Recommend

WASHINGTON CENTRAL UNIFIED UNION SCHOOL DISTRICT

Board of Directors' Policy

CHANGE MANAGEMENT

POLICY: F40

WARNED: _____

ADOPTED: _____

EFFECTIVE: _____

Overview

The objective of change management in this context is to ensure that standardized methods and procedures are used for efficient and prompt handling of all changes to control IT infrastructure, in order to minimize the number and impact of any related incidents upon service.

Purpose

To control all changes to equipment, software or procedures will be established and followed for change, integrating operational and application change control procedures, and logging all changes.

Change Advisory Board (CAB)

A CAB is a group of people who run formal CAB meetings to assess, prioritize, authorize, and schedule changes as part of the change control process.

There are two components of a best practice CAB: 1) The right people and 2) An effective CAB meeting structure.

The CAB should include at least one representative from all groups affected by the changes on the agenda (including non-IT groups and student(s) if applicable) and can include managers or non-managers, such as a network engineer or teacher or administrator. It is likely to include groups from functional and technical disciplines such as the IT Helpdesk, application support, server support, etc. An affected manager of a change (or team leader) who was invited but cannot attend a meeting may designate an alternate to attend in their place. Please ask the CAB owner (chairperson) for guidance as needed on this item (or any item in this policy document).

The CAB owner acts as a chairperson and should be a CAB member. This person is typically a change manager or on the change management team.

The responsibilities of the CAB members include the following:

- Review changes prior to the meeting.
- Assess and recommend the approval or rejection of proposed changes in a timely manner. If a CAB member doesn't approve a change, make sure they explain why.
- Attend scheduled CAB meeting(s) or send a qualified representative.
- Act as a liaison between the CAB and its team regarding change management policies, procedures, questions, or enhancements.

The responsibilities of the CAB owner include the following:

- Develop the vision and strategy for CAB meetings.
- Lead CAB meetings and make sure the required representatives attend (representatives from all groups affected by changes).
- Define and communicate the CAB members' roles and responsibilities.
- Document and communicate the CAB meeting agenda before CAB meetings and decisions after the meeting.

Regular CAB meetings should take place at least monthly; however, a weekly or biweekly schedule is recommended.

All teams affected by a change should be represented in the CAB meeting.

The CAB Meeting Agenda should include the following:

- All high-risk changes and changes marked as required by the CAB
- A review of all failed and backed out changes
- Change management process updates
- Reviews for each change that include:
    - A risk/impact assessment (on the district)
    - The effects on the infrastructure and customer service as defined in the Service Level Agreement (SLA) as well as on capacity and performance, reliability and resilience, contingency plans, and security
    - The impact on other services that run on the same infrastructure (or on software that is in the cloud)
    - A resource assessment, including the IT, district, and other resources required to implement and validate the change
    - The effect, risk, and/or impact of not implementing the change
    - Other changes being implemented on the schedule of change
    - Technical capability and technical approval required

A change that goes into production can impact many teams, including central office, parents, administrators, students, IT, and other groups. If you don't consider all technical impacts of a change, there is a higher risk of a system outage or malfunction. This makes an effective CAB essential because it provides awareness of the changes for impacted teams and makes sure all technical aspects of a change are considered.

Types of Significant Change

There are three types of significant change that should be considered:

Standard Change – Standard Change is a consistent or routine change that takes place on a regular interval (weekly, monthly, quarterly, yearly) that should be formally reviewed and approved before being implemented. These changes have fairly common steps and guidelines and are generally low risk to the environment and seldomly require modification.

Once approved, this change does not need to go back to a change advisory board (CAB) or administration team for regular approval.

However, the schedule for change must be published and communicated on a regular basis. Additionally, if a standard change causes an issue or outage, it must be brought back to the CAB for review and discussion.

Examples of Standard Change:

- Lifecycle replacement of hardware
- Routine Software Patching and Updates
- Firewall Changes not requiring a service outage
- DNS entries

Normal Change – Normal Change is a change that may be common, but may also be unique in its construct. A normal change should be reviewed (and approved/scheduled or denied) by the CAB or administration as it may contain risk to the environment such as system downtime, data loss, security risk, enumeration or dissemination of PII, PHI, or other types of information.

Examples of Normal Change:

- Storage or Virtualization Platform replacement
- Application upgrade that impacts functionality or the data model of a system
- Telephone system enhancement or upgrade work that may cause an outage

Emergency Change – Emergency Change is a Normal Change that must be introduced and implemented as soon as possible, even before the CAB or administration team needs to approve or deny the change. The CAB owner will quickly determine if emergency change is warranted for a particular circumstance. These changes typically represent a crisis or opportunity that must be addressed without undue risk to the district. While the change may need to be implemented before a CAB meeting, the change MUST still go through the CAB or administration team AFTER implementation so they can review the efficacy of the change and the emergency nature of it and provide their approval or dissent to the change. YOU MAY NOT SKIP THIS PART OF THE PROCESS.

Examples of Emergency Change:

- Implementing a security patch to a zero-day exploit
- Isolating the network from a large-scale Distributed Denial of Service (DDOS) Attack

Change Management Requirements

There shall be a formal approval for proposed changes that could potentially impact the operational environment. Prior to any operational change there shall be a risk assessment that:

- Identifies significant changes.
- Records significant changes.
- Assesses the potential impact of such changes.

- Procedures and responsibilities for aborting and recovering from unsuccessful changes
- All changes shall be reviewed in advance and requires the written approval of the or designee.
- All changes shall be communicated to all relevant individuals.

Change Policies Computers/Workstations

There shall be a formal approval for proposed Local Administrator Access: WCUUSD service users will not have the right to change the local administrator passwords on WCUUSD provided desktop computers. Service Users may request access to the local administrators group from the Information Technology Department, however, this will void the computer and the service user from being supported by the Information Technology Department. Systems that have been modified and require the assistance of the Information Technology Department will be re-loaded with the original software configuration that the Information Technology Department supplies to service users when issued a new system.

Configuration Changes: The standard network and systems configuration on WCUUSD laptops is configured so that in most cases the computer can be transferred from network to network without substantial configuration changes.

Changes to Hardware: Computer equipment supplied by WCUUSD must not be altered or added to in any way (e.g., upgraded processor, expanded memory, or extra circuit boards) without prior knowledge and authorization from the Information Technology Department.

Changes NOT Related: Any changes that are not related to the changes listed above must adhere to and comply with the District Change Management Policy.