, services effected, CI's effected) changes on an approved RFC, the change initiator will change the status back to *Recorded* and the RFC will return to the start of this process.

Emergency Changes

1. Change initiator (system analyst, web analyst, DBA, etc.) initiating request for change (RFC) will enter RFC in Help.HSC. The change type is Emergency and the status of the initial RFC is *recorded.*
2. Change initiator will attempt to contact management and get verbal approval if at all possible. Note the attempt and response in the RFC.
3. Change initiator proceeds with change.
4. The change initiator will change the status to complete and indicate if it was successful.
5. The emergency change will then be reviewed at the next CAB meeting, since it is in the completed status.
6. Change manager will then change status to *Closed*, once the CAB has met and reviewed it.

NOTE: Notification is not a part of this procedure, but if notification (CCN as well as end-user notification) can be done, it should follow the normal change process (step 7 in the normal change procedure).
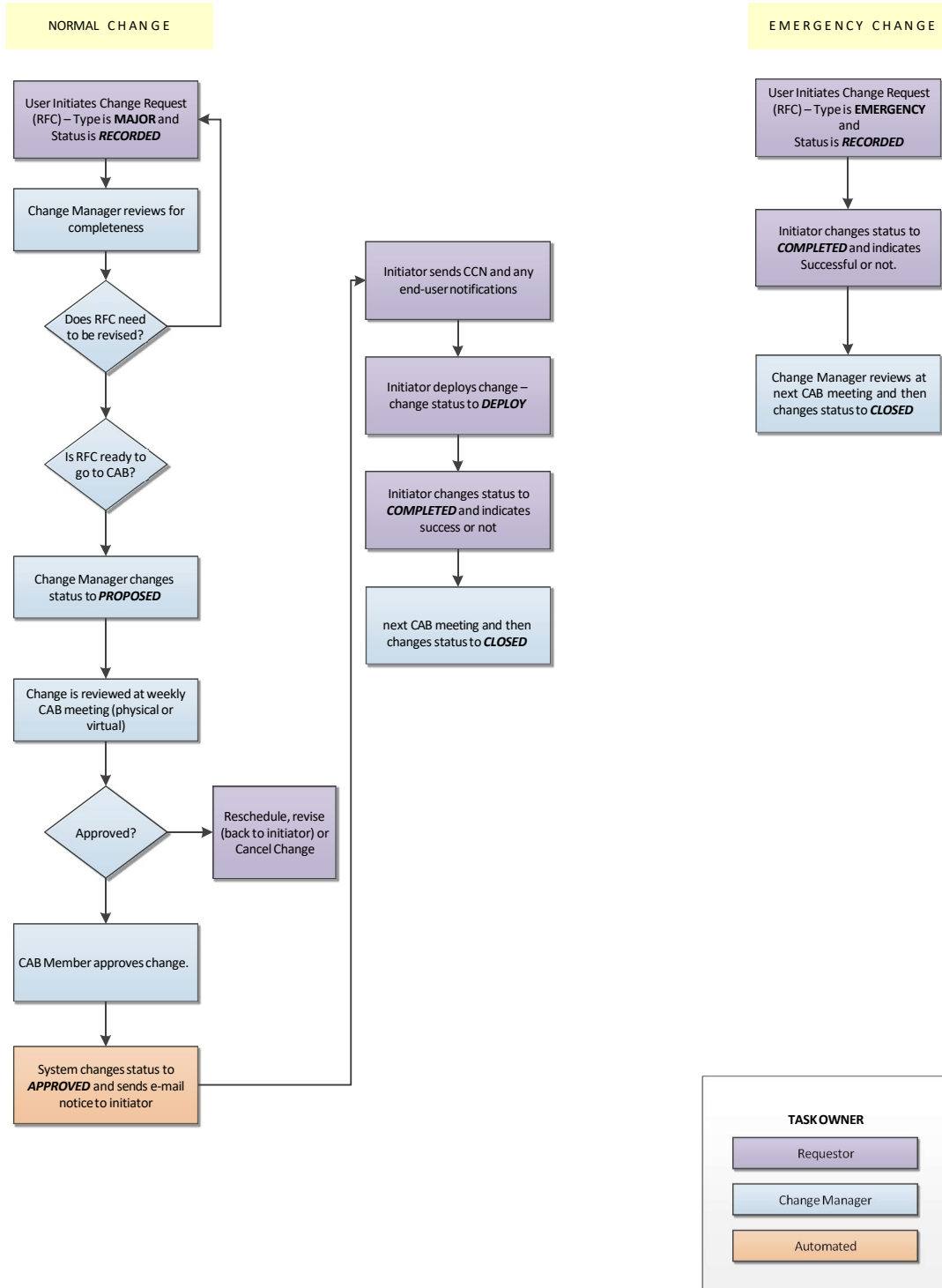
Standard Changes (both Preapproved and Local Review)

