Personnel Security Standard

Responsible Office: Technology Services
Initial Standard Approved: 10/23/2017
Current Revision Approved: 4/02/2024

Standard Statement and Purpose

Security of information relies largely on processes, procedures used by, and the behavior of individuals with privileged access to the information. This document describes the key security requirements of processes and procedures for the management of personnel with access to VCU information and the key expectations of all personnel involved in the storage, transmission, or processing of VCU information.

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 employees, contractors, and affiliates should read this Standard and familiarize themselves with its contents and provisions.

Definitions

Authorized User
An individual who has been granted access to specific data in order to perform his / her assigned duties at VCU. Users include, but are not limited to, faculty and staff members, trainees, students, vendors, volunteers, contractors, or other affiliates of VCU.

Centrally Managed Network Storage Device
An electronic storage device that is not native or directly connected to an individual's desktop, laptop or other computing device. Rather, the centrally managed network storage device is a storage device hosted and managed in a data center which has appropriate physical access protection, monitoring, and access management controls to ensure that only authorized users can access data. Storage servers that are hosted in the VCU University Computer Center or a comparable data center can be considered a Centrally Managed Network Device.

CFR Title 21 Part 11 (FDA) covered Information
Data or information that are received from the U.S. Food and Drug Administration (FDA), usually through sponsored research projects or protocols are covered under this regulation.

Cloud Computing
Internet-based computing that provides shared processing resources and data to computers and other devices on demand. This may include but is not limited to servers, networks, applications, and storage.

Controlled Unclassified Information (CUI)
Information from federal agencies that require the protection delineated under the NIST SP800-171 standards. This information is typically received as a part of a research project, and is 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

dbGaP
Data from the database of Genotypes and Phenotypes developed and maintained by the National Center for Biotechnology Information. Data from this database is regulated under the dbGaP Security Best Practices.

Data Custodian
The Data Custodians can have both a business and/or technical role, though it is typically considered a business role. The Data custodians are responsible for entering, modifying and maintaining data in the enterprise databases and information systems under their control. This includes access control enforcement, data integrity maintenance, and change management auditing. Working relationships with System Owners, Application Administrators, and System Administrators are essential to achieve desired technical dispositions. Data Custodians liaise with Data Stewards on issue resolution.

Data Handling

Data handling encompasses actions such as the generation, viewing, use, update, deletion, or the destruction of data. It also relates to the transfer or transmission of data from one location to another.

Data Steward
Data Stewards are appointed by and report to the Data Trustees. Data Stewards have knowledge of and work in accordance with numerous University rules and policies across the institution, including university policies on information security and privacy. Data stewards are Executive Subject Matter Experts (ESMEs) for the business domains under their authority and have formal accountability for effectively managing information resources on behalf of their domains.

Data Trustee
Data Trustees will carry out plans and policies to implement appropriate data management practices as defined by industry regulations, federal and state statues, and University policies and procedures. Data trustees are high-level employees (e.g., vice presidents, vice provosts, and deans) appointed by and reporting to the President, Provost and Senior Vice President of Academic Affairs, Senior Vice President of Finance and Administration or Senior Vice President of Health Sciences.

Departmental Technical / Application Administrator - Departmental technical / application administrators are responsible for proper operation and maintenance of an IT system and its associated applications. Administrators serve within the System Owner's department or within a department supporting the System Owner.

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.

HIPAA Information
Protected Health Information regulated by the Health Insurance Portability and Accountability Act (HIPAA). This information includes an individual's medical or mental history, or treatment or diagnosis information in combination with any of the 18 HIPAA identifiers. In order for Health or Medical information to qualify as PHI, the information must be collected from an existing HIPAA covered entity, or is received by a HIPAA covered entity. VCU designates several of its schools and departments as a part of the affiliated covered entity, which allows these organizations to share PHI without the execution of a Business Associate's Agreement. Any health or medical information that meets the HIPAA PHI definition will become PHI once it is sent into these organizations, and any such information coming from these organizations and other covered entities will also be considered as PHI.

Identifiable Genetic Information
Human Genome information that can be used to identify an individual. This information is regulated under the Genetic Information Non-Discrimination Act, and shall be treated as sensitive medical information by the organization. If PHI requirements are met, this information will be designated as PHI.

Irregular Data Access Activities
Data access activities made by any persons or organizations not having regular access authority, but excluding access activities made by VCU personnel wherein data is put to service for the purpose for which it is obtained.

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.

Security Information and Event Management System
A computerized tool used on enterprise data networks to centralize the storage and interpretation of logs, or events, generated by other software or hardware running on the network.

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 Administrators may work within the System Owner's department/organizational unit or be contracted services with the University Computer Center or a 3rd party.

System Owner
A system owner is an employee with the oversight responsibility 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.

