California State University Northridge	**Information Technology Standard Operating Procedure** CHANGE MANAGEMENT CONTROL	**Page** 1 of 10	
		SOP#: XXXX-90-09-0XX	**Revision#:** Version 0.X

Prepared by: Greg Nicols **Date:** 7-09-2012	**Approved by (IT Sr. Director):** Chris Olsen **Date:** 7-10-2012
Last revised by: Chris Olsen **Date:** 7-10-2012	**Last approved by (IT Sr. Director):** **Date:**

1.0 PURPOSE

Campus Information Technology strives to deliver high-quality services to students, faculty and staff. Part of the campuses commitment to quality includes the minimization of unscheduled downtimes that can create considerable disruption to University business and interfere with the educational mission of the University. Non-emergency changes to production hardware and software should be implemented during normal, scheduled downtimes, with adequate notice given to affected customers, and with appropriate consultation with stakeholders. Furthermore, major changes to hardware and software should only occur after careful review by Campus IT technical and by the Director of IFS.

2.0 SCOPE

Change Management applies to:

1. Production systems, network equipment and applications, database systems and environments, enterprise applications, servers/systems/appliances, desktop environments, VoIP and analog telephone instruments and management systems, security controls, and other technology infrastructure equipment/systems in production.
2. Systems/devices/applications/technologies that are transitioning to production.
3. Test environments, such as the enterprise web test infrastructure, that are used by the campus community for testing.
4. The Campus failover environment hosted at CSU, Sacramento.

3.0 RESPONSIBILITY

	Role (Title)	**Responsibility**
1	Change Requester	• Input the Change Request and identify systems that interface with confidential data.

		• Develop a test plan and test the change (where possible); • Prepare a back-out plan; • Remediate security vulnerability findings; • Obtain buy-off from key stakeholders/ system owners; • Attend weekly CMR meetings (where appropriate); • Implement the change and confirm successful; • Update/close the Change Request case.
2	Supervisor/Lead	• Review/approve unit changes to proceed to CMR meetings.
3	Application Developer/Database Programmer	• Conduct code reviews in accordance with campus development standards.
4	IT/Sr. Directors	• Approve emergency change requests; • Review/approve pre-approved changes; • Recommend changes to change blackout periods.
5	Information Security	• Conduct vulnerability scans; • Review change requests involving confidential data systems;
6	Change Management Review Team	• Review and approve non pre-approved changes; • Identify appropriate sequencing and timing for changes;
7	Sr. Dir. of Infrastructure Services/ ISO	• Approve change requests at weekly CMR meetings.
8	VP for IT/CIO, AVP for IT, or Sr. Dir. of IFS/ISO.	• Approve exceptions to the CMR processes;

4.0 DEFINITIONS

1. Change. See 2.0.
2. IT Change Management Dispatcher. Responsible for preparing change requests for discussion at the IT-led Change Management meetings.
3. Change Management Team. Identified the group of participants for the scheduled Change Management Request meetings. Participants include:

   a. Senior Director, Infrastructure Services & ISO

b. Senior Director, Information Systems

c. Director, Virtual Services and Systems

d. Director, Telecom and NOC

e. Director, User Support Services

f. Director, Business Consulting Services

g. Director, Identity Management

h. Director FTC Operations

i. Lead, Systems group

j. Lead, Network Operations Center

k. Lead, Information Security

l. Lead, Network

m. Lead, Web Services

n. IT Communications

4. IT-led Change Management Meetings (Time, day, and location)

   IT-led Change Management meetings are held to discuss non pre-approved change requests. Discussions include a review of change planning actions, risk/impact assessment, communication plans, and stakeholder review/approvals.

   a. Meeting Time. 9:00am

   b. Day. Wednesday (weekly)

   c. Location. Sequoia Hall 250A

5. Change Windows

   a. Designated days/weeks/hours where approved changes may be executed.

6. Change implementer. The person(s) responsible for:

   a. Planning the change,

b. Submitting the appropriate change control documentation by 2:00pm Tuesday,

c. Leading the implementation of the change,

d. Initiating the quality assurance process following the change, and

e. Documenting the completion of the change.

7. Change client or requestor. The individual responsible for requesting that a change take place.

8. Quality Assurance Team. The Campus staff members responsible for assuring that the change has been implemented correctly and that there is no negative impact on campus systems or services.

5.0 CLASSIFICATION OF CHANGES

Based on the definitions above, changes are classified into four categories—pre-approved, non pre-approved, out-of-band (includes Emergency Changes), and CMS.

a. Non Pre-Approved (Maintenance window: **Saturday 12:01am to 6:00am)**:

Tend to be higher risk changes that require an outage to a production system, or result in a user-visible feature/application change. Requires review by the Change Management Review team.

b. Pre-approved.

