# RUL - 70.00.5 - SERVER CONFIGURATION MANAGEMENT RULE

| Authority: Information Technology | Responsible Office: Information Technology Services |
|---|---|

| | |
|---|---|
| Number: | RUL - 70.00.5 - SERVER CONFIGURATION MANAGEMENT RULE |
| History: | Reformatted/Updated: March 28,2016; Revised: May 10, 2016 |
| Related Policies/Sources: | ITS Change Management Rule, |
| Contact Info: | Information Technology Services, 919-530-7423 |

## 1. Purpose

The purpose of this rule is to establish management direction and high-level objectives for server change management and control. This rule will ensure the implementation of server configuration change management and control strategies to mitigate associated risks such as:

1.1. Minimize risks during change
1.2. Provide a change communication process
1.3. Reduce the number of emergency/urgent/unplanned changes by developing a calendar and schedule for maintenance/downtime
1.4. Ensure that proper change management steps occur with proper documentation, testing and signoffs
1.5. OSSEC Change Management Software is in place to track any changes to server configurations.

## 2. Rule

A Request for Change (RFC) must be submitted and approved with all the corresponding information needed. The guidelines for RFCs are outlined in the ITS Change Management rule. Information that should be included to inform a decision:

2.1. Project/incident Requested change
2.2. Priority

2.3. Requester and Technical Lead
2.4. Build, test, review dates
2.5. System/Application/Service affected
2.6. Type - Selects a type of change, which triggers an appropriate workflow. Out-of-box, these choices are:
2.6.1. Routine - low-impact, commonly performed change
2.6.2. Comprehensive - high impact change with a more complex procedure.
2.6.3. Urgent – can't wait for the weekly meeting. Emergency - high impact change, created in response to a critical situation.
2.7. Risk – what is the risk if the change isn't done and to making the change
2.8. 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. Affected systems/dependencies –what other systems/dependencies will be impacted as a result of this change.
2.9. Communication strategy – define the type of communication and to whom if needed for large impact changes.
2.10. 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.
2.11. Testing sign off for pre and post implementation by all affected parties.
2.12. Back out Plan – what is the plan to return to the previous state?
2.13. Provide additional information as needed or requested.

## 3. Scope

This rule provides guidance regarding change management for NCCU ITS servers, and services. For the purposes of this rule, change is defined as an alteration to software, hardware, or another aspect of the NCCU IT environment. This rule applies to all employees, contractors, consultants, temporary employees, and other individuals who may perform work at NCCU, including those workers affiliated with third parties who require access to NCCU Information Systems at all locations.

## 4. Rule Enforcement

A record or series of records which allows the processing carried out by a computer system to be accurately identified, as well as verifying the authenticity of such amendments. Systems changes will be monitored and recorded by OSSEC Change management server.