Cyber Tree Systems
A Business IT Solution Company

# Change Control Policy

## 1.0 Purpose

The purpose of this policy is to provide guidance for how change will be accomplished within the CTS organization on corporate-owned systems and networks, where corporate-owned is defined as any system operating in a CTS production environment on the company network, whether within the company-owned facilities or issued to company agents or employees for use at remote locations for company business.

This policy seeks to minimize systems and network disruption introduced by unmanaged change and maintenance activity. It is management's intent that improved communication and coordination be used to improve system and network stability.

## 2.0 Scope

### *2.1 Applicability*

This policy applies to all CTS employees and affiliates at all CTS facilities and locations worldwide.

### *2.2 Ownership*

This policy is under the direct control of the CTS Corporate CIO with input from the corporate change control manager and other members of management with interest in the program.

This policy is implemented by the CTS Change Control Committee (hereafter CCC). The CCC is made up of the CTS Corporate Change Control Manager, the CTS CIO, and representatives from each CTS division and regional office. The CCC will meet from time to time as scheduled and sit en banc to review and approve change. The CCC will approve change using a simple voice vote with a majority consensus prevailing except that the Change Control Manager and the Corporate CIO each have the ability to veto any change request.

## 3.0 Policy

### *3.1 General Guidelines*

Change can be classified as follows:

CASE 1: Change that requires prior approval of the CTS CCC to implement.

CASE 2: Change that requires notification to the CTS CCC after the fact of implementation.

CASE 3: Change that does not require any notification to the CTS CCC.

CASE 4: Change that is uncertain as to whether or not it requires interaction with the CCC.

Firewall and VPN infrastructure changes are explicitly categorized as CASE 1 changes and require CCC pre-approval. These include any modifications to firewall rules, VPN configuration, encryption protocols, or access policies that could impact security or network stability.

All changes to any network or system device that alter the general availability of any functional service or capability will require interaction as either CASE 1 or CASE 2 change. This includes both the implementation and removal of such services or capabilities.

Changes that affect only single users or the internal operation of specific services or capabilities, such that general use of the system is not affected, are considered CASE 3 changes and do not require interaction. IF YOU ARE NOT CERTAIN THAT A CHANGE IS CASE 3, IT IS A CASE 4 CHANGE. Specific CASE 3 changes include:

Password resets or changes for one user or a set of single users changed at one time. Group privilege changes are not CASE 3 changes; they are CASE 1 or CASE 2.

## *3.2 Specific Guidance*

### *3.2.1 Regional/Divisional Change Control Officer*

Each CTS Region or Division will appoint one person as a Change Control Officer. That person may not be the Regional Manager. It is strongly urged that a designated backup Change Control Officer also be identified and properly trained and kept current with ongoing issues.

### *3.2.2 Change Type 1 - Prior Approval*

Unless required by business availability needs or documented as not requiring CCC approval, all changes to any service or capability must be presented to and approved by the CTS CCC prior to implementation.

All firewall, VPN, and security-related infrastructure changes must undergo a risk assessment and impact analysis before submission to the CCC.

Complete the change request form and follow all steps as outlined in the CTS Change Control Procedure.

### *3.2.3 Change Type 2 – Emergency Change Notification*

When there is not sufficient time available to seek and gain CCC approval, each CTS associate is empowered to make necessary changes for continued business operations that are consistent with the established risk management practices of the organization. However, these changes must be fully documented and reported at the next CCC meeting following the implementation of said change.

Emergency firewall or VPN modifications must be logged in the incident tracking system immediately after implementation, including justification, scope, and rollback plan.

### *3.2.4 Change Type 3 – Non-Reportable Change*

Activities that do not require CCC approval or notification are still subject to all logging and other reporting requirements as may apply.

All CASE 3 changes must be recorded in internal system logs, with automated logging enabled for review by security teams as part of regular audits.

### *3.2.5 Change Type 4 – Unknown Change Impact*

In general, if a change is not known to be CASE 3, it should be considered CASE 1 or CASE 2. If time permits and CASE 1 or CASE 2 change is considered to be burdensome, Regional Managers or individuals designated by the CIO or the Corporate Change Control Manager may query the CTS CIO or the Corporate Change Control Manager to determine which case applies to a specific change item.

### *3.2.6 Periods of Rapid Change*

On some occasions, at the direction of the CTS CIO, the Corporate Change Control Manager may direct the CTS community to implement a rapid change protocol. When the protocol is in force and only for the period specified, all change is to be considered CASE 3 change. This means that changes may be made with the review and approval of only the Regional Manager. All such changes are exempt from CCC approval or reporting but must be logged and reported after the fact using the change control log.

### *3.2.7 Change Windows*

Each headquarters unit and remote location will establish coordinated change windows—posted periods of time when network and systems activity is at a natural ebb and during which complex change activities will have minimal impact on business operations.

All planned firewall, VPN, and security changes must occur within designated change windows, unless an emergency exception is granted by the CCC.

Change logs must include timestamps, implementing personnel, and a detailed impact assessment.

## 4.0 Enforcement

Any employee found to be in violation of this policy may be subject to disciplinary action, up to and including termination of employment.

Failure to document and log changes appropriately, especially for CASE 1 and CASE 2 changes, will be considered a policy violation subject to review by the CCC.

NOTE: As part of the ISA 4810 course, infractions of the rules regarding CCC process will result in a grade penalty.

## 5.0 Definitions

| Terms | Definitions |
| --- | --- |

# 6.0 Policy Document History

## *6.1 Policy Document History*

### *1.x Versioning*

| Name | Date | Reason |
|---|---|---|
| Chief Security Officer | 1/15/20xx | Current revisions |
| CIO | 1/17/20xx | CEO Review |
| | | |

### *2.x Versioning*

| Revision Number | Date | Editor | Reason |
|---|---|---|---|
| 2.0 | 1/16/2025 | Aidan Schmeckpeper | Separated into library and prepared for future edits. |
| 2.1 | 2/19/2025 | Aidan Schmeckpeper | Better conform to new organizational chart and firewall/VPN policy |

## *6.2 Applicable Parties*

This document is strictly confidential and should only be distributed or viewed by the following parties:

- CTS Designated Associates
- CTS Regional Employees
- CTS Management Team
- CTS Auditing Team

## *6.3 Review Period*

This document is subject to review by the Information Security Policy Committee (ISPC) at a minimum interval of every 6 months) and at a maximum interval of every 24 months.

### *6.3.1 Previous Reviews*

| Committee | Review Date | Approval Date |
|---|---|---|
| Corporate CIO | 2/4/20xx | 2/4/20xx |
| Corporate CIO | 1/23/20xx | 1/23/20xx |
| CIO | 1/21/20xx | 1/21/20xx |
| Corp. Change Control Officer | 1/20/20xx | 1/20/20xx |
| Corp. Change Control Officer | 8/22/20xx | 8/22/20xx |
| ISPC | 7/15/20xx | 7/15/20xx |