I. Incidental routine changes that follow pre-defined/well-practiced and approved processes/procedures with minimal chance of unexpected outcome, and minimal risk of impact and minimal impact in the event of unexpected outcome. Does not require an outage to a production system, and does not involve systems containing/interfacing with Level 1 data, as documented in the CSU Data Classification Standard, OR

II. Change to an individual user's mailbox, workstation, etc.

Examples of pre-approved changes:

I. Access Control List (ACL) changes and firewall rule updates (following documented ISO approval). Friday mornings, 8am-11am;

II. Internal DNS entry updates (as needed);

III. External DNS updates. Friday mornings, 8am-11am.

c. Out-of-Band Changes: Changes scheduled for execution outside of the normal maintenance window.

I. Emergency Changes are carried out as needed to respond to (or prevent) an outage event. **As needed**. Emergency changes do not require prior approval of the Change Management Team; however do require approval from the Sr. Director for the respective department, AVP for IT, or VP for IT/CIO (or Director if all are unavailable). Emergency changes require Root Cause Analysis review.

II. Other changes as needed.

d. Common Management System (CMS) Maintenance: Standard time for CMS-delivered changes. **Wednesday (weekly) 8:00pm to 11:59pm**

6.0 PROCESS DOCUMENTATION FOR CHANGES

All change-related documentation must be placed in the EBSuite tracking system.

6.1 PROCESS FLOW FOR NON PRE-APPROVED CHANGES

1. Identify scope of issue, systems and services involved. Recommend a course of action.
2. Determine the impact of making the change:
   a. Systems/services affected.
   b. Outages/duration associated with the change.
3. Develop action plan, test procedures and back out requirements.

4. Identify the stakeholders and if prior notification/involvement is required.
5. Determine if a code review is necessary (in accordance with campus development standards).
6. Complete vulnerability scan in coordination with the IS team, and remediate findings.
7. Change Initiator submits a completed EBSuite ticket for change to the Change Management Dispatcher.
8. CMR team reviews all Requests for Change,
9. Sr. Dir of IFS/ISO (or designee) approves/rejects the Change.
10. IT Communication prepares and implements a communication plan.
11. Change requester implements the change.
12. Quality Assurance Team performs testing as required to verify the proper application of the change, and reports the results of the testing to the Change Management Team, and ISO
13. Update and close CMR EBSuite ticket.

6.2 PROCESS FLOW FOR PRE-APPROVED CHANGE MANAGEMENT REQUEST

1. Pre-approved change lists are reviewed/approved annually by the IT Directors, and do not require weekly/review and approval of the Change Management Team, Information Security Officer, or VP for IT/CIO.
2. As needed, pre-approved changes are submitted and tracked via the campus case management system.
3. Pre-approved changes are executed in accordance with department-level processes and identified days/times for execution.

6.3 PROCESS FLOW FOR EMERGENCY CHANGES (ECMR)

1. Identify scope of critical problem, systems and services involved. Recommend a course of action.

2. Create an Emergency CMR ticket and assign it to IT CMR Dispatch

3. Review issue with Supervisor or Director and obtain approval to perform corrective actions.

4. Director sends notification out to IT leadership. Identify issue, options with pros/cons (including related risk and impact), and recommended course of action.

5. Develop action plan, test procedures and back out requirements.

6. Test, where possible, proposed emergency changes and confirm expected results.

7. Implement changes and closely monitor affected services.

   a) Changes are successfully implemented, issues are addressed.
      I. Director notifies IT leadership of successful completion of changes.
      II. RCA begins.

   b) Changes do not resolve issues.
      I. Execute back out procedure.
      II. Analyze reason for change failure.
      III. Revise action plan.
      IV. Return to step #5

8. Discuss issue in next scheduled RCA meeting.

9. Update and close ECMR EBSuite ticket.

6.4 CSU, Sacramento Failover Environment Changes

CSUN maintains a failover environment using CSU, Sacramento's virtual server and storage resources. The failover environment must remain inline with production system versions for equipment maintained in CSUN's data center environment. As such, the failover environment will be upgraded, patched, and otherwise "changed" the week prior to making the same changes to CSUN's production environment.

Changes made to the failover environment must be reviewed by the Change Management team, and can be completed during the Out-of-Band change window.

6.5 Changes to Confidential Systems

Confidential systems are server-based databases or applications that transact, store, or otherwise interface with confidential data such as Social Security Numbers (SSNs) or Medical/Heath data (see complete list on the CSUN IT Security web site - http://www.csun.edu/it/security/protecteddata.html) and require the following additional change review controls prior to change execution.

- IS team reviews each proposed change.
- IS team conducts vulnerability scan immediately (within reason) following the change.
- Where code is modified, a code review is completed in accordance with the Application Development Standard.

7.0 BLACKOUT/FREEZE PERIODS

Except as required to respond to or prevent a system outage or disruption in services, or for changes required to comply with business process changes for regulatory systems, no major changes will be performed during the following periods:

(1) Two weeks prior to the first instructional day of each semester (Spring and Fall) to two weeks following the first instructional day of each semester, **and**

(2) One week prior to the day that final exams commence until the weekend following instructor grading.

