A. Purpose

Virginia State University (VSU) management in an effort to preserve the integrity and stability of its systems and infrastructure has established a change management policy that will govern the change control/configuration management process. Change Management is the process of communicating, coordinating, scheduling, and monitoring changes to the university's information technology environment. This process was developed and aligned with guidance from the Commonwealth's IT Security Standards, Information Technology Infrastructure Library (ITIL), and industry best practice.

B. Scope

The Change Management process includes all systems used by Virginia State University to perform its duties and responsibilities. These systems include hosted and non-hosted systems as the university recognizes its responsibility in ensuring the integrity and stability of the all systems that support the goals and mission of the university regardless of its direct or indirect oversight authority.

C. Authority, Responsibility, and Duties

The roles and responsibilities were established to ensure the integrity of the change control process; therefore, the following defines the roles and responsibilities that govern this process:

1. **Business Owner, System Owner and Data Center Manager** - The initiation of all changes must come from an authorized source. The business/system owner of the given system or the Data Center Manager (when general maintenance is required) are the authorized individuals and source of all changes.

2. **Change Management Administrator (CMA)** – The CMA is responsible for ensuring that change control activity from initiation to close is appropriately documented and acts as the gatekeeper to ensure that only authorized changes are forwarded to the IT Change Advisory Board (CAB). (In essence, the CMA acts as the compliance expert ensuring that the approval/sign-off at the different phases of the process have been completed according to policy.)

3. **IT Change Advisory Board (CAB) –** The CAB is responsible for change approval/denial, placing change in closed status and ensuring that each change has the following: appropriate priority/schedule, implementation plan approval, test/validation sign-off, implementation of rollback plan/criteria, and post implementation lessons learned discussion

4. **Data Center Manager** – is responsible for implementation of the change plan approved by the CAB. Changes will be tested in development/test environments prior to moving changes to the production environment. The Data Center Manager ensures that changes are approved by the Business and System Owners prior to placement in production.

5. **System Users** – The system users are responsible for testing changes prior to change implementation and also perform post implementation review once the change has

been implemented into the production environment to ensure the integrity of the system and that its data has not been compromised by changes implemented.

6. **Project Manager** – The Project Manager will ensure plans are developed and executed accordingly and in compliance with Commonwealth Project Management Standards.

D. Definitions

The IT security definitions and terms can be found in the Commonwealth of Virginia (COV) Information Technology Resource Management (ITRM) Glossary. It is referenced on the ITRM Policies, Standards, and Guidelines web page on www.vita.virginia.gov/library.

E. Policy Statement

This policy applies to all University employees (permanent, temporary, contractual, faculty, administrators, and students) who are responsible for the development, coordination, and execution of the University's change control process.

F. Guiding Principles

The following principles guide the development and implementation of the VSU Information Change/Configuration Management Process.

1. The VSU Change/Configuration Management Process is and shall continue to be designed to:
   a. Ensure integrity and stability of VSU systems and IT environments;
   b. Protect against any anticipated threats or hazards to the security or integrity of the information;
   c. Protect against unauthorized changes to systems and environments; and
   d. Assess the potential security impact of change prior to implementation.

2. VSU sensitive information is:
   a. A critical asset that shall be protected;
   b. Restricted to authorized personnel for official use; and
   c. Considered and protected when changes are administered.

3. VSU recognizes that integrity and stability of its' systems are:
   a. Cornerstones of maintaining public trust;
   b. Managed to address both business and technology requirements; and
   c. Aligned with VSU priorities, Commonwealth Standards, and industry best practices.

4. VSU recognizes that to stay innovative and flexible to technology changes; yet maintain controls to protect the integrity of its' systems and environments, the Change/Configuration Management Policy and Procedures:
   a. Will require annual review or more frequently if required to address environmental changes and
   b. Will continue to ensure alignment with the Commonwealth's Information Security Standards SEC 501-09 and SEC 525-02.