1. Change initiator (system analyst, web analyst, DBA, etc.) initiating request for change (RFC) will enter RFC in Help.HSC or the Clinical change database. Change type is either *Local Review* or *Preapproved*. Changes should be entered into the system prior to making the change. The status of the initial RFC is *recorded.*
2. Change initiator is responsible for making sure all the necessary sections have been filled out and are clear. For local review changes the initiator will change the status to *Proposed* and will select the approver. Preapproved changes skip this step.
3. If the RFC is a local review change, the approver will receive an e-mail notification of the change. They will review RFC for completeness and may work with initiator for any needed clarifications. Approver will then approve the change. This will automatically change the status to *Approved* (may take a few minutes). The system automatically notifies initiator of approval.
4. Once change initiator is informed of approval, they will follow the change notification matrix (Appendix E) which may involve sending internal Change Control Notification (CCN- which can be done via a one step in the Help.HSC system), and any external change communications per their communications plan. Communications initiated to external users should conform to the standard e-mail communication template found in Appendix E.
5. For local review changes, the change initiator completes the RFC by changing the status to *Competed* and selecting the successful or not successful field. For preapproved changes, the change initiator closes the RFC by changing the status to *Close.*

NOTE: The change manager is not involved in any of the standard change process. However, once the local review change is marked as completed, the change may be reviewed by the appropriate CAB and at that point the change manager would then close the change. If the change does not need to be reviewed by the CAB, the initiator will change the status to *closed.*

Detail Change Procedure Diagrams

NORMAL CHANGE

EMERGENCY CHANGE

User Initiates Change Request (RFC) – Type is **MAJOR** and Status is *RECORDED*

Change Manager reviews for completeness

Does RFC need to be revised?

Is RFC ready to go to CAB?

Change Manager changes status to *PROPOSED*

Change is reviewed at weekly CAB meeting (physical or virtual)

Approved?

Reschedule, revise (back to initiator) or Cancel Change

CAB Member approves change.

System changes status to *APPROVED* and sends e-mail notice to initiator

Initiator sends CCN and any end-user notifications

Initiator deploys change – change status to *DEPLOY*

Initiator changes status to *COMPLETED* and indicates success or not

next CAB meeting and then changes status to *CLOSED*

User Initiates Change Request (RFC) – Type is **EMERGENCY** and Status is *RECORDED*

Initiator changes status to *COMPLETED* and indicates Successful or not.

Change Manager reviews at next CAB meeting and then changes status to *CLOSED*

TASK OWNER

Requestor

Change Manager

Automated

NORMAL CHANGE

User Initiates Change Request (RFC) – Type is **MAJOR** and Status is *RECORDED*

↓

Change Manager reviews for completeness

↓

Does RFC need to be revised?

↓

Is RFC ready to go to CAB?

↓

Change Manager changes status to *PROPOSED*

↓

Change is reviewed at weekly CAB meeting (physical or virtual)

↓

Approved? → Reschedule, revise (back to initiator) or Cancel Change

↓

CAB Member approves change.

↓

System changes status to *APPROVED* and sends e-mail notice to initiator

Initiator sends CCN and any end-user notifications

↓

Initiator deploys change – change status to *DEPLOY*

↓

Initiator changes status to *COMPLETED* and indicates success or not

↓

next CAB meeting and then changes status to *CLOSED*

EMERGENCY CHANGE

User Initiates Change Request (RFC) – Type is **EMERGENCY** and Status is *RECORDED*

↓

Initiator changes status to *COMPLETED* and indicates Successful or not.

