CONE HEALTH	**Guideline:** ITS Change Management Procedure	
	Department Responsible: SW-ITS-Administration	**Date Approved:** 06/07/2024
	Effective Date: 06/07/2024	**Next Review Date:** 06/07/2025

INTENDED AUDIENCE:
Entire workforce

DEFINITIONS:

- A **change** is defined as the addition, modification, or removal of approved, supported, or baseline hardware, network, software, application, environment, or system in production use.
- A **change request (CR)** is a formal documented request for a technology change that is reviewed and approved prior to implementation.
- The **Change Advisory Board (CAB)** is the governing authority for change management policy, procedures, and metrics. This board reviews requested changes, assesses risk level and organizational impact, as well as approves, tables, rejects, or denies change requests.

PROCEDURE:
In accordance with the standards set forth under federal and state statutory requirements (hereafter referred to as regulatory requirements), Cone Health is committed to ensuring the confidentiality, integrity, and availability of all protected health information (PHI/ePHI), sensitive, and confidential data (hereafter referred to as covered information) it creates, receives, maintains, and/or transmits. and confidential data (hereafter referred to as covered information) it creates, receives, maintains, and/or transmits.

The purpose of this procedure is to define roles, responsibilities, and processes for change management and to ensure that the business operations and client/consumer are not negatively impacted as a result of system change or upgrade.

Scope and Goals:
The scope of this procedure is to define the processes associated with change management. Goals of this procedure are as follows:

- Define the change control process
- Establish time requirements for submissions to the Change Advisory Board

Roles and Responsibilities:
Specific roles are defined using industry best practices within the context of the Change Management function only and are not intended to correspond with organizational job titles. In some cases, a single role may be shared by multiple persons; and in other cases, a single person may assume multiple roles.

ROLE	FUNCTIONAL RESPONSIBILITIES
System/Application Owners	System/application owners are responsible for, but not limited to, the following activities:

ROLE	FUNCTIONAL RESPONSIBILITIES
	• Formally identifying individuals who are authorized to submit change requests and attend Change Advisory Board meetings to discuss the request. • Vendors who are responsible for system/application maintenance, upgrades, modifications, etc. will be required to participate in Cone Health's change management process. System/application owners are responsible for ensuring vendors abide by the requirements of this procedure.
Change Requestor	This is the person who initiates the change request and submits the required documentation. Only managers within the group that are accountable and responsible for the change (the change owner) or the individual implementing the change tasks can submit a change request. Specifically, this means that no group will be allowed to submit a change request for any other group. The responsibilities of the change requestor are: • Completes the Change Request form, leveraging appropriate resources as needed. • For preapproved change requests, completes the required checklist (one-time event only). • Optional attendee at Change Advisory Board (CAB) meetings. • As needed, participates in the review of any unsuccessful changes and works with the change owner to initiate related new or modified change requests.

Change Owner	This person has overall responsibility and accountability for the requested change. In many cases, the change requestor and the change owner will be the same individual. The change owner is responsible for providing required information about the change and assists with prioritization as needed. This person is typically involved throughout the process, providing required documentation and clarification, as well as representing the change at meetings of the Change Advisory Board (CAB).
	
	The responsibilities of the change owner are:
	• Has responsibility and accountability to ensure progression of the change through the change management process.
	• Works with the change management facilitator to define priority.
	• Attends Change Advisory Board (CAB) meetings to answer questions and thoroughly represent all aspects of their change request (attendance is required, or the change will not be approved).
	• Develops high-level plans involving other resources as required that identifies:
	  ○ Resources required
	  ○ Equipment and software requirements