The Cancer Genome Atlas (TCGA) data
Data from The Cancer Genome Atlas data repository developed and maintained by the National Cancer Institute, regulated by the TCGA data use agreement, which enforces dbGaP Security Best Practices and the Policy for Sharing of Data Obtained in NIH Supported or Conducted Genome-Wide Association Studies (GWAS).

United States (U.S.) person
Within the context of this document, the definition for U.S. person applies to the handling of export-controlled information. U.S. Person, as is defined by the United States Government is means a person who is a lawful permanent resident as defined by 8 U.S.C. 1101(a)(20) or who is a protected individual as defined by 8 U.S.C. 1324b(a)(3). It also means any corporation, business association, partnership, society, trust, or any other entity, organization or group that is incorporated to do business in the United States. It also includes any governmental (federal, state or local) entity.

VCU Information
VCU Information refers to information in paper, electronic or oral format that is collected, generated, transmitted, processed or stored by a VCU employee, consultant, contractor or other affiliate in the course of their work and is used to support the academic, research, patient care or administrative operations in VCU.

VCU Managed IT System
An IT system that is administered by a VCU employee and hosted on the VCU network or in the cloud, and is officially sanctioned by the VCU Information Security Office to handle University information.

VCU Networks
Computer network that is registered to VCU and managed by VCU Technology Services or Technology Services designated personnel.

Contacts

VCU Technology Services officially interprets this Standard. The VCU Information Security Office is responsible for obtaining approval for any revisions as required by the appropriate governance structures. If you have any questions about this Standard send an email to the VCU Information Security Office (infosec@vcu.edu).

Standard Specifics and Procedures

The sections below delineated the standard specifics and procedures.

A. General Requirements for all Personnel with access to Category III data/information.

1. **Definition and documentation of roles and responsibilities.**
   All personnel who manage or access information must be designated with one of the following roles, and understand the responsibilities associated with their role. (Data Trustee, Data Steward, Data Custodian, System Owner, Departmental Technical / Application Administrator, System Administrator)(F1)

2. **Information security awareness training.**
   All employees will be provided general information security awareness training on an annual basis. The training material may include any of the following but is not limited to:
   - Authentication
   - Authorization
   - General physical, electronic security
   - Appropriate use
   - Maintaining confidentiality of sensitive data
   - Information security reporting
   - Phishing and other email/phone/sms scams
   - Safe web browsing (M10)

   At a minimum, 85% of all active employees are expected to complete the information security awareness training.

3. **Security awareness training records for personnel.**
   Required security awareness training activities must be documented for all individuals. (N13)

4. **Disable data / physical access following separation from the unit or the organization.**
   All employee, contractor and affiliate data and physical space access must be removed without unreasonable delay following separation from the business unit or organization. (M5)

5. **Require role-based training for Information Technology Staff.**
   All employees with responsibilities in managing Information Technology (IT) systems must complete an IT staff security training on an annual basis. The VCU Information Security Office is responsible in providing such training.(M12)

B. Security requirements for personnel with access to CAT II Data/Information.

The requirements delineated in this section are applicable to personnel with access to VCU information/data that are classified as Category II. In addition to the requirements in the Category III Section, all personnel with access to Category II information/data must also adhere to the following requirements:

1. **Workforce clearance/screening.**

   All employees must undergo a standard employment background check by VCU Human Resources (HR). Individuals with failed background checks must undergo additional evaluation before access to information is provided (M7). .

2. **Access authorization/clearance procedure.**
   All business units must document account clearance and access authorization procedures. Documentation must be periodically updated. Documentation must include, but is not limited to:
   - Account authorization and clearance processes for employees and contractors
   - Account activation process
   - Account modification process
   - Account review process based on both timeframe and event (N18)

3. **Access termination procedure.**
   All business units must document access termination procedures. Documentation must be periodically updated. Documentation must include, but is not limited to:

   - Account review for all existing initiatives prior to disabling
   - Account review for all future requirements prior to disabling
   - Account disablement and removal from IT systems
   - Physical access termination
   - Return of all VCU assets (N19)

C. Security Requirements for Personnel with Access to Category I Information/Systems.

The requirements delineated in this section are applicable to personnel with access to VCU information/data that are classified as Category I. In addition to the requirements in the Category III and CAT II Sections, all personnel with access to Category I information/data must also adhere to the following requirements:

1. Personnel clearance and screening

All personnel, including but not limited to contractors, affiliates, and student assistants, must undergo a standard employment background check by VCU Human Resources (HR) or a comparable unit, such as a staffing agency or a business partner. Individuals with failed background checks must undergo additional evaluation before access to information is provided (M2)

2. Periodic review of access controls.

All employee, contractor, and affiliate access to data must be periodically reviewed for current justification. At a minimum, this review must be conducted annually. All-access identified without current justification must be removed without unreasonable delay. (M2)

3. Access control management and review following a change in role.

All employee and contractor access to data must be reviewed for current justification following a change in individual role. All-access identified without current justification must be removed without unreasonable delay. (M3)

