REG - 70.00.3 - ITS CHANGE MANAGEMENT REGULATION

Authority: Chancellor	Responsible Office: Information Technology Services

Number:	REG - 70.00.3 - ITS CHANGE MANAGEMENT REGULATION
History:	Effective Date: February 15, 2006, Reformatted/Updated: September 24, 2006; Revised: May 10, 2016
Related Policies/Sources:	
Contact Info:	Information Technology Services, 919-530-7423

1. Purpose
This document provides guidance regarding change management for NCCU ITS networks, systems and services. The change is defined as an alteration to software, hardware, or another aspect of the school's IT environment.

2. Regulation
Change Management helps organizations understand and work to minimize risks of changes to the IT environment. It assists in managing the people/communication and technical aspects to ensure that changes are planned, have been tested, have included key stakeholders, have back out plans, have a clear understanding of the impact, have appropriate communication strategy and have been approved prior to implementation.

3. Scope
3.1 These guidelines apply to all employees, contractors, consultants, temporaries, and other workers at NCCU, including those workers affiliated with third parties who require access to NCCU information systems at all locations.

3.2 The specific objectives of applying a change management system are to:

3.2.1 Minimize risks during change;
3.2.2 Provide a change communication process;
3.2.3 Reduce the number of emergency/urgent/unplanned changes by developing a calendar and schedule for maintenance/downtime; and
3.2.4 Ensure that proper change management steps occur with proper documentation, testing and signoffs.

3.3 Basic Procedures for Change Management

The basic procedures for change management include the following:

3.3.1 Rationale/plan
3.3.2 Test
3.3.3.Management Meeting
3.3.4.Review
3.3.5.Approval
3.3.6 Announcement
3.3.7.Implementation
3.3.8 Report and Control

3.4 Request for Change (RFC)

3.4.1 A change request can be the result of one of the following:

3.4.1.1 Problem management where an issue, or a series of related issues, is identified and a mitigating change is necessary to prevent (or minimize) future effects;
3.4.1.2 Results of a business decision that will require some modification (add, delete, change) to the supporting technology; and/or
3.4.1.3 Due to outside influences (i.e. governmental regulations or changes made by business partners).

3.4.2 **All changes must be linked to an incident/ticket or project NO change request should be submitted verbally unless it is an emergency (with written approval and documentation submitted after the fact).**

3.5 Documentation and Review of Change

3.5.1 Once a change request is in place, the change management team (CMT) must review the change request with as much information as possible in order to assess the requested change fully. The CMT consists of the IT Executive Leadership and others as needed (see page three). Its function is to review the change from a process and governance standpoint to assure that all foreseeable risks have been identified and mitigated, and that plans are in place for any problems that may arise.

3.5.2 Information that should be included in the change request that will be used to inform the decision:

3.5.2.1 Project/incident
3.5.2.2 Requested change
3.5.2.3 Priority
3.5.2.4 Requester
3.5.2.5 Technical Lead
3.5.2.6 Build, test, review dates
3.5.2.7 System/Application/Service affected
3.5.2.8 Type - Selects a type of change, which triggers an appropriate workflow. Out-of-box, these choices are:
3.5.2.8.1 Routine - low-impact, commonly performed the change.
3.5.2.8.2 Comprehensive - high impact change with a more complex procedure.
3.5.2.8.3 Urgent – can’t wait for weekly meeting
3.5.2.8.4 Emergency - high impact change, created in response to a critical situation.
3.5.2.8.5 Risk – what is the risk if the change isn’t done and to making the change.

3.5.3.8.6 Impact – what is the campus impact of making or not making the change; who are the affected customers of the change as well as the impact of any system/service outage.
3.5.3.8.7 Affected systems/dependencies –what other systems/dependencies will be impacted as a result of this change.
3.5.3.8.8 Communication strategy – if needed for large impact changes
3.5.3.8.9 Schedule - Includes a requested by date, a planned start and end time, and work start and end dates. This includes any post implementation testing needed by the end users across campus
3.5.3.8.10 Testing sign off for pre and post implementation by all affected parties
3.5.3.8.11Back out Plan – what is the plan to return to the previous state

3.5.2.9 Additional information as needed/requested

3.6 Updating/Closing an RFC

Once a Change has been approved, the requestor/technical lead is responsible for updating the RFC.

