Change Control Procedure

Subject	Effective Date	Division / Area	Approval:	Signature
Change Control Procedure	Effective Date: 03/27/2024 Issue Date: 03/27/2024 Review Date: 03/27/2025	Business & Finance / Office of Information Technology	**Rose McAuliffe** **VP Business & Finance/CFO** **3/25/2024** **Al Speckens** **Interim Deputy CIO** **3/25/2024**	Rose McAuliffe Al Speckens

Stanislaus State

Change Control Procedure

1 PURPOSE

Stanislaus State is fast becoming a campus that heavily relies on technology and data to achieve strategic goals. Faculty, staff, and students depend on OIT to keep multiple, high availability services operating without disruption. Therefore, our Change Control process must evolve and mature to meet this evolution and its related expectations. The following principles are the foundation to achieving this outcome.

As a division we must operate from a mindset of:

- Service Excellence - Changes introduced do not interfere with the achievement of explicit or implicit service level commitments to business partners and customers.
- High Availability – Unavoidable change related service disruptions are kept to an absolute minimum.
- Strategic Support – Changes must conform to stated business and technical plans and strategies.
- Efficiency – Changes are processed promptly, efficiently, and in a non-bureaucratic manner, appropriately blending formality with effectiveness.
- Communication, coordination – Changes are communicated to all affected parties, internal and external, timely and informatively.
- Partnership – All stakeholders, internal and external, provide informed consent prior to proceeding with change implementation.
- Reliability – Changes are implemented in an orderly and consistent way using established (and repeatable) methods and procedures.
- Control – Changes are implemented in accordance with scheduled implementation date or implementation windows or as agreed to by customers.
- Continuous Improvement – Change activities are measured, correlated to a problem management process, and reported. Experience gained is incorporated into changing policies and practices, creating a learning organization.
- Web Standards and Security - Adhere to the OWASP Top 10, which details web standard web application awareness and security practices through ongoing network scans via Qualys.

DEFINITION OF A “CHANGE”

According to ITIL, a Change is "the addition, modification or removal of anything that could have an effect on IT services." Most often, a change is an event that has been approved by the change authority, is evaluated, and implemented while minimizing risk, adjusts the status of a configuration item (CI), and adds value to the business and its customers.

The most crucial element of this definition is that a change is a risk. The word "could" refer to a possibility and, "possibility" is a central notion of risk. Whether the impact is potentially negative or positive, it is still a risk.

The definition also refers to “The addition, modification or removal of anything...". By referring to "anything" instead of Configuration Items (CIs) means that Change Control is more than simply a process to maintain the accuracy of the CMDB.

2 CHANGE CONTROL PROCEDURE

All changes to OIT systems, services and applications must follow a structured process to ensure appropriate planning and execution.

Prior to submitting a change request, it is the responsibility of the change requestor to verify that the application or system exists in the OIT application inventory DB and that the maintenance window recorded coincides with the one requested, otherwise, consult with your manager to determine whether this request will be out-of-band or if the window should be changed in the application inventory database.

There are three types of changes in scope for change control:

- Routine Change
- Emergency Change
- Standard Change

Recommendations shall include:

- All changes requiring official stakeholder communications orchestrated by OIT communications coordinator must be submitted 2-3 weeks prior to implementation.
- Changes should be documented thoroughly, including risks and a back-out plan.
- Changes should be reviewed by the submitter’s manager/director prior to the Change Control meeting.
- The submitter of the change request(s) must attend a change control meeting or bring someone up to speed to represent and speak to their change to gain approval on your behalf.
- All changes must be reviewed and approved by the Change Control Board.

This procedure is to establish management direction and high-level objectives for change control.

3 SCOPE

This Change Control procedure applies to all changes to production applications and systems.

OPERATIONAL WORK

Some common activities that do not affect an IT Service and are not changes and can be considered operational work, these include Incidents, Problems, and Service Requests such as:

- A service request to order standard hardware or software.
- The creation of an additional user account
- Resolution of an incident which does not require a change.
- Testing hardware to ensure that it is not defective (burn/bench testing prior to deploying (commissioning) the hardware in production.
- Adding a network port
- Provisioning a server in the VM environment

Even though these examples may not be changed, they may result in a change request if the requested work poses a potential risk to the organization.

Since operational work is not tracked through the Change Control Process, it should have separate processes by which it is logged, such as an Incident, Service Request, or a Project and the related procedures should be well defined and documented. The initial decision to determine what is and what is not an operational change falls under the direct manager's judgement. If it is determined that some aspect of the operational work poses a potential risk to the organization, then the chance control board may require that it go through the Change Control process.

4 CHANGE CONTROL BOARD

The Change Control Board is composed of the OIT executive team.