(3) Other dates identified as having critical campus events/activities, such as peak registration periods.

Note: Pre-approved changes are exempted from blackout/freeze periods.

7.0 REVIEW

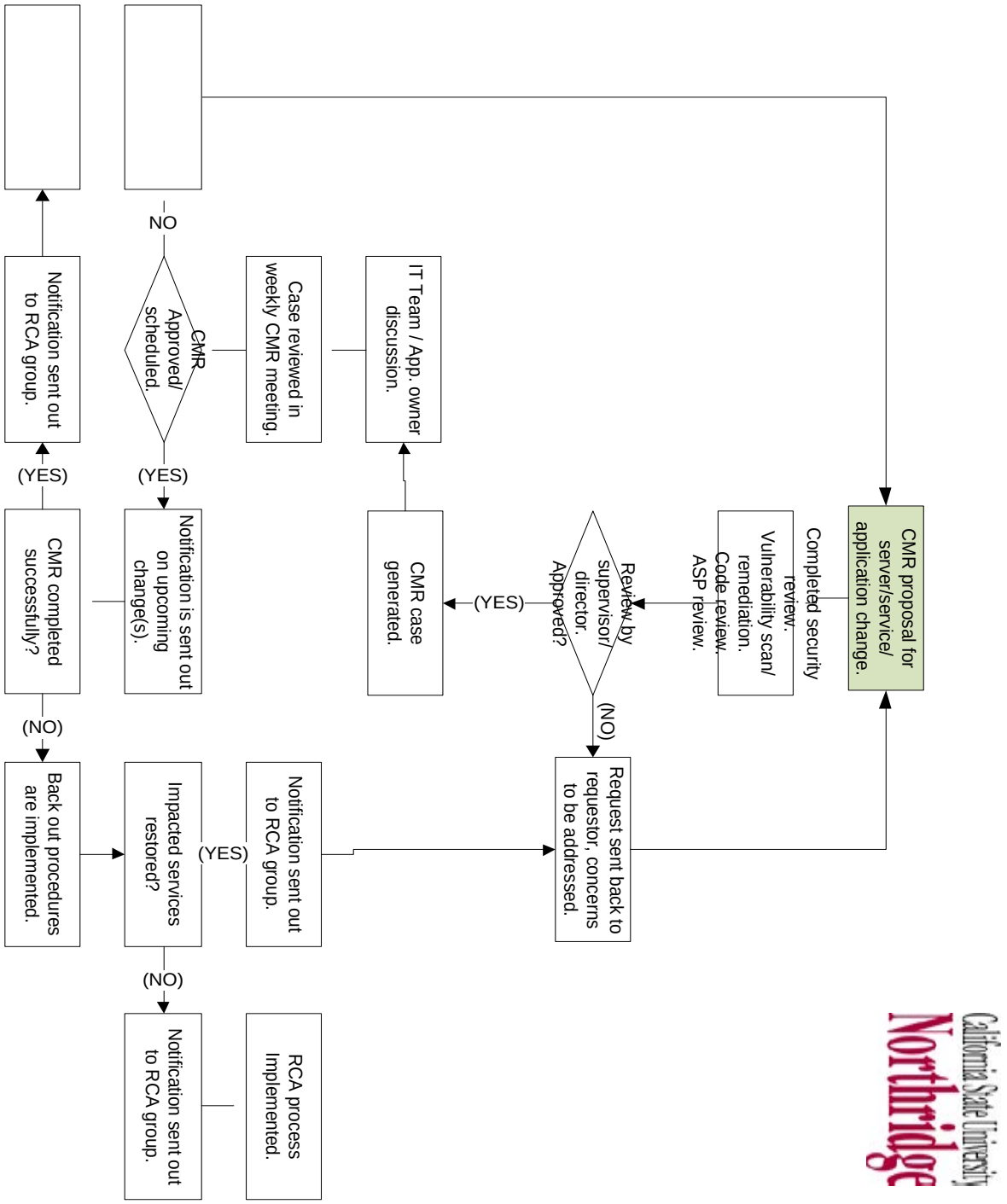
IT Directors will review the effectiveness of this business practice on an annual basis, and make adjustments as needed.

9.0 EXCEPTIONS

Exceptions to this procedure may be granted by the VP for IT/CIO, AVP for IT, or Sr. Dir. of IFS/ISO.

California State University Northridge	Information Technology Standard Operating Procedure CHANGE MANAGEMENT CONTROL	Page 9 of 10	
		SOP#: XXXX-90-09-0XX	Revision#: Version 0.X

10.0 CHANGE MANAGEMENT FLOW DIAGRAM



11.0 EMERGENCY CHANGE MANAGEMENT FLOWCHART