ROLE	FUNCTIONAL RESPONSIBILITIES
	○ Vendor or other third-party organizations' involvement ○ Overall schedule ○ Testing ○ Back-out ○ Communications ○ Service/product hand over requirements for operational support (if applicable) • Ensures that the change request form and supporting documentation (e.g., implementation plan, test plan and results, back-out plan) are complete. • Ensures that assigned change tasks are appropriately scheduled, resourced, and implemented. • Validates and signs off on the change implementer's test, implementation, and back-out plans; if the change owner is also the implementer, the test and implementation plans must be approved by management. • Communicates with the change requestor and change management facilitator concerning status (as appropriate). • Ensures appropriate and timely communication to Information and Technology Services staff affected by the change. • Reviews implementation of the change and ensures that all work activities, including documentation of changes as per standard procedure, are complete. • Updates the status of all change tasks and closes the change request when all tasks are complete. • Post-implementation, participates in the review of any unsuccessful changes or incidents caused by the change and works with the change requestor to initiate related new or modified change requests as needed.
Change Management Facilitator	This person serves as facilitator of the CAB meetings, focusing on the process rather than any single change request. The responsibilities of the change management facilitator are: • Serves as a liaison between implementers, requestors, owners, and approvers. • Reviews and filters all change requests. • Establishes priority and impact in conjunction with the change owner. • Runs the CAB meetings and provides meeting agendas and copies of all necessary review information. • Coordinates approvals for urgent change requests on behalf of the CAB. • Maintains and manages the change calendar. • Validates change closure information is complete.

ROLE	FUNCTIONAL RESPONSIBILITIES
	• Reports non-compliance with change management policies and procedures to ITS leadership teams as appropriate.
Change Advisory Board	CAB membership is comprised of Information and Technology Services leadership managers and above. CAB attendance is mandatory for all members. If a delegate is sent, that person must be authorized to make decisions on behalf of the group they represent, and the change management facilitator needs to know of the absence and who the delegate will be. delegate will be. CAB members minimally should have a broad understanding of the business and clinical needs of the user community, as well as the technology environment and ITS support functions. The CAB is responsible for, but not limited to, the following activities: • Assess changes "prior" to implementation to avoid disruption to production systems. • Ensure appropriate recovery/back-out procedures exist so that the impact of any failure during a change can be minimized. • Communicate change status to the business and management who are affected by the change prior to, during, and after the change control process. • Ensure that all changes are submitted in accordance with this procedure and all changes are authorized by the appropriate business owner. • Ensure a risk analysis has been conducted on the purposed change.
Change Implementer	Individual(s) responsible for executing individual change tasks as defined in the approved implementation plan. In some cases, the change implementer will be the same individual as the change requestor and/or the change owner. In the case where there are multiple implementers, change tasks will be assigned by the change owner after the change request has been approved. The responsibilities of the change implementer are: • Creates or contributes to the implementation plan and back-out plan, • Develops a plan to test the change before implementation. • Conducts testing and/or coordinates the testing with the end-users. • Communicates test results to change owner. • Confirms the change implementation schedule. • Advises on communication content related to the impact of the change (e.g., outage windows, desktop restart requirements). • Contributes to the production support handover documentation (if applicable).

ROLE	FUNCTIONAL RESPONSIBILITIES
	• Makes changes to the environment and documents those changes as per standard procedure (e.g., a production change log), including related vendor case or ticket numbers. • Executes validation plan post-implementation to verify if the impact of the change met expectations. • Reports outcome of implementation to change owner. • Executes back-out plan and/or appropriate corrective activities, as needed. • Post-implementation, participates in the review of any unsuccessful changes or incidents caused by the change and recommends process enhancements.
Operations/Business Owner	Individual(s) responsible for: • Assess business/operational impact of change. • Approve business/operational change. • Assist with identifying end users for communications, testing, and validation. • Assist with identifying implementation schedule. • Final sign-off of completion of work.
Chief Information Security Officer (CISO)	The CISO is responsible for, but not limited to, the following activities: • Participate as a voting member of the CAB. • Evaluate all change control requests to ensure they do not negatively impact system security controls. • Assess system security controls after changes have been made to ensure that controls are operating as expected.

Change Management Program:
Changes to information technology can be the result of any one of the following reasons:

- New deployment: Deployment of hardware or software.
- New functionality: Deployment of additional functionality to existing hardware or software.
- Maintenance: Hardware or software fixes, backups, repair defects, etc.
- Security: Hardware or software fixes, backups, etc.
- Upgrade: Hardware or software upgrades.
- Enhancement: Request from client/customer.
- Other: Changes which do not fall within previous categories.