3.6.1 **Roles and Responsibilities**

3.6.1.1 Requester

The individual requesting the change is responsible for:
3.6.1.1.2 ensuring that the appropriate testing has been completed and signed off
3.6.1.1.3 verifying to ITS that the key stakeholders have been informed and also signed off on the request
3.6.1.1.4 identifying the existing project or ticket connected to the change request
3.3.1.1.5 working with ITS on an appropriate back out a strategy
3.3.1.1.6 certifying once the change is complete that the change was successful and if not work with ITS on remediation/back out

3.6.1.2 Technical Contact(s)

These individuals (both in ITS and functional areas) are responsible for:

3.6.1.2.1 coordinating alone with the requester to complete request documentation
3.6.1.2.2 understanding the impact of the change
3.6.1.2.3 ensuring that key stakeholder has been informed and in agreement
3.6.1.2.4 ensuring that the necessary ITS resources are available on requested implementation date

3.6.1.3 Work Groups

Work Groups are responsible for implementing changes assigned to them once the change has been approved. The work group may be similar to the Technical Contact(s) and has the same responsibilities.

3.6.1.4 Change Management Team

The Change Management Team consists of the following people:

3.6.1.1 Chief Information Officer (or designee),
3.6.1.2 Director of Networks and Systems
3.6.1.3 Director of Enterprise Information Systems,
3.6.1.4 Director of Audit Compliance and Business Continuity,
3.6.1.5 Director of Client Services

3.6.1.6 Director Classroom Computer and Events
3.6.1.7 Director Web Services
3.6.1.8 Other ITS or Campus Department Representative(s) as needed.

3.6.2 **Governance of Change Management**

3.6.2.1 Change Management Team

The Change Management Team will review each request based on the criteria listed above and approve requested a change and schedule or ask the technical lead to gather more information from the requester.

3.6.2.2 Enterprise Systems Council (ESC)

This council is responsible for assisting ITS in determining scheduled maintenance windows and planning for major upgrades. The coordination of these upgrades is critical to maintaining quality service to the campus.

3.6.2.3 Change Management Meetings

3.6.2.3.1 These meetings can be held weekly or as needed. A member of the ESC will be invited to a change management meeting as necessary. The purpose of the meeting is to:

3.6.2.3.1.1 Bring all required parties together to assess the feasibility of implementing the change and provide status.
3.6.2.3.2.1 To review the status of all open changes, schedule for the current and upcoming weeks.
3.6.2.3.3.1 Discuss high impact changes.
3.6.2.3.4.1 Approve or disapprove each change as well as the Change Schedule.

3.6.2.3.2 Meeting Attendees

3.6.2.3.2.1 Change Management Team members
3.6.2.3.2.2 Other Department Representative(s) as needed

3.6.2.4 Approving the Change

A majority of the CMT must be present and approve a change for the request to move forward. Otherwise, the change will be held until such time as a majority has met and approved. Any member of the CMT can hold a change if a significant concern is made. The technical contact will be notified to gather additional information to address any concerns.

3.6.2.5 Monthly Report

The monthly report consists of charts showing the number of changes submitted during the month by category (i.e. high, medium and low risk), the number of problems caused by changes and the process measurements for the month.

3.6.2.6 Additional Meetings

Post-mortems will be convened on an "as needed" basis. It will be held for changes resulting in significant problems to determine what, if anything went wrong and how any such problems can be

prevented in the future.

3.6.2.7 Campus Communications

If the change has a broad impact, communications will go out to the entire campus and/or appropriate parties by email and/or web posting. Communications will be coordinated through the CMT and project/technical leads.

4. **Rule Enforcement**
This requested changes will always go into effect with 24 hours when seen fit for security reasons. Any or all person(s) or department(s) who will be effected by the change will receive an emergency email from "security@nccu.edu." If there are reasons for changes or updates, but there are no immediate risks, a minimum of 7 days will be provided before the change management will go into effect after the announcement of the changes are made.