Change Management Policy

Section 1. PURPOSE AND SCOPE

The purpose of change management is to ensure that standardized methods and procedures are used to alter the production environment, minimizing negative impact to services and customers and ensure audit compliance. The specific objectives of applying a change management system are to:

- Implement changes on a schedule when possible
- Establish and publish a calendar that specifies the "maintenance window" and the timing requirements of systems changes
- Eliminate or reduce the number of changes that are regressed due to issues without change planning, testing and implementation
- Provide a back out plan for all changes
- Ensure change requests comply with Clark change management procedures
- Ensure implemented changes comply with Clark baseline standards

This document describes the policies that guide change requests, reviews and approvals, as well as how changes are tested, communicated, logged, and implemented. 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 changes to hardware, software and firmware. This policy is to ensure information resources are protected against undocumented changes as well as ensure coordination with other activities in the university. Every change to covered Clark ITS information resource such as operating systems, computing hardware, network, system and application software, and contracted information resource services, are subject to this Change Management Policy and must follow the documented IT Change Management Process.

This policy applies to mission critical, ITS-supported production systems (hardware, software, applications, network) upon which a functional unit of the university relies upon to perform its normal business activities (consult with the Director of Enterprise Applications for most current list of systems covered by the scope of this policy). Changes made to individualized services (i.e., desktops/laptops), lower priority systems, non-Clark serviced and SaaS systems, and non-production IT services - such as systems that are in development or testing environments - are outside the scope of this policy at this time.

Section 2. PROCEDURES AND ENFORCEMENT

The Vice President for Information Technology is charged with the responsibility to periodically review the policy and propose changes as needed. Failure to adhere to the provisions of this policy statement may result in loss of Clark University access

privileges; disciplinary action up to and including termination; or civil/criminal prosecution.

Section 3. ENTITIES AFFECTED BY THIS POLICY

This policy applies to any individual responsible for the management, operation, and/or maintenance of Clark administrative and academic systems. This includes:

- ITS Division employees who install, operate, and/or maintain IT assets upon which Clark University relies on to conduct the business of the University.
- Non-ITS employees (i.e., typically functional business owners) who share responsibility for the assessment, testing, and application of patches, upgrades, and modifications that impact systems under their management/supervision.

Clark employees, vendors, contractors, partners, students, collaborators and any others doing business or research with Clark are also subject to the provisions of this policy since they may have occasion to request/approve a change or test an upgrade/patch, and are thereby subject to following the prescribed process.

Section 4. EXCEPTIONS

In the case where a patch/upgrade or other update is found to be non-compatible with an application or the environment, appropriate measures will be taken to minimize the risk. In addition, if a mission critical service is determined to be in immediate jeopardy or already disabled, no prior notice will be necessary to fix the environment. Once service has been restored, communication and documentation will be provided. There are times when change must be made outside the maintenance windows for business reasons. Upgrades, patches, or other updates and other changes can be made outside the published maintenance window as long as it is agreed upon by both ITS and the business ahead of time.

Related Policies and Regulations

Change Management Process

Change Management Form (Login Required)

Standards for the Protection of Personal Information of Residents of the Commonwealth (201 CMR 17.00)

History/Revision Information

Responsible Office/ Division: ITS

Effective Date: October 22, 2014
Last Amended Date: July 23, 2015
Next Review Date: July 23, 2023