Change Control Requests:
Only workforce members who have been pre-approved by their respective business unit manager will be authorized to submit change requests to the CAB. Improperly filled out or incomplete change requests will not be reviewed by the CAB.

Requestors must be prepared to discuss the following when submitting a change to the CAB:

- Description of the change.
- Reason for the change.

- A clearly defined back-out procedure to be implemented in the event of failures of issues.
- Any risks that will be introduced by the change. If the risks are significant, what mitigation plans will be used to reduce the overall risk.
- Proposed date and time for the change to occur (if outside of normal release schedule).
- Anticipated maximum downtime associated with the change (include time for back-out procedure).
- Description of the information systems that will be changed/affected.
- List of impacted parties.
- Name of person(s) making the change.

There are three categories of change requests: Preapproved, Normal, and Emergency. The categorization dictates roles, processes, and implementation schedules., Normal, and Emergency. The categorization dictates roles, processes, and implementation schedules.

1 - Preapproved

Select change activities are preapproved and follow a streamlined change management process. Preapproved changes have the following characteristics:

- Preventative maintenance that has preapproved recurring scheduled downtime does not have to go through the change management process.
- The planned activities are routine, i.e., a version of the same change has been implemented multiple times in the past and is expected to be repeated in the future.
- The activities/tasks required are well known, documented, and follow a predefined path and time limitation.
- The risk is widely agreed to be low.
- There is no discernible impact on clinical/business processes, end users, or other technology systems/applications.
- No communication is necessary outside of the change management roles defined in this document.

The change management facilitator, with the advice and consent of CAB, will define and manage the list of change activities that are pre-approved.

Preapproved change requests should be submitted no less than 2 days and no more than 10 days prior to the planned change date/time. All preapproved changes will be tracked but are not required to be reviewed by the CAB.

Note: For changes implemented at a regular interval (monthly or more frequent), the CAB may approve an extended period during which a new preapproved change request is not required for each instance. For example, a weekly change task, such as automatic application updates, may be authorized until the end of the calendar year under a single preapproved change request and a new preapproved change request would be required for the following calendar year.

2 - Normal

A normal change request moves through the change management process on a preprocess on a predetermined schedule that is paced for detailed analysis and review. It is not driven by a need to resolve an active incident or service disruption nor to prevent an impending system failure.

A normal change request generally is:

- Submitted for review at least 3 business days prior to the planned implementation start time and no later than the deadline for review at the next CAB meeting (see *Change Advisory Board (CAB) Meetings* section below for deadline information).
- Implemented and completed within 7 to 14 days after approval.

Note: Any normal change request that requires more than 14 days to implement should be broken up into more manageable sets of activities with shorter time spans. For example, large complex projects may have long pilot or early adopter periods and/or phased deployment waves that require multiple change requests.

3 - Emergency

Emergency change requests shall be defined as any action that is necessary for the immediate and continued operation of essential business functions and required to be implemented before the required CAB members are able to review and approve. The requestor will seek the approval from an ITS director, executive director, or vice president beforehand. After the affected system/application/ database/infrastructure has been modified, they will submit a change request and it will be approved post-change by the board. In the judgment of the requestor, if the request is considered an emergency, he/she will make every attempt to contact appropriate CAB members to alert them to the request and its resolution, either by phone or email.

Change Advisory Board (CAB) Meetings

The purpose of the CAB is to make decisions regarding whether or not proposed changes (i.e., performance, operation, improvements, patching, etc.) to network infrastructure, databases, applications, systems and services will be implemented.

Change requests that are not considered “urgent” or “incident response” will be reviewed for completeness, accuracy, and impact to the organization. The CAB is responsible for reviewing change control requests and discussing issues, concerns, or making suggestions with the requester and those who support the implementation of the change. The CAB has the option to ask the requestor to present additional documentation prior to approving.

Changes require unanimous agreement by the CAB members in attendance. If a change is agreed to by the board, it is communicated to the requestor and the teams who will be responsible for implementation. Requests that are not approved will be considered as “under review.” As long as a request is considered “under review,” it will not be approved until all members of the CAB approve the request.

