Change Management Standard

Responsible Office: Technology Services
Initial Standard Approved: 03/23/2017
Current Revision Approved: 05/03/2023
Revision Version: 1.1

Change Summary:

Version	Summary Changes	Approved
1.0	**Initial document**	**03/23/2017**
1.1	**Updated Change Management documentation requirements, updated configuration management documentation requirements in alignment with ISO/IEC 27002:2022. Updated links to supporting documentation.**	**05/03/2023**

Standard Statement and Purpose

The purpose of Information Technology Change Management is to respond to the customer's changing business requirements while maximizing value and reducing incidents, disruption and rework and to respond to the business and IT requests for change that will align the services with the business needs.

This Standard should be used in conjunction with the documents listed in the Related Documents section.

Noncompliance with this Standard may result in disciplinary action up to and including termination. VCU supports an environment free from retaliation. Retaliation against any employee who brings forth a good faith concern, asks a clarifying question, or participates in an investigation is prohibited.

Table of Contents

Who Should Know This Standard

All persons responsible for the technical and management support of systems should read and this Standard and familiarizing themselves with its content and provisions.

Definitions

Category I Information

Information protected under federal, state or industry regulations and / or other civil statutes, where if lost may require breach notification and cause potential regulatory sanctions, fines and damages to the institution's mission and reputation. More information on data and information classification can be found in the VCU Data Classification Standard.

Category II Information

All proprietary information that if improperly released has the potential to cause harm to the institution, its mission or its reputation, but do not require breach notifications, and security or privacy of such data is not regulated or required by law or contract. Such data includes proprietary and properly de-identified research information, business related email or other communication records, financial information, employee performance records, operational documentations, contractual information, intellectual property, internal memorandums, salary information, and all other information releasable in accordance with the *Virginia Freedom of Information Act (Code of Virginia 2.2-3700)*. More information on data and information classification can be found in the VCU Data Classification Standard.

Category III Information

All non-proprietary data that is considered publicly available for unrestricted use and disclosure, where if lost or illegitimately modified, these data will generate no negative impacts to individual departments, schools, colleges, or the institution as a whole. Such information is available to all members of the University community and to all individuals and entities external to the University community. Such data can make up public website information, public press release, public marketing information, directory information, and public research information.

Controlled Unclassified Information (CUI)

Information from federal agencies that requires the protection delineated under the NIST SP800-171 standards. These types of information typically are received as a part of a research project, and are required through the Federal Acquisition Regulation clauses. Although dubious at the moment, the U.S.

National Archive is made the authoritative source for the definition of CUI, and the list of potentially covered information can be found at the National Archive CUI Registry: https://www.archives.gov/cui/registry/category-list.html.

Data Custodian
A data custodian is an individual or organization in physical or logical possession of data for data stewards. Data custodians are responsible for protecting the data in their possession from unauthorized access, alteration, destruction, or usage and for providing and administering general controls, such as back-up and recovery systems. The data custodians are directly responsible for the physical and logical security of the systems that are under their control.

Data Steward
The data steward is a University director or equivalent position who oversees the capture, maintenance and dissemination of data for a particular operation. The data steward is responsible to ensure data quality, develop consistent data definitions, sensitivity classifications, determine data aliases, develop standard calculations and derivations, define security requirements, document all appropriate "business rules" and monitor data quality within the source system and/or data warehouse. The data steward is also responsible for communicating data protection requirements to the data custodian; defining requirements for access to the data.

Data Trustee
Data Trustees will carry out plans and policies to implement guidance from the Data and Information Management Council. Data trustees are high-level employees (e.g., vice presidents, vice provosts, and deans) appointed by and reporting to the President, including but limited to Provost and Senior Vice President of Academic Affairs, Vice President of Finance, Vice President of Administration, Vice President of Research, or Senior Vice President of Health Sciences.

Federal Information Security Management Act (FISMA)
Federal Information Security Management Act (FISMA) requires the use of the National Institute of Science and Technology (NIST) Special Publication (SP) 800-53 as a common security framework for the management of various information belonging to federal government. The framework outlines the expected security controls for information that are rated at the low, moderate, or high level, where each level requires additional controls to be implemented. This regulation can impact the research projects involving federal government data, or projects that are funded by federal government. The moderate and high-level controls are a set of minimal baseline set to handle any data with medium to high sensitivity.

Information Technology Baseline
An information technology baseline is a set of technical requirements that define the minimum required standard practices. Technology Baselines are used in conjunction with Technology Standards and Policies.

Information Technology Guideline

An information technology guideline is a recommended practice that allows some discretion or leeway in its interpretation, implementation, or use.

Information Technology Standard
An information technology standard is a formal document for an established norm of methods, criteria, and processes for technology subjects.

IT Change Management (Change Management)
IT Change Management is designed to respond to the customer's changing business requirements while maximizing value and reducing incidents, disruption and rework and to respond to the business and IT requests for change that will align the services with the business needs. The Change Management process seeks to ensure that changes are recorded and then evaluated, authorized, prioritized, planned, tested, implemented, documented and reviewed in a controlled manner. This process seeks to assure that the necessary corrective action(s) are taken thereby maximizing value and reducing incidents, disruption and rework.