- CIO
- Director of Technology Services
- Director of Information Services
- Director of Client Services
- Director of Learning Services
- Information Security Officer

The Change Control Board is responsible for approving and rejecting all change request(s).

5 CHANGE CONTROL MEETING

The followings individuals are expected to attend the meeting:

- Change Control Board
- Directors and Managers
- Submitter of Change Request(s)
- Leads and SMEs

If the individual required is not able to attend the Change Control meeting, he/she should send a representative. All individuals are responsible to review and raise any potential concerns about the impact of any change requests.

6 TYPES OF CHANGES

6.1 Routine Change

Also known as a recurring change is a repeatable change that has been pre-authorized, has documented procedures, is regularly scheduled, controls risk, and has predictable outcomes.

Examples:

- Windows Updates/Patching
- Voicemail Restarts
- Custom Development Patches
- Datawarehouse Report Updates

6.2 EMERGENCY CHANGE

A change that must be introduced as soon as possible due to current or negative service impacts. (Note: Missing the standard submission window/deadline does not constitute an emergency.)

Examples:

- Zero Day Patch
- Hardware Failure or Failing Hardware
- Software Updates to address urgent business requirements.

6.3 STANDARD CHANGE

The Standard Change is defined by what it is not. Since it is not a routine or an emergency change, it is simply every other change and must be authorized.

Examples:

- Application Patching/Upgrade
- System Parameter Change
- Hardware Change Out
- Scheduled event that would normally take place in a standard change window.
- Agent Patching/Upgrade

7 CHANGE PROCEDURES

7.1 Routine Changes:

1. Submitter's manager/director to review the change and its impact with CM Board considering:
    a. Impact on campus i.e. stakeholders
    b. Documentation format based on documentation framework.
2. The submitter and immediate supervisor coordinate change requests with affected parties/dependencies and initiate any required communications to the affected parties and the campus.
3. CM Board reviews related documents based on approved documentation framework.
4. Change request is scheduled and reviewed at the Weekly Change Control Meeting:
    a. If approved
        i. Change is entered in the Change Control calendar for recurring changes.
        ii. Change request is closed.
    b. Exception
        i. If the proposed change is rated low and approved by immediate supervisor, then it can be logged in Change Control and completed without meeting review.

7.2 Standard Changes:

1. Complete Change Control form for the specific change, using TeamDynamix Form.
2. Submitter's manager/director to review change and impact assessment prior to the Change Control meeting.
3. Submitter and immediate supervisor to coordinate change request with affected parties/dependencies and initiate communications to campus.
4. Change requests are reviewed at the Weekly Change Control Meeting.
5. Change requests are approved, rejected, on-hold, cancelled.
6. If approved
    c. Change request is implemented and tested.
    d. Change request is closed.

7.3 EMERGENCY CHANGES:

1. Change control procedure for Complete Change Control form for the specific change, using TeamDynamix Form.
2. Submitter's manager/director to review change and conduct impact assessment prior to further coordination.
3. Submitter and immediate supervisor to coordinate change request with affected parties/dependencies and initiate communications to campus.
4. An email documenting the emergency nature of the change should be sent to the Change Control TDX workflow for approval. Approval is required from at least one Change Control Board member.
5. Change requests are approved, rejected, on-hold, cancelled via email.

6. If approved.
    a. Change request is implemented and tested.
    b. Change request is closed.

If a change request gets implemented but encounters issues and needs to be backed out, it is recommended that the issues be documented and captured in the form on the Change Control TeamDynamix site.

8 Maintenance Schedules

All changes are recommended to occur within the maintenance windows. Refer to the inventory spreadsheet to find out the designated maintenance window for specific systems, services and applications.

A. 3rd Wednesday & Thursday of Month 12:00 AM – 6AM for dev/test systems 1st Wednesday & Thursday of Month 12:00 AM – 6AM for production systems	B. Friday 12:01 AM – 6AM	C. Friday 6 PM – Saturday 6 AM	D. Exception - TBD

A. OS (Operating System) Patch management: Dev/Test/Prod
B. Upgrades or Application/Database Patching (Low/Medium Impact)
C. Upgrade or Application/Database Patching (High Impact)
D. Exception

8.1 OTHER REGULARLY SCHEDULED MAINTENACE TASKS

1. Server Vulnerability Scans: Thursdays at 10:00pm – 11:59pm
2. Web Vulnerability Scans: Schedule TBD

8.3 CHANGE FREEZE PERIODS

During business-critical times of the year for teaching in learning, there will be a period in which no IT changes are encouraged or allowed except in an emergency and with CIO consent and approval. Those periods of the year are:

- A week before and week of the beginning of Fall and Spring semester.
- A week before and week of the end of Fall and Spring semester.
- The day of deadline for final grades submission for the Fall and Spring semesters.

