Information Systems and Technology Security

Change Management Procedure

Original author's name:	Pkkirisankar Jagannath
Most recent date:	November 22, 2022
Most recent version number:	v1.0
Process owner:	Program Director

Document History

Version	Date	Revised by	Description
v1.0	November 22, 2022	Pkkirisankar Jagannath	Original Draft
v1.0	November 22, 2022	Kulpreet Singh	Ratified Version

Designated document recertification cycle in days:	[Cycle 30 90 180 **365**]
Next document recertification date:	November 22, 2023

Change Management Procedure

The **22nd Century Technologies,** (the "Company") Change Control Standard builds on the objectives established in the **Asset Management Standard** and provides specific instructions and requirements for establishing and maintaining baseline protection standards for Company network devices, servers, and desktops.

The **22nd Century Technologies Change Control** process exists to prevent unauthorized or undesired changes to 22nd Century Technologies-managed client Systems. “Systems” includes 22nd Century Technologies-managed servers, environments, data centers, code bases, code repositories, databases, websites, applications, build and deployment scripts, and monitoring agents.

The Change Management Procedure implements the requirements established in the Change Control Standard and Configuration Management Standard. This procedure supports the maintenance of baseline protection standards for Company network devices, servers, and desktops.

1. Scope

All employees, contractors, part-time and temporary workers, and those employed by others to perform work on Company premises or who have been granted access to Company information or systems, are covered by this procedure and must comply with associated standards and procedures.

- **Change Control** refers to the formal and approved process for submitting, reviewing, and approving changes to the production environment including functions such as testing, documentation, implementation, validation, and tracking.
- **Information Assets** are defined in the Asset Identification and Classification Standard.

2. Requirements

a. Change Request

Change Requests may be initiated via email, telephone, or the 22nd Century Technologies Support PAL by system users, project managers, assets owners, or asset custodians.

- **The team is responsible for submitting a Change Request in Support PAL on behalf of the requestor if the request has been initiated via email or telephone.**

- The team is responsible for processing all Change Requests in accordance with Change Control standard requirements and the 22nd Century Technologies Service Level Agreement. **All Change Requests submitted in Support PAL must clearly document:**

  - Requestor name and contact information
  - Submission date
  - Description of the change
  - Justification for the change
  - Cost justification, if appropriate
  - Request change date
  - Impact on production environment
  - Change requests must have selected one of four priority categories:
    - Severity 1(Critical Business Impact)
    - Severity 2 (Moderate Business Impact)
    - Severity 3 (Minimum Business Impact)
    - Severity 4 (Low or no Business Impact)

- The team can proceed to begin the change request process if the change request is not missing any information or selections.

- **The team is responsible for requesting additional information from the requestor if the change request is incomplete or is unclear.**

Change Request Task Checklist	Responsible
b. Review the change request. • The Team is responsible for reviewing and validating the Change Request. • A Change Request that requires a modification to user’s privileges or access must be processed through the submission of an Access Control Form. The Team will process the Access Control Form in accordance with the Access Control Procedure. • Change Requests that have a Priority Category selection of Severity 1 must be escalated immediately to the Manager.	• Team
c. The Team will assign a Change Control Manager to the Change Request: • The Team will assign a Change Control Manager after a formal review of the: ▪ Description of the Change ▪ Justification of the Change ▪ Impact of the Change • The Assigned Change Control Managers is responsible for validating	• Team • Change Control Manager

the: ▪ Description of the Change ▪ Justification of the Change ▪ Impact of the Change • The Assigned Change Control Manager is responsible for Updating Change Request after completing initial validation and will proceed to complete the next task.	
d. The Change Control Manager will validate or reassign the priority categorization selected in the Change Request in accordance with the Implementation Timeframe defined in the Change Control Standard. **e.** The Change Coordinator will assign the Change Control request to the Manager and the Change Advisory Board for approval:	• Change Control Manager
f. The Manager will review the Change Request and proceed to the **Change Review and Evaluation Tasks.**	• Manager