↓

Change Manager reviews at next CAB meeting and then changes status to *CLOSED*

TASK OWNER

Requestor

Change Manager

Automated

Appendix D – Impact and Analysis Template

RISK ASSESSMENT

Risk Score: Low/Medium/High

1. How often has this change been successfully made?
   1 Routinely   2 Occasionally   3 Never

2. What is the degree of difficulty to implement this change? (Consider the complexity of the change, number of devices involved, number of steps in the process, time pressure and number of people involved to accomplish it.)
   1 Low   2 Medium   3 High

3. Has this change been successfully tested, or will it be, prior to implementation?
   1 Yes   2 No

4. Which test environment have you, or will you, use for this change?
   1 Separate/duplicate   2 Shared   3 Partial   4 Production/none

5. Have the recovery procedures ever been successfully tested?
   1 Yes/NA   2 No

6. What type of support is available if external technical assistance is needed?
   1 On site   2 Remote   3 On call   4 Not available

7. What is the degree of difficulty and effort for the Vendor/Partner, if needed, to return the system/component to an operational state?
   1 NA   2 Low   3 Medium   4 High

8. What is the probability of this system/component failing?
   1 Never/low   2 Medium   3 High

9. What is the probability of this change negatively affecting any of the applications, databases, servers or infrastructure components supporting a tier 1 application?
   1 Low/NA   2 Medium   3 High

IMPACT ASSESSMENT

Impact Score: Low/Medium/High

1. What amount of downtime will the user experience, outside of the regularly scheduled maintenance window?
   1 None   2 Less than an hour   3 Greater than 1 hour   4 Greater than 4 hours

2. What is your recovery capability if this change fails?
   1 Easy backout or alternate/fail-over is available and will provide almost immediate service
   2 An alternate is available, but needs to be brought online
   3 No alternate system/component or spare is available

3. Could Patient Safety/Care potentially experience a negative impact due to this change?
   1 Yes   2 No

4. Could providers or mission-critical programs (e.g., academic classes, Poison Center) potentially experience a negative impact due to this change?
   1 Yes   2 No

5. Is end user training required, prior to implementation?
   1 Yes   2 No

6. If the change were to fail, what is the worst case scenario? (In or outside of the regularly scheduled maintenance window)
   1 None   2 Slowdown   3 Partial of full outage

7. If a partial or full outage is possible, has the business successfully tested their manual/contingency procedures, should the change fail?
   1 NA/Yes   2 I don't know   3 No

8. How many IT services/business applications are impacted by this change?
   1 None   2 One or two   3 Three or more   4 All

9. Approximately how many users/workstations will be negatively impacted during the change implementation?
   Number of users/workstations

Appendix E – Change Communication Guidelines

Change Notification Matrix

Change Type	Risk	Internal Notification	External Notification
Normal	High	Required	Required
	Medium	Required	Suggested
	Low	Suggested	As needed
Standard	High	Suggested	As needed
	Medium	As needed	As needed
	Low	As needed	As needed
Emergency	All	If possible	As needed

Change Notification Templates

Template for internal (IT) announcement (Change Control Notification) of an outage or change:

> *Change ID:*
> *Requestor:*
> *Start Date/Time:*
> *End Date/Time:*
> *Outage Start Date/Time: (if needed)*
> *Outage End Date/Time: (if needed)*
> *Description:*
> *Reason:*
> *Other Impacts:*
> *Test Plan:*
> *Recovery Plan:*

NOTE: In the Help.HSC system, you can select the HSC CCN E-Mail one-step under the Change Request Actions menu and the one-step will create the above notification template and will send the Change Control Notification.

Template for public announcements of an outage or change:

> *Event:*
> *When:*
> *Purpose:*
> *Impact to Users:*
> *Details:*
> *More Information/Questions:*

Change Notification Groups

When using the Help.HSC CCN one-step for notifying internal IT staff of changes, the following groups are available to include in the To: or Cc: lines.

- HSC-IT-All – All of the below e-mail groups
- HSLIC-Techs – All HSLIC IT staff.
- HSLIC-Techs-DepartmentContacts – All the HSC departmental IT staff.
- Informatics – Radiology informatics IT group.
- SRMC-IT-Staff – All SRMC IT staff.
- UNMH-IT-Staff – All Hospital IT staff.
- UNMMG-IT – All UNMMG IT staff.

For any change that may affect the entire HSC, the HSC-IT-All group should be used. If the change will only affect a specific group, then that group can be used.