Administrative Procedure 7207

INFORMATION TECHNOLOGY-
CONFIGURATION MANAGEMENT

Responsible: Office of Information Technology

PURPOSE

This Administrative Procedure establishes a process for changes to Information Technology (I.T.) systems and infrastructure to ensure changes are aligned with best practices and handled systematically and consistently. The scope of this Administrative Procedure is applicable to all Information Resources within Washoe County School District (District). All users of District including employees, contractors, vendors, or others of the organization are responsible for adhering to this Administrative Regulation.

DEFINITIONS

1. "Customer" The person, entity, department, location that the change supports and benefits.

2. "Change Control Board (CCB)" A panel of members that review the changes. Made up of enterprise I.T. members and coordinators.

3. "Change Management Advisor" Oversees the Configuration Management Procedure. Schedules and manages CCB meetings. Generates reports of changes that were implemented for trend analysis.

4. "System Administrator" Installs, operates, and maintains Information Systems. Responsible for implementing changes on the system in support of operational or security requirements.

5. "System Owner" Owns the business process that the I.T. system supports. Responsible for oversight of the system and for ensuring that changes are implemented in accordance with this procedure.

PROCEDURE

1. Baselines

    a. The District establishes a system baseline for information systems that System Administrators and Security employees can reference and control. This baseline serves as a common reference point upon which system development and enhancements are built.

    b. Changes to the baseline will be reviewed and updated after every change has been approved by the CCB and implemented by the appropriate system administrator.

c. System administrators update the baseline configuration and track previous versions.

d. The revision history enables the potential to roll back to a previous known, good configuration.

e. The District leverages automated auditing tools to monitor system states and configuration items to detect any unauthorized changes to the baseline.

f. Where configuration items cannot be managed by automated tools, a repository of changes must be regularly updated, managed, and reviewed by the system administrator.

g. Changes to system and organization baselines must be reviewed, managed, and approved through the configuration management process.

2. Change Requests

a. Changes are system-level modifications or configuration changes that have the potential to introduce unintended impact to the Confidentiality, Integrity, or Availability of a system or directly to users of the system.

b. There are three types of changes:

i. Emergency Changes occur when the security or availability of a service is impacted, and a change must be implemented as soon as possible. An Emergency Change may be implemented to either proactively or reactively prevent a system failure. These changes are such a high priority that they bypass group and peer review and approval, and are immediately authorized by default;

ii. Scheduled Changes (or normal changes) are service changes that follow a prescriptive process which requires approval before being implemented, reviewed, and closed. Most changes are Scheduled Changes; and

iii. Standard changes are pre-authorized changes that are low risk, relatively common, and follow a standardized procedure or work instruction. These changes are frequently implemented, with repeatable steps, and have a proven history of success. Standard changes are pre-approved to follow a streamlined process in which group level or peer approval and CCB authorization are not required. Approved Standard changes may be predefined in a catalog of templates maintained by the Change Management

Advisor to make accessing and requesting the standard change more efficient. Standard changes are reviewed after implementation.

3. To make a change, a System Administrator must have prior approval. Change Requests are submitted, analyzed for functionality and security impacts, approved (Change Control Approval), scheduled, performed, and reviewed.

    a. Trigger – something occurs where the system configuration needs to change. This can be for functionality, security, or compliance purposes. This request is communicated to I.T. through a work order or ticket.

    b. Determine type of change (Emergency, Standardized, Scheduled). The System Administrator performing the change independently analyzes the work to be performed and determines the priority level and circumstances around how the work needs to be performed.

    c. The System Administrator submits a Change Request (CR) through the enterprise ticketing system. The CR includes:

        i. An overarching description of the change

            1) Configuration item. The item that is being changed;

            2) Change summary. A short description of the change;

            3) Change type (Emergency, Standardized, Scheduled). The type of change being performed. Determines the schedule, timing, and review process for the change;

            4) Date required. The deadline for when the change needs to be implemented in order to provide services for the organization;

            5) Proposed implementation date;

            6) Expected duration. How long the change is expected to take to implement;

            7) Site \ location. Where the configuration item is located. May be multiple sites, buildings, or regions; and

            8) Priority. Critical (emergency), high, medium, low (timelines for implementing based on criticality). Based on operational and compliance requirements.

ii. Impact

1) To Users;

2) To Services. Includes services directly provided by the system as well as inter-dependency and integration analysis; and

3) To Business.

iii. Additional Costs

1) Resource;

2) Operational; and

3) Licensing.

iv. Communication Plan

1) How users are notified about the change;

2) Service alert required; and

3) Website update required.

i. Testing Plan

4) How the change has been tested to ensure that it will be successful.

ii. Rollback Plan

5) How we revert the change if it fails; and

6) The system has a backup and recovery plan.

4. Security Impact Assessment (SIA) is performed and attached to the CR. The SIA identifies security and compliance risks associated with the change.

5. Change Control Board members review the CR and associated SIA individually.

   a. If no additional review is necessary, The CCB can approve the change via email.

   b. If additional review is necessary, the CCB can elect to meet and review the change.