Change Review and Evaluation Task Checklist	Responsible

g. The Manager will review and select an initial categorization of potential impact level of the change request from the following categories: o Major o Significant o Minor • **The Manager must select a potential impact level of Major or Significant for any of the follow types of changes**: ▪ New Technology (New OS variant, including COTS and appliance, none of which currently exist in the environment) ▪ New Cloud Service Offering or Feature ▪ Potential Change to FIPS 199 Categorization Change ▪ Use of new external services in support of the cloud service or operations ▪ Removal of system components or service offering ▪ Change in PaaS, SaaS or IaaS Provider ▪ Adding/Removing/Disable Security Controls ▪ Changing alternative or compensating security controls ▪ Upgrade of OS ▪ New Virtual Server ▪ New Code release ▪ New Boundary Protection Mechanisms or changes to existing mechanisms ▪ Changes to Routing Rules ▪ Change or update to backup mechanisms or processes	• Manager

▪ New cryptographic modules or services or changes to existing modules/services ▪ New data center location or transfer to new data center location ▪ Scanning tool changes ▪ New system monitoring capabilities or replacement of system monitoring capabilities ▪ New/upgrade of Database Management Service ▪ New Authentication mechanisms or changes to existing mechanisms ▪ Change in cloud service ownership that may result in major changes ▪ Movement of information system data to a different system boundary • The Manager is responsible for updating the Change Request with a justification statement for the impact level assignment. • The Manager may proceed to approve or reject a Minor impact level request but must also request approval from the Program Manager or another Change Advisory Board Member. • The Manager may approve a change request with a Critical severity level but also request approval from Program Manager **and** another Change Advisory Board Member.	
h. The Change Advisory Board will review all Change Requests formally during scheduled Change Advisory Board meetings.	• Change Advisory Board • Assessment Panel • 3PAO

o The Change Advisory Board will formally review any changes that were approved due to a Minor impact level selection since the last meeting. If the Change Advisory Board determines a Change Request has been approved at a minor impact level but potentially may have a significant or major impact it must be immediately reported to the Assessment Panel for analysis. o The Change Advisory Board will formally review all change requests with a significant or major impact level. A Security Impact Analysis must be conducted and documented in the Change Request. o The Change Advisory Board must conduct a formal Security Impact Analysis in coordination with 22nd Century Technologies Assessment Panel for any of the following types of changes: ▪ New Technology (New OS variant, including COTS and appliance, none of which currently exist in the environment) ▪ New Cloud Service Offering or Feature ▪ Potential Change to FIPS 199 Categorization Change ▪ Use of new external services in support of the cloud service or operations ▪ Removal of system components or service offering ▪ Change in PaaS, SaaS or IaaS Provider	

▪ Adding/Removing/Disable Security Controls ▪ Changing alternative or compensating security controls ▪ Upgrade of OS ▪ New Virtual Server ▪ New Code release ▪ New Boundary Protection Mechanisms or changes to existing mechanisms ▪ Changes to Routing Rules ▪ Change or update to backup mechanisms or processes ▪ New cryptographic modules or services or changes to existing modules/services ▪ New data center location or transfer to new data center location ▪ Scanning tool changes ▪ New system monitoring capabilities or replacement of system monitoring capabilities ▪ New/upgrade of Database Management Service ▪ New Authentication mechanisms or changes to existing mechanisms ▪ Change in cloud service ownership that may result in major changes ▪ Movement of information system data to a different system boundary o The Change Advisory Board and the Assessment Panel must submit a FedRAMP Significant Change Form in accordance with the latest FedRAMP requirements for any Significant Change to a FedRAMP authorized system boundary. The Significant Change Request must be validated by an accredited 3PAO. The Significant Change Request must include:	

▪ 22nd Century Technologies Contact Information ▪ System Information ▪ 3PAO Information ▪ Narrative detailing the background and a description of the change ▪ All applicable types of change ▪ Security Controls Impacted ▪ Status of Change ▪ Validation ▪ Demand/Justification o Any request for a New Cloud Service Offering or Feature impacting a FedRAMP Authorized System boundary; the Change Advisory Board and the Assessment Panel must request a 3PAO to complete a FedRAMP New Cloud Service Offering (CSO) or Feature On-boarding Request Report. o Any change requests for FedRAMP authorized system boundaries cannot proceed to the next task until receiving formal authorization of the change request by the designation Agency Authorizing Official or the FedRAMP PMO.	
i. The Change Advisory Board will reject or approve the Change Request. • The Change Advisory Board must formally document and update the status of the Change Request including: • Assign approved change requests to specific production maintenance schedules	• Change Advisory Board