Payment Card Industry Data Security Standard (PCI-DSS)
Payment Card Industry Data Security Standard is a set of comprehensive requirements for enhancing payment card data security. Compliance with the PCI DSS helps to alleviate vulnerabilities that put cardholder data at risk.

Standard Operating Procedure (SOP)
A set of documented processes which when followed defines the routine operational actions for a business unit or an IT asset. Their purpose is to achieve efficiency, quality output and uniformity of performance, while reducing miscommunication and failure to comply with policies, standards and guidelines.

System Administrator
An analyst, engineer, or consultant who implements, manages, and/or operates a system on behalf of the Trustee, Data Steward, and/or Data Custodian.

System Owner
A system owner is an employee with the oversight responsibility and accountability for the management of an IT system. The system owner is typically not the administrator managing the system, but rather the departmental business manager and sponsor of the system. The system owner holds the authority to provision, de-provision, or modify the IT system to address specific business needs.

Contacts

VCU Technology Services officially interprets this Standard. The Information Security Office (ISO) is responsible for obtaining approval through the appropriate governance structures. Questions about this Standard should be directed to the Information Security Office (infosec@vcu.edu).

Standard Specifics and Procedures

The following section includes the specifics and procedures included in this Standard.

A. General Requirements

These requirements apply to all VCU systems.

1. Consistent change management process needed for equipment, software, and procedures.

All change management requests must be documented in detail, including a formal Methods and Procedures (MoP) document specifying, at a minimum:

- The business impact
- Approval process
- Communications plan
- Schedule
- Implementation Plan
- Changes to system documentation where applicable
- Test plan
- Fall back procedures.
- Change status (pending / successful / failed)

The TS Change Management Process Guide can be used as the guidance document for the formation and management of a change management process. (F14)

2. Emergency changes must be carefully and formally controlled.

All emergency change management requests must be documented in detail, including a formal Methods and Procedures (MoP) document specifying, at a minimum:

- The emergency justification
- Business impact
- Approval Process
- Communications plan
- Schedule
- Implementation Plan
- Changes to system documentation where applicable
- Test plan
- Fall back procedures
- Change status (pending / successful / failed)

The TS Change Management Process Guide can be used as the guidance document for the formation and management of an emergency change management process. (F15)

B. Special Requirements

The following requirements apply to all applicable systems used to handle specific data types; all data types in this section are considered Category I.

1. Configuration management procedures.

Formally document configuration management procedures for applicable systems. At a minimum, the procedures must include the following:

- Source configuration guidance from a trusted source
- Procedures for restricting unnecessary services
- Procedures for provisioning and deprovisioning of access
- Procedures for inactivity timeout
- Procedures for disabling insecure vendor default configurations
- Procedures for clock synchronization
- Procedures for patching of IT systems
- Procedures for system functionality changes
- Procedures for the installation of software and features
- Procedures for the removal of software and features
- Procedures for security monitoring and incident response
- Up-to-date contact information for IT system
- date of last change
- version of configuration procedure
- relation to configuration of other assets

Documentation must be periodically reviewed and updated. Required for PCI-DSS and FISMA (mod+high) (N28)

2. Formal system acceptance procedures are required.

All new systems must complete the following formal system acceptance procedures prior to deployment:

- Agreed upon security controls and verification
- Documented definition of system owner and administrator
- Consultation with system owner and administrator at all stages of provisioning
- Verification that manual processes are effective
- Confirmation that installation of a new system will not affect existing systems
- Documented operations training on the new system
- Preparation and testing of the Standard Operating Procedures (SOP)

The System Owner, in conjunction with the System Administrator and Data Custodian are responsible for the review and determine of the impact of a new system installation. The System Administrator, Information Security Office and System Owner will need to review the installation

of new system and verify that it does not affect the confidentiality, integrity and availability of existing systems (e.g. port openings, system updates, installation of outdated software, etc.). Formal acceptance (through email or a form) is required. Required by FISMA (mod+high) and CUI. (K2)

C. Exception Request

All requests for exception(s) to this policy are evaluated by the Information Security Office on a case-by-case basis. Exception requests should be made using the Information Security Exception Request Form. The completed exception request form is automatically emailed the Authoritative Unit Head listed in the request. After the Authoritative Unit Head approves the request, the Information Security Office will provide the secondary review and approval as appropriate. Evaluation criteria for exception include the requirement to which an exception is requested, the sensitivity of the information affected, compensating controls in place to mitigate additional risks, and business processes affected by the exception. The Information Security Office will send the exception request review decision and any additional correspondence to the requestor's and the authoritative unit head's email addresses.

Forms

1. **VCU Information Security Exception Form**

Related Documents

The VCU Information Technology Policy Framework contains VCU Information Technology policies, standards and baseline requirements, all of which must be followed in conjunction with this Standard. The framework also includes information technology guidelines as recommendations and best practices.

1. **Computer Network and Resources Use Policy**
2. **Information Security Policy**
3. **Exposure and Breach of Information Policy**
4. **Data Classification Standard**
5. **Network Management and Security Policy**
6. **Change Management Process Guide**
7. **Information Technology Policy Framework**
8. **ISO/IEC 27001:2022 (E)**

Revision History

Approval/Revision Date	*Title*
None – New Standard	

FAQs

There are no FAQs associated with this Standard.