OVERVIEW
With an ever-evolving Information Technology (IT) environment, frequent change to applications, systems, and to the overall infrastructure has become commonplace. Change can offer several advantages such as increased performance, functionality, security, or reliability; however, changes made to an information system can also have a significant impact on the functionality, usability, and security of the environment and surrounding systems. Therefore, it is essential to document, assess, and evaluate the possible effects that each change may present prior to implementation.

To minimize the impact that change related incidents may have on the confidentiality, integrity, and availability of information within the university, a structured approach to change is needed. Management of changes is critical to providing a robust and valuable Information Technology infrastructure and addresses the need for ensuring that standardized methods and procedures are used for the efficient and prompt handling of all changes.

The goal of a successful Change Management process is to reduce the amount of unplanned work, a.k.a. firefighting, as a percentage of total work done.

Purpose
The purpose of the Change Management Best Practice is to provide guidance on managing changes in a rational and predictable manner so that staff and clients 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.

Definitions
Information Systems: any and all computer printouts, online display devices, magnetic storage media, and all computer-related activities involving any device capable of receiving email, browsing Web sites, or otherwise capable of receiving, storing, managing, or transmitting electronic data including, but not limited to, mainframes, servers, personal computers, notebook computers, hand-held computers, personal digital assistant (PDA), pagers, distributed processing systems, network attached and computer controlled medical and laboratory equipment (i.e. embedded technology), telecommunication resources, network environments, telephones, fax machines, printers and service bureaus. Additionally, it is the procedures, equipment, facilities, software, and data that are designed, built, operated, and maintained to create, collect, record, process, store, retrieve, display, and transmit information.

Change Management: The process of controlling modifications to hardware, software, firmware, and documentation to ensure that Information Resources are
protected against improper modification before, during, and after system implementation.

**Change:**

- Any implementation of new functionality
- Any interruption of service
- Any repair of existing functionality
- Any removal of existing functionality

**Emergency Change:** When an unplanned immediate response to imminent critical system failure is needed to prevent widespread service disruption.

**Information and System Classification**

University faculty, staff, students, and others have a business need to collect, transmit, store, or process information. Protecting the confidentiality, integrity, and availability of this information is the responsibility of the entire university.

The *Information Classification Policy (IT0115)* and *Computer System Classification Policy (IT0116)* formalize this responsibility, define a framework for categorizing information and computer systems according to the perceived risk to the university, and provide a methodology for implementing these practices. Refer to those policies for definitions of ownership, responsibilities, system classifications, and information classifications mentioned hereafter.

University policies mentioned in this document can be found from the *University of Tennessee System Policy Search Page* at “http://www.tennessee.edu/policy/”. Best practice documents are referenced from the *Information Security Office home page* at “http://security.tennessee.edu/”.

**Scope**

This best practice shall apply to all Information Systems classified as Critical or Highly Critical, those systems holding Confidential Information, and to those networks, devices, applications, databases, any non-production system that contains Confidential Information, or any service the disruption of which would adversely affect the mission of the University. The principles of minimizing unplanned downtime and protecting the integrity of University information systems are pivotal in properly applying this Best Practice within each organization.

Items that would be considered out-of-scope for this best practice are:

- Changes to non-production systems
- Password resets
- User adds/deletes
- User modifications
- Machine reboots when no configuration change has occurred
• Other routine maintenance tasks which do not cause a system configuration change

**Compliance**

Any non-compliance with the university’s Information Technology Security Strategy, policies, or best practices must be reported to the ISO. Non-compliance can result in immediate withdrawal or suspension of system and network privileges and/or disciplinary action. Reference the *Information Technology Acceptable Use of Information Technology Resources Policy (IT0110)* for information concerning non-compliance issues.

**Exceptions**

Compliance with the university’s Information Technology Security Strategy, policies, and best practices are mandatory. In some instances, exceptions to policies and best practices must be made due to extenuating circumstances. Such exceptions must be documented and approved prior to implementation. The process for reviewing and approving/disapproving requests for exceptions can be found at [http://security.tennessee.edu/](http://security.tennessee.edu/).
CHANGE MANAGEMENT GUIDELINES

Policy and Procedures
Each organization must develop a formal, documented, change management policy and procedure that:

- Defines all roles and responsibilities related to change management
- Are consistent with all applicable laws, policies, regulations, standards, and Best Practices (for example, HIPAA, FERPA, PCI-DSS, GLBA, and State or Federal Laws)
- Documents approval by senior IT management, IT Director(s), and the appropriate business manager(s)
- Establishes and defines a suitable maintenance downtime window during which planned outages can be expected for system changes to be made

Change management policies and procedures must be integrated with and communicated to both IT and business management functions. These policies and procedures must be reviewed periodically by IT and business management to ensure suitability and completeness.

