**Configuration Management**

The Contractor shall adhere to the following CTEP Configuration Management (CM) policy:

* 1. All system enhancement requests shall be vetted through the CTEP CM process to ensure proper evaluation and prioritization of changes to applications in the production environment according to its impact on the customer, implementation complexity, security, and IT resources.
  2. Depending on the type of change, the Contractor shall present information necessary to make decisions for authorization and implementation of the change. The CTEP approved Change Request (CR) document shall be used to establish a common understanding and agreement among stakeholders regarding the scope of changes (data, software, hardware, network, and people). The Contractor lead is responsible for ensuring that the CR document contains supporting information associated with the change and the recommendations and decision from the CM Review Board (CM RB). The Contractor shall use the following guidelines for assessing the change type (see Table 1).
     1. **Standard Change**: This change type is a preauthorized change to the service or infrastructure. It has an accepted procedure to deliver a specified change need (e.g., maintenance activities, including but not limited to, updates of codes, reports, XML transactions, patching, system updates, etc.). Standard changes shall have a written procedure on how it is done. Except in emergency situations, updates and patches shall be tested to ensure there is no impact on operations. If the system fails after implementation of updates, the system shall be rolled back to its original state, and all findings shall be reported as per Disaster Recovery specifications.
     2. **Minor Change**: This change type is a modification to the appearance and/or function in one application (e.g., application-specific workflow). The change shall not impact the logical data flow of the system, require the hardware to be taken offline, and/or require the software to be restarted without a redundant system to ensure that the software is active for end-users. The CR documentation shall include the business, functional, and technical specifications, the requestor’s information, test plan, end-user notification/ training plan, implementation plan, and back out plan.
     3. **Major Change**: This change type includes a modification to the appearance and/or function of multiple applications (e.g., end-to-end workflow). This change may involve the addition of new technical components into the data model. Also, it may have an impact on the logical data flow of the system, require the hardware to be taken offline, or require the software to be restarted without a redundant system. The CR documentation shall include the business, functional, and technical specifications, the requestor’s information, test plan, end-user notification/training plan, implementation plan, and back out plan.
     4. **Emergency Change**: This change type requires the change to be performed quickly to satisfy an immediate need. It may include a repair to an error in a service that is negatively impacting the research mission. An emergency change is a condensed Standard Change and if possible, the change shall be tested before implementation. Immediate notification to the COR is required upon realization of any system failure for any reason to include natural or man-made disasters.
  3. To ensure conformity to the CM process, changes shall not be implemented to live systems unless an approval was received after review by the CM RB consisting of business and IT stakeholders. After a change is approved by CM RB, the phases of scheduling, building, testing, and implementation shall commence. The CM RB decision shall be entered in the CR document and the decision communicated back to the request owner. The designated CM RB Lead in consultation with the COR shall approve Emergency Change requests.
  4. Only the changes that are approved and scheduled in the change window shall be implemented. After the change is complete, the Contractor lead shall document and report the status (e.g., implemented, failed, or backed out) and lessons learned to CM RB and the COR. All new and closed CR documents shall be uploaded in the designated storage location with the appropriate naming convention.
  5. The Contractor shall provide a proposed maintenance schedule for Standard Changes to include downtime for maintenance/updates with the least impact to the operations of the systems. The Government anticipates peak hours for all systems to be weekdays from 8:00 AM - 8:00 PM Eastern Standard Time (EST).
  6. The Contractor shall work with end-users and NCI Contractors to document the business process flow, gather requirements, and classify the change. The Contractor shall review the current state with every change request to ensure standardization of system workflows and content. The Contractor shall consider ways to reduce complexity of maintenance tasks, support data quality and increase ease of use of the application and other integrated systems.
  7. The Contractor shall work with end-users to validate the business specifications to ensure the change is aligned with operational, regulatory, and scientific needs (e.g., conform with terminology standards for data exchange and FDA reporting, support research data collection in cancer Data Standards Repository (caDSR), support existing or new trials, aligned with operational requirements of NIH/NCI and new/current MCOs).
  8. The Contractor shall collaborate with other NCI Contractors on access management activities to prevent permission creep, e.g., analyze system workflows to ensure that system profiles, roles, and permissions are designed to match the user’s function within the organization.
  9. The Contractor shall collaborate with other NCI Contractors on enhancement and integration activities to ensure that the functional and technical specifications meet the customer’s needs, and work with internal and external stakeholders to identify system improvements to eliminate waste (e.g., retire redundant features/systems) and decrease resources for system maintenance and support.
  10. The CR document shall include detailed requirements with clear assignment to a specific component within the system and associated challenges/risks. The corresponding documentation (e.g., Implementation Plan, Training Plan) shall contain references to targeted performance improvement goals.
  11. The contractor shall maintain development, test, and production environments.
  12. The Contractor shall verify that content changes (new development, enhancements, dependencies etc.) are moved to the production environment upon approval by the request owner or the COR. The Contractor shall resolve defects to ensure the end-user is not impeded from completing their work or using workarounds to overcome system issues whenever possible. The Contractor shall provide resources to adequately handle ad hoc maintenance needs as well as customer support prevent interruptions.
  13. The Contractor shall work with CTEP leadership to identify solutions to improve data processing capabilities, data transmitting mechanisms, data storage, operating systems, and port and protocol changes. All software and hardware requirements shall conform to the Cybersecurity and NIST Standards.

**Table 1.** Change Type(s)

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Category** | **Standard** | **Minor** | **Major** | **Emergency** |
| **Risk Impact** | Low | Low-Moderate | High | Unknown |
| **Application(s)** | One or many | One | Many | Unknown |
| **Content** | Accepted procedure | Display and format (Layout) | Logical/Physical Data flow | Unknown |
| **Contracts** | One or many | One | One or many | One or many |
| **Reason** | Routine updates | End-user request | End-user request | Satisfy an immediate need |
| **Operations** | No Impact | No impact  (End-user training) | May Impact  (End-user training) | Unknown |