

## Change Management

**Policy:** IT-INT 2.1  
**Issuing Office:** VP/CIO-CCIT  
**Responsible Officer:** DIR/CSO  
**Responsible Office:** OISP

---

### Executive Summary

The Clemson Computing & Information Technology (IT) infrastructure at Clemson University is expanding and continuously becoming more complex. There are more people dependent upon the network, more client machines, upgraded and expanded administrative systems, and more application programs. As the interdependency within the IT infrastructures grows, the need for a strong change management process is essential.

From time to time IT elements require an outage for planned upgrades, maintenance or fine-tuning. Additionally, unplanned outages may occur that could result in upgrades or maintenance. Managing these changes is a critical part of providing a robust and valuable IT infrastructure

Change Management is a process, which by its lack of maturity can have the most dramatic impact on the business. Unapproved, unplanned, and uncoordinated changes can impact the business customer on a frequent basis. Additionally, without the ability to control when, how and by whom things are changed in the production environment, other processes such as Release and Configuration Management cannot be effectively implemented. A controlled Change Management process is a dependency for several other IT business practices.

### Purpose

The purpose of the Change Management Policy is to manage changes in a rational and predictable manner so that staff and customers can plan accordingly. Changes require serious forethought, careful monitoring, and follow-up evaluation to reduce negative impact to the user community and to increase the value of IT resources and their resultant services.

### Policy

#### **Policy Coverage:**

The Clemson Computing & Information Technology Change Management Policy applies to all individuals that install, operate or maintain IT resources and services.

## **Change Management:**

- Every change to a Clemson Computing & Information Technology resource such as: operating systems, computing hardware, networks, databases and applications are subject to this Change Management Policy and must follow the Change Management Procedures.
- All changes affecting computing environmental facilities (e.g., air-conditioning, water, heat, plumbing, electricity, and alarms) must be reported to or coordinated with the leader of the Change Management process.
- A Change Management Change Advisory Board (CAB), appointed by CCIT leadership, will meet regularly to review change requests and to ensure that change reviews and communications are being satisfactorily performed.
- A Change Advisory Board/Emergency Committee will be established comprised of a subset of the CAB and responsible for assessing and approving urgent changes as a result of a system or service incident.
- A Change Management Governance Board (CMGB) comprised of CCIT leadership, will be convened to approve any change which will result in an interruption of a critical service or for which a scheduled implementation cannot be reached. The CMGB will be convened on the recommendation of the CCIT Change Manager.
- A formal written change request must be submitted for all changes, both scheduled and unscheduled.
- All scheduled change requests must be submitted in accordance with change management procedures so the Change Advisory Board has time to review the request, determine and review potential failures, and make the decision to allow or delay the request.
- Each scheduled change request must receive formal Change Advisory Board approval before proceeding with the change. The only exception to this will be those changes receiving pre-approved status or those changes that have been delegated, such as password changes.
- Emergency changes require CCIT Change Manager and Computing, Systems and Operations Director of Operations approval prior to implementation. Any emergency change affecting those services deemed “critical” will be communicated to the CMG/EB or CMGB as required.
- The CCIT Change Manager may deny a scheduled or unscheduled change for reasons including, but not limited to, inadequate planning, inadequate backout plans, the timing of the change will negatively impact a key business process such as year end accounting, or if adequate resources cannot be readily available. Adequate resources may be a problem on weekends, holidays, or during special events.
- Customer notification must be completed for each scheduled or unscheduled change following the steps contained within the Change Management Procedures.
- A Change After Action Report (AAR) must be completed for each change, whether scheduled or unscheduled, and whether successful or not.
- All information systems, services and processes must comply with the change management process that meets the standards outlined above.
- Other equipment or facilities that may affect the production environment are also subject to compliance with the change management process.

## **Disciplinary Actions**

Violation of this policy may result in disciplinary action which may include termination for employees and temporaries; a termination of employment relations in the case of contractors or consultants; dismissal for interns and volunteers; or suspension or expulsion in the case of a student.

## **Definitions**

*Change Management.* The practices of ensuring all changes to Configuration Items are carried out in a planned and authorized manner. This includes ensuring that there is a business reason behind each change, identifying the specific Configuration Items and IT Services affected by the change, planning the change, testing the change, and having a backout plan should the change result in an unexpected state of the Configuration Item.

*Change Advisory Board (CAB).* A CAB is an integral part of a defined change management process designed to balance the need for change with the need to minimize inherent risks. A CAB is comprised of representatives of the key functional areas of CCIT, customer representatives, security office, service desk and Service Management staff. The CAB is responsible for oversight of all changes in the production environment. Plus the changes may involve hardware, software, configuration settings, patches, etc.

*Change Advisory Board/Emergency Committee.* The CAB/EC is a subset of the full CAB responsible for assessing and approving urgent changes as a result of a system or service Incident.

*Change Management Governance Board (CMGB).* The CMGB is comprised of the executive leadership of CCIT and the Change Manager. The CMGB is responsible for assessing and approving emergency changes as a result of a system or service Incident. The CMDB may be convened by the CCIT Change Manager in those situations interruptions of Clemson University's critical services. Additionally, the CMGB may be called upon to rule on scheduling issues that cannot be resolved by the normal CAB and CCIT Change Manager.

## **Related Documents**

Change Management Standard Operating Procedures

[http://ccit.clemson.edu/departments/CSO/Operations/chg\\_mgmt/SOP.pdf](http://ccit.clemson.edu/departments/CSO/Operations/chg_mgmt/SOP.pdf)

## **Revisions**

Current: 1.0

Next Revision: June 8, 2008

Administrative Update:

## **Approvals**

Approved, CCIT Executive Staff  
June 8<sup>th</sup>, 2007