- Provide an explanation for all rejected or deferred change requests - Formally document the functional security requirements, assurance criteria, security controls impacted, and results of any testing performed during the Security Impact Analysis that are the basis for the approval decision.	
j. The Change Advisory Board must assign a Change Control Manager for all approved Change Requests and proceed to the **Change Implementation and Validation Tasks.**	- Change Advisory Board - Change Control Manager

Implementation and Validation Task Checklist	Responsible
k. Change Control Manager will perform or assign testing task to prepare for the implementation of the change. - The Testing must be conducted in the development environment. - The tools, methodology, and results of testing must be documented and updated in the Change Request. - The Change Control Manager will determine whether results of testing have validated the functional security requirements, assurance criteria, and address the security controls documented in the CAB approval. Successful validation in the testing environment can proceed to the next task.	- Change Control Manager - Team - Change Advisory Board

- The Change Control Manager must report any test results that have failed to validate the functional security requirements, assurance criteria, or addressed the security controls sufficiently to the CAB. - The CAB is responsible for determining whether the Change Request should proceed to the next Task.	
l. Change Control Manager will update documentation in preparation of implementation in the production environment including: o Implementation checklist outlining tasks and time estimates o Rollout procedures, responsibilities, and activities o Back-out procedures and restoration activities o Testing procedures to validate the change after implementation	- Team - Change Control Manager
m. The Change Control Manager will validate or reassign the priority categorization selected in the Change Request in accordance with the Implementation Timeframe defined in the Change Control Standard. **n.** The Change Coordinator will assign the Change Control request to the Manager and the Change Advisory Board for approval.	- Change Control Manager - Change Advisory Board
o. Once the Change Control Manager and CAB have determined that the	- Change Control Manager

Change Request will be implemented the Change Control Manager must document the: o Implementation checklist outlining tasks and time estimates o Rollout procedures, responsibilities, and activities o Back-out procedures and restoration activities o Update the 22nd Century Technologies Configuration Management Plan and configuration baselines in the 22nd Century Technologies filesystem **p.** The Change Control Manager will schedule and implement the Change Request. o The Change Control Manager shall follow documented rollout procedures to implement approved changes into the production environment o The Change Control Manager will ensure that the Team Member responsible for testing the Change Request in the Development Environment does not transfer the code from the staging environment to the production environment without coordination with another Team Member or the Manager. o The Change Control Manager is updated the Change Control Request following implementation. Results of changes to the production environment should be reported to	• Team • Manager • Change Advisory Board

the appropriate Asset Owner(s) and the Change Advisory Board	
q. The Change Control Manager will complete the post implementation review. • The Change Control Manager is responsible for conducting security testing or requesting the Team to ensure vulnerabilities were not introduced or service was not interrupted. The Change Control Manager must immediately notify the Manager, Change Advisory Board, and the Program Manager if new vulnerabilities were identified. • The Change Control Manager is responsible for conducting security testing or requesting the Team to ensure vulnerabilities were not introduced or service was not interrupted. The Change Control Manager must immediately notify the Manager, Change Advisory Board, and the Program Manager if new vulnerabilities were identified. If vulnerabilities or disrupted service in the production environment are identified, then the Change Control Manager shall follow documented back-out procedures to restore the production environment to its pre-implementation state.	• Change Control Manager • Team • Manager • Change Advisory Board • Program Manager