9 Impact Level

The designated maintenance windows for each system (see application inventory link above) are intended as a guideline. The impact of each individual change will need to be assessed based on the criteria below. The change may be scheduled in a different window due to this impact assessment.

When classifying the type of impact of a change, please use the criteria matrix below.

	EVALUATION CRITERIA			
	Service Impact	Service Criticality	User Experience	Timing
High	Service interruption or downtime required.	Campus-wide mission critical service	User experience is expected to change significantly.	Critical academic and/or business cycle is impacted.
Medium	Service interruption or downtime.	Business-unit mission critical or campus-wide with > 100 users	User experience change is expected to change minimally.	No critical academic and/or business cycle is impacted.
Low	No service interruption	Not mission or business unit critical, < 100 Users	User experience is not expected to change.	No critical academic and/or business cycle is impacted

10 Communication Types

Staff is directed to consult with their direct managers to determine the appropriate type of campus notification for each requested change. Campus notifications must be in accordance with the evaluation criteria above. Criticality of the maintenance might vary due to the change's time, such as summer or winter break when change requires less communication.

Below are example types of communication identified:

a) Stan State OIT Website: OIT Maintenance calendar with link to change request.
b) System Message via OIT Communications
c) Monday Briefing
d) Broadcast Emails
e) Targeted email(s)
f) Voicemail to all campus users
g) Notification to the VP for Business & Finance / CFO for high risk

IMPACT & COMMUNICATION MATRIX

The following are recommended communications based upon the category and impact level of each change. The Change Control Board may recommend additional communication types based on the specific change request and time of year. Key academic and administrative dates should be considered in this process. Criticality and impact of the change might vary based on the date and time of the change, Messaging type must be reviewed with the immediate supervisor prior to the change, typically 2-3 weeks prior to the requested change and will be discussed at the Change Control meeting to ensure appropriate messaging type is chosen.

- Staff and supervisors should coordinate with IRT's communication specialists to develop content, schedule, and deploy communications accordingly.

Routine Change announcement type

- Stan State OIT Website: OIT Maintenance calendar with link to change request (to be created)
    - Users are inundated with emails and messages of all types, and we must use the most appropriate messaging type for our announcement to insure effectiveness.
    - Use of targeted messaging is encouraged.

Standard & Emergency Changes announcement type

	CSUSTAN OIT Website	System Message	Monday Briefing	Broadcast Emails	Targeted Email	Email VP of B&F
Low	x	x				
Medium	x	x	x		x	
High	x	x	x	x	x	x

Criticality and impact of the change might vary based on the date and time of the change, Messaging must type must be reviewed with the immediate supervisor prior to the change and will be discussed at the Change Control meeting to insure appropriate messaging type is chosen based on the time of the year and critical campus events.

12 ROOT CAUSE ANALYSIS FOR SYSTEM FAILURES

Issues with production applications, infrastructure or systems that result in a degradation of service, or a service interruption may be subject to a root cause analysis and review by the Change Control Board. The Root Cause Analysis process is intended as a continuous improvement tool by which the organization can learn from and, when appropriate, help minimize the likely hood of a repeat occurrence. Actions taken may include, but are not limited to, a new procedure, an update to one

or more existing procedures or a change to the system or application itself. The Root Cause Analysis Form can be found on the Change Control TeamDynamix site.

12.1 WHEN A ROOT CAUSE ANALYSIS IS REQUIRED

A Root Cause Analysis will be performed when there is a degradation of service, or service interruption to an application, infrastructure or system reported in TDx process.

12.2 ROOT CAUSE ANALYSIS PROCEDURE

1. The Manager that has responsibility for the infrastructure, system or application will be responsible for performing or delegating the root cause analysis.
2. The Manager or designee will fill out the Root Cause Analysis Form within one week of the occurrence. If the Root Cause Analysis will take longer than one week, then the Manger or designee will keep the Change Control Board advised on the progress of the analysis at each change control meeting until completed.
3. The Manager or designee will upload and attach the completed Root Cause Analysis Form to the specific and related outage record in TDx.
4. The Change Control Meeting will display the analysis and provide an opportunity for the Manager to present the Root Cause Analysis and the Change Control Meeting immediately following the form uploaded at the next scheduled meeting.
5. The Manager or designee will present the findings of the Root Cause Analysis to the Change Control Board, ensuring all questions on the form are covered in the presentation.
6. The Change Control Leader, in conjunction with the Manager, will lead a constructive, learning oriented discussion, Q/A Session around the Root Cause Analysis.
7. The Manager will consider and incorporate any recommendations or new lessons learned as a result of the discussion into the report and resulting changes and/or procedures.
8. Any changes to the affected applications, infrastructure or systems that require remediation as a result of the issue, will go through the Change Control Process and be the responsibility of the MPP owner to complete.