6. Change Requests are Approved, Deferred, or Rejected.
   a. Approved CRs are scheduled for implementation.
   b. Deferred change requests are put back into the CCB queue.
   c. Rejected CRs are cancelled and will not be performed based on the prospective risk or impact associated with the change.
7. After CRs are scheduled, they may be implemented, failed, or cancelled.
   a. CRs that are implemented are completed successfully. System Administrators performing the procedure closes the Change Request.
   b. CRs that are failed are unable to be completed for technical or operational reasons.
   c. CRs that are cancelled are not completed due to technical or operational reasons.
8. The CCB reviews the changes performed monthly and analyzes changes, frequency, impacts, and additional resources needed to improve service delivery.
9. Enforcement
   a. Any user found to have violated this Administrative Procedure may be subject to disciplinary action as provided for in other agreements.

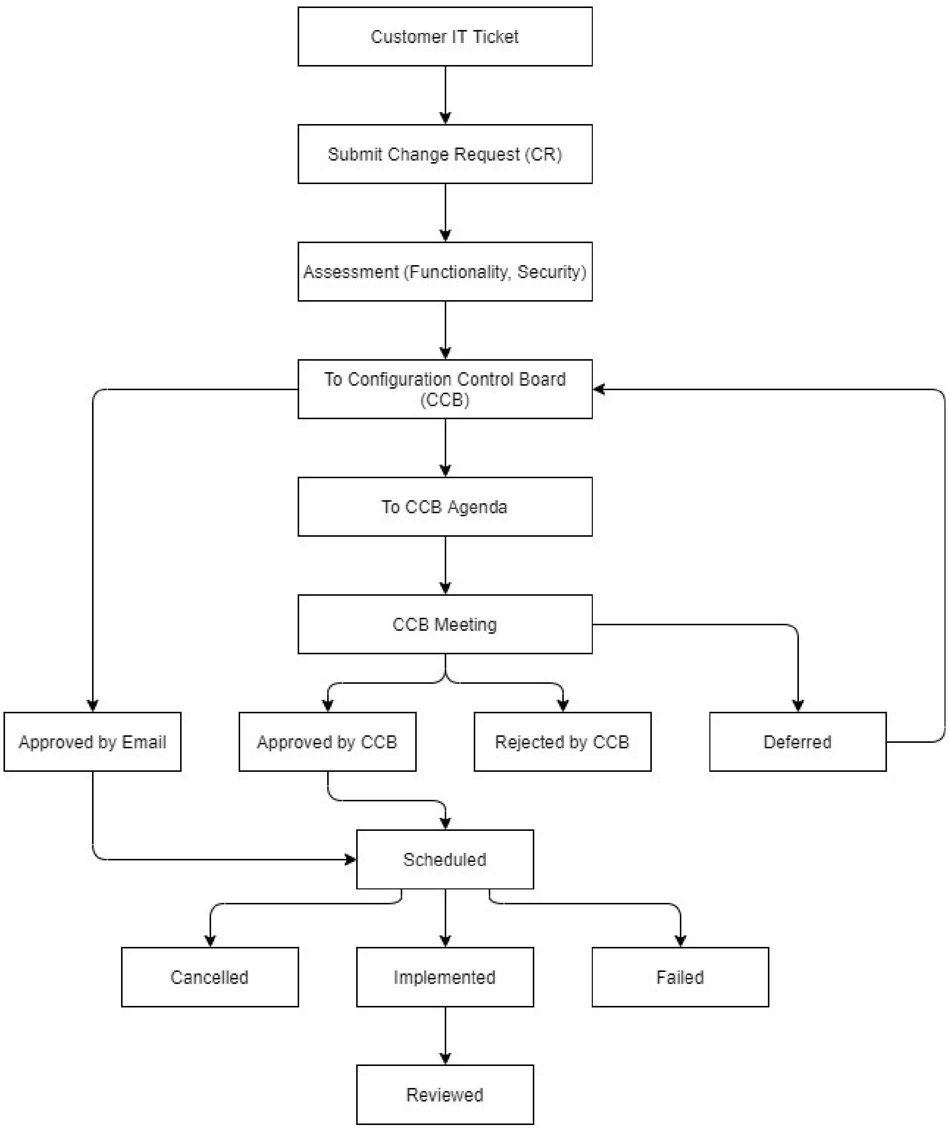
LEGAL REQUIREMENTS AND ASSOCIATED DOCUMENTS

1. This Administrative Procedure reflects the goals of the District's Strategic Plan and aligns/complies with the governing documents of the District, to include:
   a. Board Policy 7205, Information Technology – Data Access; and
   b. Administrative Regulation 7211, Responsible Use and Internet Safety.

REVISION HISTORY

Date	Revision	Modification
07/25/2022	1.0	Adopted

IT Change Management Process


Customer IT Ticket
Submit Change Request (CR)
Assessment (Functionality, Security)
To Configuration Control Board (CCB)
To CCB Agenda
CCB Meeting
Approved by Email
Approved by CCB
Rejected by CCB
Deferred
Scheduled
Cancelled
Implemented
Failed
Reviewed