THE UNIVERSITY OF ALABAMA IN HUNTSVILLE

OIT CHANGE MANAGEMENT COMMITTEE

-INTERIM-

Number 02.01.36

Division Office of Information Technology (OIT)

Date August 2015

Purpose The purpose of this policy is to state the procedures that must be followed to ensure information technology resources are protected against undocumented changes.

Policy This policy establishes the procedures required to ensure protection of IT resources against undocumented changes as well as to ensure coordination with other activities in the university. For purposes of this policy, a change is defined as anything that transforms, alters, or modifies the operating environment or standard operating procedures. This policy establishes the process for managing these changes to hardware, software, and firmware.

This document describes the process by which changes are requested, reviewed, approved, communicated, tested, logged, and implemented. The overriding goal is to provide a high level of availability and service to our customers.

Procedure

1.0 Audience

This policy applies to Office of Information Technology (OIT) personnel who install, operate, or maintain information technology upon which any unit of The University of Alabama in Huntsville (UAH) relies on to conduct business and/or achieve the mission of the university. The university community also needs to be aware and informed of this policy because it may want or need to request a change, approve, test, etc. IT resources and, thus, are thereby subject to following the prescribed process.

2.0 Scope

This policy covers changes to OIT-supported systems (hardware, software, applications, and network environment) upon which any functional unit of the university relies in order to perform its normal business activities. Examples of these systems include, but are not limited to: enterprise resource planning systems, databases, authentication systems, servers, learning management systems, network switches, routers, firewalls, wireless solutions, intrusion detection systems, system management software, web servers, and any other user facing services. Changes not covered by this policy are changes that affect only an individual. Examples of changes not covered under the scope of this policy include, but are not limited to, changes to an employee's desktop or laptop computer, allocation of IP addresses, etc.

Changes may be required for many reasons, including:

- User requests
- Vendor recommended/required changes
- Changes in regulations
- Hardware and/or software upgrades
- Acquisition/implementation of new hardware or software
- Hardware or software failures
- Changes or modifications to the infrastructure
- Environmental changes (electrical, air conditioning, data center remodels, etc.)
- Unforeseen events
- Periodic maintenance

3.0 Process

3.1. Formal Change Request

All requests for planned change will be documented by creating a new change request. The change request will be completed by the change requestor (OIT staff). The change should be approved by the OIT director, or directors, that are in charge of the impacted systems before entering the change request.

3.2. Change Analysis and Justification

The change requestor will work to develop a specific justification for the change and identify the impact on infrastructure, business

operations and budget, identify business as well as technical risks, develop technical requirements, and review specific implementation steps.

3.3. Change Approval and Scheduling

The Change Management Committee shall consist of:

- Chief Information Officer
- Director of Academic Technology & Client Services
- Director of Enterprise Applications & Identity and Access Management
- Director of Networks & Infrastructure
- Chief Information Security Officer

This committee will assess the urgency and impact of the change on the infrastructure, end user productivity and budget. This committee will serve to evaluate business impact, scheduling conflicts and user inconvenience of all changes and approve, or disapprove, the change.

3.4. Change Implementation

Once the change, and timing, is approved by the Change Management Committee, the change requestor should complete the change as approved in a manner that will minimize impact on the infrastructure and end users. In the event that the change does not perform as expected or causes issues to one or more areas of the production environment, the committee will determine if the change should be removed and the production environment returned to its prior stable state.

3.5. Change Review

The Change Management Committee will ensure formally the change has achieved the desired goals and will conduct a review. Post-implementation actions may include acceptance, modification, or backing-out of the change. The committee formally documents the final disposition of the change as part of the Change Request.

3.6. Change Documentation

To maintain a consistent record of changes, the following will be recorded:

- Proposal date
- Proposal unit and person performing change
- Proposed change date and time
- Change details
- Change back out plan
- Expected outage length
- If the change:
    - is business or operational change
    - is new or discontinued service
    - is security or OS patches, hotfixes
    - is scheduled maintenance
    - impacts DR or COOP
    - should be communicated externally
    - requires documentation updates to the help desk
    - is approved
    - affects the data center
    - is an emergency change
- Completion date of the change

4.0 Change Categories

This policy categorizes change as: Planned Major; Maintenance and Minor; and Emergency and Unplanned Outage. Of the three change categories, Planned Major Change requires the most rigorous and extensive change process and subsequent procedures.

4.1 Planned Major Change

Examples of planned major change are:

- Change that results in business interruption during regular business hours
- Change that results in academic interruption within a term
- Change that results in business or operational practice change
- Changes in any system that affect disaster recovery or business continuity
- Introduction or discontinuance of a new information technology service

4.2 Maintenance and Minor Changes

Examples of this type of change are:

- Application-based security or business needs patches
- Operating system patches (critical, hotfixes, and service packs)
- Regularly scheduled maintenance
- Changes that are not likely to cause a service outage

4.3 Emergency and Unplanned Outage Changes

Examples of this type of change are:

- Building is without service
- A severe degradation of service needing immediate action
- A system/application/component failure causing a negative impact on business operations
- A response to a natural disaster
- A response to an emergency business need
- A change requested by emergency responder personnel

5.0 Emergency Change Process

The manager/director will make decisions about high impact emergency changes. These types of emergency changes are authorized only to repair IT service errors that are severely impacting the business, when a situation has occurred that requires an immediate action that cannot wait until the normal advertised window to either restore service or prevent a significant outage.

The emergency change process differs from the normal change process in that:

- Approval is granted, and documented via e-mail in advance of the change by authorized manager/directors. If the appropriate manager/director is unavailable, then the CIO should be contacted for approval in advance of the change. If the CIO is unavailable, the change should still be documented via e-mail. In the rare event that e-mail service is down/unavailable, the change should be

documented in writing, and signed by the authorized manager/director.
- Testing may be reduced or even eliminated in extreme situations.
- Updating of the necessary change request may be deferred until normal business hours.

Emergency changes require:

- Technical change review and approval in writing, usually by the manager or director of the department making the change.
- If it is not possible to notify the Director of Academic Technology & Client Services and the Help Desk Coordinator of the emergency change in advance of the change, they should be notified as soon as possible after the change.
- Notification of the change to Change Management committee as soon as possible after the change.
- Submission of a Change Request within one business day after the issue has been resolved.
- Change Management committee review of the emergency change at the next Change Management meeting.

Sanctions:

- Emergency change procedures should be considered the exception rather than the norm. Failure to comply with emergency change procedures is considered a serious breach of risk management practices and may result in disciplinary action including dismissal.

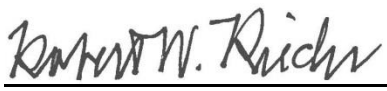
6.0 Compliance with Policy

Failure to abide by this policy may result in the loss or suspension of IT privileges, claims for reimbursement of damages, disciplinary action, and/or referral to appropriate state/federal law enforcement authorities.

Violations that constitute a breach of the Student Conduct Code, the Faculty Handbook, or the Staff Handbook will be referred to appropriate authorities. OIT personnel may take immediate action as needed to abate ongoing interference with system or network operations or to ensure integrity of university systems or data.

Review The UAH Cybersecurity and Policy Advisory Council is responsible for the review of this policy every three years (or whenever circumstances require).

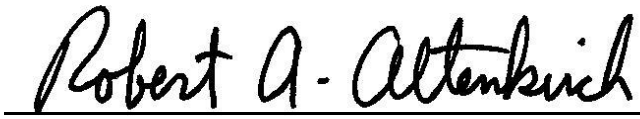
Approval



Chief University Counsel

Provost and Executive Vice President for Academic Affairs

APPROVED:



President