G. Baseline Configuration Management

1. For System configuration management the Data Center Manager (or designee):
   a. Documents and retains as a baseline (current state) of its systems and applies more restrictive security configurations for security configurations for sensitive agency IT system, as necessary.
   b. Monitors systems for security baselines and policy compliance.
   c. Reviews and revises all security configuration standards annually, or more frequently, as needed.
   d. Reapplies all security configurations to IT systems, as appropriate, when the IT system undergoes a material change, such as an operating system upgrade.
   e. Modifies individual IT system configurations or baseline security configuration standards, as appropriate, to improve their effectiveness based on the results of vulnerability scanning.

2. For University devices used for international travel Data Center Manager (or designee):
   a. Installs all operating system security updates
   b. Installs all anti-virus, firewall, and anti-spyware security application software updates
   c. Encrypts the computer hard disk or at least all sensitive information on the device.
   d. Updates the web browser software and implement strict security settings.
   e. Updates all application software to be used during the trip.
   f. Disables infrared ports, Bluetooth ports, web cameras, and any hardware features not needed for the trip.
   g. Configures the device to use a VPN connection to create a more secure connection.
   h. Configures the device to disable sharing of all file and print services.
   i. Configures the device to disable ad-hoc wireless connections.
   j. Ensures that all required cables and power adapters are packed with the computing asset.

H. Configuration Change Control Environment

1. System and configuration changes are requested through the CAB. This governing body will determine whether the change is feasible, warranted based on the university needs and a unique system (to ensure that duplication is avoided).
2. All changes will have the oversight and approval of the CAB prior to implementation and follow the University's Change/Configuration Management Procedures.
3. The CAB (or member designee) will:
   a. Determine the types of changes to the information system that are configuration-controlled;
   b. Review proposed configuration-controlled changes to the information system and approve or disapprove such changes with explicit consideration for security impact analyses;
   c. Document configuration change decisions associated with the information system;
   d. Implements approved configuration-controlled changes to the information system;
   e. Retains records of configuration-controlled changes to the information system for a minimum of one year;

f. Audits and reviews activities associated with configuration-controlled changes to the information system; and
g. Coordinates and provides oversight for configuration change control activities that convenes on a regular basis to review changes prior to implementation.

I. Exceptions to Change/Configuration Management Requirements

Emergency Changes will follow the Control and Configuration process; however, the timing of sign-off and approval windows may fall outside the normal timeframes. For each exception, the requesting System Owner shall document:

1. Justification of requested change,
2. The scope and extent,
3. Identify and mitigating risks associated with change,
4. Solution identified, tested and implemented; and
5. The specific duration of the change.

Each request shall be in writing to the CIO as the chair of the IT Change Management Advisory Board and approved by the IT Change Management Advisory Committee. VSU CIO indicating the acceptance of the defined residual risks. Included in each request shall be a statement detailing the reasons for the exception as well as mitigating controls and all residual risks. The requesting System Owner will be informed of the action taken. Denied exceptions may be appealed to the Vice President for Administration.

Once the exception request is approved by the VSU CIO, the request is then submitted to the Vice President of Administration for signature.

J. Violations of Policy

Violation of this policy may result in:

- Disciplinary action under the Virginia Department of Human Resources Policy 1.60, Standards of Conduct (4/16/08, 6/1/11).
- Prosecution under "Virginia Computer Crimes Act." § 18.2-152.1.

References

Virginia Information Technology Agency (VITA):
Information Security Standard (SEC 501-09.1) (12/08/2016)
Hosted Environment Information Security Standard (SEC 525-02) (08/11/2016)
Project Management Standards (CPM 112-03.3) (07/1/2016)

Virginia Department of Human Resources Management:
Policy 1.60 Standards of Conduct (4/16/08, 6/1/11)
Policy 1.75 Use of Electronic Communication and Social Media (8/01/01, 3/17/11)

9/6/17
Approval By: ____Date: ____________
President