Baseline Configuration
Each organization should develop, document, and maintain a current baseline configuration for each information system. This baseline configuration provides a fallback position if a system is compromised to the point of being unusable and must be rebuilt from scratch.

- The baseline configuration provides information about a particular component’s makeup (for example, the standard hardware and software load for a server or workstation including updated patch information) and the component’s logical placement within the environment.
- The baseline configuration also provides the organization with a well-defined and documented specification to which the information system is built and any deviations, if required, are documented.
- Each organization must establish, document, and enforce mandatory configuration settings for information systems and their components.
- Each organization must employ procedures or automated mechanisms to centrally manage, apply, and verify the established configuration settings.

Change Management Procedures
Each organization must authorize, document, and control all changes to information systems using an organizationally approved process (for example, a chartered Change Control Board). This process should include representation from all appropriate entities affected by system changes.

- A written memorandum of understanding should be arranged between the IT organization and appropriate building service providers. This document should detail a notification system so that the IT organization
will be informed of any changes affecting computing environmental systems (e.g. air conditioning, heat, electricity, alarms, fire suppression, etc.) in time to take proper precautions and minimize potential downtime.

- The organization must employ procedures or automated mechanisms to:
  o Document a proposed change request to an information system
  o Notify appropriate approval authorities
  o Highlight approvals that have not been received in a timely manner
  o Inhibit change until necessary approvals are received
  o Execute changes efficiently and within a documented change management maintenance window
  o Document completed changes to the information system
  o Update the baseline configuration information for the changed system

- A change request must be submitted for all changes, both scheduled and unscheduled, in a timely manner to allow for review and approval or denial of the change request, and should include, but is not limited to:
  o Justification
  o Contact information of the proposed change owner
  o Identification of the benefits, deliverables, and risks of the change
  o Risk analysis, a plan to reduce identified risks, and a plan to roll back changes in the event of failure
  o Regulatory compliance benefits or issues
  o Identification of the systems and people who may be impacted by the proposed change
  o Budgetary cost estimate of the change
  o Test plan and evaluation method
  o Implementation specifications
  o Process for indicating the success or failure of the proposed change

- A Change Management Log must be maintained to generate, retain, and review a record of all changes. The log must contain, but is not limited to:
  o Date of submission
  o Nature of the change
  o Identification of the business owner
  o Date of change completion
  o Name of technician who completed the change
  o Indication of success or failure

- All changes must be communicated to all those who can and will be affected by the proposed change.

- The organization must include a procedure to address emergency change requests.
  o Emergency requests should be handled in a similar manner to standard requests, with differences to allow for expedited testing, evaluation, and implementation.
  o All emergency requests must be thoroughly tested to ensure quality without adding additional disturbances to the information system.
  o Emergencies should be clearly defined and exist only as a result of:
- A Critical or Highly Critical system that is completely out of service
- Severe degradation of a Critical or Highly Critical service needing immediate action
- A response to a natural disaster, or a response to an emergency business need

**Monitoring Configuration Changes**
Each organization must monitor changes to the information system and conduct a security impact analysis to determine the effects of the changes.
- Prior to change implementation, and as part of the change approval process, the organization must analyze changes to the information system for potential security impacts.
- After the information system is changed (including upgrades and modifications), the organization must check the security features to verify that the features are still functioning properly and perform vulnerability scans of the modified system.

The organization must audit activities associated with configuration changes for each information system.

**Access Restrictions for Change**
- Each organization must approve individual access privileges and enforce physical and logical access restrictions associated with changes to the information system in keeping with the Principle of Least Privilege.
- Only qualified and authorized individuals can obtain access to information system components for the purpose of initiating changes, including upgrades, and modifications.
- Roles and responsibilities defined in the Change Management Policies and Procedures are designated to qualified personnel, communicated to the organization, and enforced throughout the change management process.
- Each organization must employ an automated mechanism to enforce access restrictions and support auditing of the enforcement actions.