Decisions made by the CAB are final and binding. The CAB is comprised of “voting” representatives from the following business areas:

- Infrastructure Connectivity and Data Center
- Enterprise Architecture
- Integrations
- End User Device and Field Services
- Enterprise Administration
- Security and Access Management
- Application Services
- Others as needed, depending on the change requests that will be reviewed for approval

In addition to the voting members, personnel submitting change requests must attend the meeting that their request will be reviewed.

The CAB will meet weekly on Tuesdays at 11:00 a.m. When their request is on the agenda, change owners (or their designated representatives) will attend CAB meetings to answer questions and thoroughly represent all aspects of their change request. If the change owner (or their designated representative) fails to attend the meeting for a requested change, the change will be ***deferred*** until the following week. Change requestors are optional attendees at the meeting.

The primary objectives to be accomplished at the weekly CAB meeting are as follows:

- Review and approve, deny, reject, or defer changes presented during CAB, based on the following:
  - Risk and impact
  - Planned start/finish dates and times
  - Thoroughness of test plans and implementation plans
  - Documented and realistic support and back-out plans
  - Timely and informative communication to affected clinical, business, and ITS staff
- When appropriate, recommend a scheduled time frame to implement a change, taking into consideration known business and clinical needs, system restriction, and upcoming events such as month-end, year-end, holidays, and other scheduled change implementations. Also, review and request resolution from change owner if a requested change schedule overlaps and/or conflicts with another requested change.
- Request post-implementation reviews (PIRs) when previous changes have resulted in incidents, if a PIR has not already been scheduled.

Change Notification Weekly Distribution List
This distribution list is comprised of ITS and system administrators.

On a weekly basis, the change management facilitator sends an email to the distribution list that itemizes at a high-level:

- All CAB-approved, scheduled changes for the coming week.
- Any emergency changes implemented in the past week that were not included on the prior week's email.

Change Calendar and Scheduling

The change calendar is used by change requestors, change owners, the change management facilitator, and the CAB to identify potential conflicts when determining a timeframe to schedule a specific change. If possible, the change calendar should be published to a location where it can be reviewed by all Information and Technology Services staff who may be stakeholders for scheduled changes.

The change management facilitator is the owner of the change calendar and is responsible for its content, including:

- Scheduled maintenance windows for specified systems.
- Change windows (if specified by the CAB), which are predetermined timeframes during which changes generally have the least risk or clinical/business impact.
- Change moratoriums (if specified by the CAB), which are timeframes when changes are not allowed (e.g., during end-of-month data financial processing, payroll processing, major holidays when staffing will be lower than usual).
- Scheduled outages related to an approved change.

Modifying or Withdrawing Change Requests

Once a change request has been submitted and a situation arises that the request must be updated, corrected, or withdrawn, an email is to be sent to the change management facilitator ASAP. After review, the change management facilitator can, at their discretion, require that a new Change Request Form be submitted for updates or corrections.

Training and Documentation

Change management policies and procedures documentation and training will be provided to current staff and be included in new employee onboarding education. The initial rollout and long-term communication and education plans must address the needs of all audiences within Information and Technology Services, as well as system administrators in other departments.

The Change Request Form, the preapproved change checklist, and any other templates (e.g., implementation plan, test plan) will be stored on the ITS Policies and Procedures SharePoint Site.

Documentation Retention

Change control requests, board decisions, and other pertinent change management documentation will be retained for a period of no less than 6 years from the date of the documentation.

Exception Management

Exceptions to this procedure will be evaluated in accordance with Cone Health's Information Security Exception Management procedure.

Applicability

All employees, volunteers, trainees, consultants, contractors, and other persons (i.e., workforce) whose conduct, in the performance of work for Cone Health, is under the direct control of Cone Health, whether they are compensated by Cone Health or not.

Guideline: ITS Change Management Procedure

Compliance

Workforce members are required to comply with all information security policies/procedures as a condition of employment/contract with Cone Health. Workforce members who fail to abide by requirements outlined in information security policies/procedures are subject to disciplinary action up to and including termination of employment/contract.