• The Change Control Manager is responsible for conducting security testing or requesting the Team to ensure vulnerabilities were not introduced or service was not interrupted. • The Change Control Manager must update baseline configuration documentation, builds, and scripts if implemented changes have been adopted as production standards. The Change Control Manager must clearly identify what updates have been made to configuration documentation if it is not provided in the Change Request.	
r. The Change Advisory Board will formally review the post implementation tasks that were completed since the previous Change Advisory Meeting. • The Change Advisory Board is responsible for ensuring the Change Control Manager completed the Implementation and Validation Tasks and updated all configuration management documentation. • The Change Advisory Board will ensure the Change Control Manager reported the Change in the production environment to the appropriate Asset Owner(s). • The Change Advisory Board will review audit logs and the Change Request to ensure that no single Operations Team Member promoted or committed a change to the	• Change Advisory Board • Program Manager • Assessment Panel

production environment without coordination with another team member or the Manager. • The Change Advisory Board will review audit logs and the Change Request to ensure that no single Operations Team Member promoted or committed a change to the production environment without coordination with another team member or the Manager. • The Change Advisory Board will notify the Program Manager and the Assessment Panel of any significant or major change to a FedRAMP authorized system boundary. ○ The Assessment Panel and Program Manager will be responsible for updating the Risk Register and the System Security Plan as necessary for all security controls impacted by the change.	

Retention and Destruction Task Checklist	Responsible
s. All system life-cycles will follow the Life Cycle Management Standard. • The following tasks shall be performed to retire enterprise-wide systems and applications developed by the Company or on behalf of the Company from the production environment:	• Change Control Manager • Team • Change Advisory Board

o Conduct unit testing and integration testing on the system after component removal. o Conduct operational transition for component removal/replacement. o Determine data retention requirements for application software and systems data. o Document the detailed technical security design. o Update Company policies, standards, and procedures, if appropriate. o Assess and document how to mitigate residual application and infrastructure vulnerabilities. • Disposal of system components must comply with the Life Cycle Management Standard.	

3. Responsibilities

The Program Manager approves the Change Management Procedure. The Program Manager also is responsible for ensuring the development, implementation, and maintenance of the Change Management Procedure.

Company management, including senior management and department managers, is accountable for ensuring that the Change Management Procedure is properly communicated and understood within their respective organizational units. Company management also is responsible for defining, approving and implementing procedures in its organizational units and ensuring their consistency with the Change Management Procedure.

Asset Owners (Owners) are the managers of organizational units that have primary responsibility for information assets associated with their functional authority. When Owners are not clearly implied by organizational design, the CEO will make the designation. The Owner is responsible for defining processes and procedures that are consistent with the Change Management Procedure; defining the access control requirements for information assets associated with their functional authority; processing requests associated with Company-approved access request procedure; determining the level of access and authorizing access based on Company-approved criteria; ensuring the revocation of access for those who no longer have a business need to access information assets; and ensuring the access controls and privileges are reviewed at least annually.

Asset Custodians (Custodians) are the managers, administrators and those designated by the Owner to manage process or store information assets. Custodians are responsible for providing a secure processing environment that protects the confidentiality, integrity, and availability of information; administering access to information assets as authorized by the Owner; and implementing procedural safeguards and cost-effective controls that are consistent with the Change Management Procedure.

Users are the individuals, groups, or organizations authorized by the Owner to access to information assets. Users are responsible for familiarizing and complying with the Change Management Procedure and associated guidelines; following Company-approved processes and procedures to request and obtain access to information assets; ensuring authorization credential such as password and tokens are not written down or stored in a place where unauthorized persons might discover them; reporting immediately to the **Information Security Helpline at 703-879-7996** when authorization credentials have been or may have been compromised; and maintaining the confidentiality, integrity and availability of information accessed consistent with the Owner's approved safeguards while under the User's control.

4. Enforcement and Exception Handling

Failure to comply with the Change Management Procedure and associated guidelines and procedures can result in disciplinary actions up to and including termination of employment for employees or termination of contracts for contractors, partners, consultants, and other entities. Legal actions also may be taken for violations of applicable regulations and laws.

Requests for exceptions to the Change Management Procedure should be submitted to the Company Program Manager. Exceptions shall be permitted only on receipt of written approval from the Program Manager. The Program Manager will periodically report current status to the Company CEO or its designee.

5. Review and Revision

The Change Management Procedure will be reviewed and revised in accordance with the **Information Security Program Charter**.

Recommended: ________________________

Signature

Pakkirisankar Jagannath

Program Manager

Approved: ____________________________

Signature

Anil Sharma

CEO