4. Formal employee sanction process for non-compliance.

All incidents involving mishandling and misuse of information must be reported to, documented, and reviewed by the Information Security Office. The Information Security Office will coordinate the handling of incidents and policy violations with appropriate units within the University and in accordance with University policies and State and Federal laws. (F8)

5. Communication of applicable policies and procedures to individuals handling the data.

Data stewards are expected to communicate the applicable data handling policies, standards, procedures, and other regulatory requirements to Data custodians requiring access to data for which they are the responsible steward. Data custodians are expected to review the applicable policies, standards, procedures, and regulatory requirements prior to accessing the data. (F9)

6. Identification and documentation of account types.

All accounts on IT systems handling data must be properly identified and documented. This includes, but is not limited to, the following account types:

- Group
- System
- Application
- Individual
- Temporary
- Emergency (M6)

D. Special Requirements for Personnel Handling VCU Data/Information.

The following requirements apply to personnel handling special data/information. All data types listed in this section are considered Category I information/systems and must also adhere to the requirements listed in the Category I information/systems section.

1. Define and implement role-based access control.

All roles must have specific group-based access permissions. Data access assignments must be based on data steward and data custodian roles and positions and associated group memberships. Required for PCI-DSS, FISMA (mod), CUI, and CFR Title 21 Part 11 (FDA) covered information. (M4)

2. Security incident/breach handling training.

All individuals who handle applicable data must complete security incident and data breach handling training. This training includes, but is not limited to:

- Reporting requirement
- Reporting process
- Response guidance

The aforementioned training may be combined with general security awareness training. Required for CJI, PCI-DSS, CUI, and CFR Title 21 Part11 (FDA) covered information. (M11)

3. Role-based security awareness training.

All applicable individuals must complete role-specific security awareness training. The training will apply to individuals with access to applicable data and must outline the expected handling behavior for such data. Required for CJI, FISMA (low+mod). (M12)

4. Regulation-based security and privacy awareness training.

All applicable individuals must complete regulation-specific security and privacy awareness training. This training includes, but is not limited to:

- Health Insurance Portability and Accountability Act Privacy Training (HIPAA)
- Payment Card Industry Data Security Standard Data Handling Training (PCI-DSS)

Required for PCI-DSS, HIPPA, dbGaP, and TCGA. (M13)

5. Security awareness training on insider threat.

All individuals must complete insider threat security awareness training. This training includes, but is not limited to:

- Fraud recognition
- Disgruntled employees
- Inappropriate use of privileges

The aforementioned training may be combined with general security / privacy training. Required for FISMA (mod), PCI-DSS, and CUI. (M14)

6. Data handling by U.S. person only, no others can access, handle or store data.
All applicable data must be accessed, handled and stored only by United States (U.S.) persons. Required for export control information. (M15)

7. Representative must be a member of VCU Security Listserv (Secure-L).
Business units handling data must have an appropriate representative enrolled in the VCU Information Security Office Secure-L listserv. Required for CJI, PCI-DSS, and FISMA (mod). (M16)

8. Annual Review and execution of rules of behavior / acceptable use.
All individuals with access to data must understand and execute the following documents annually:

- Acceptable use policy (AUP)
- Rules of Behavior

Required for PCI-DSS. (M9)

9. Employee confidentiality agreement / Acceptable use agreement.
All employees must understand and execute the following signed documents:

- Employee confidentiality agreement
- Acceptable use policy (AUP)

Required for PCI-DSS, CJI, HIPPA, FISMA (mod) and PII of EU Citizens. (M8)

10. Apply segregation of duties to functions in the environment.
The following segregations of duty apply to the groups specified:

- The mission-critical function group must not share duties or functions with the information control group.
- The software development group must not share duties or functions with the code review group.
- The software quality assurance group must not share duties or functions with the production operations group.
- The audit group must not share duties or functions with the security operations group.

Required by PCI-DSS, FISMA (mod), CUI, and CFR Title 21 Part 11 (FDA) covered information. (F16)

11. Require Criminal Background Check for Positions designated as Sensitive
Require criminal background checks for sensitive positions as designated by VCU Human Resources in accordance with The Code of Virginia § **2.2-1201.1** (M7)

Forms

1. **VCU 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. Other related documents are listed below.

1. **Computer and Network Resource Use Policy**
2. **Information Security Policy**
3. **Exposure and Breach of Information**
4. **Data Classification Standard**
5. **Network Management and Security Standard**
6. **Human Resources – Forms - Separating Employee Guidelines**
7. **Technology Services – Separation from Employment Recommendations**
8. **22 CFR Part 120 - ITAR**
9. **Code of Virginia H 2391 - § 2.2-1201.1.**
10. **Department of Human Resource Management – Policy Guide Sensitive Positions**

Revision History

Approval/Revision Date	Title
10/23/2017	New Standard (effective 10/23/2017)
4/2/2024	Update outdated link to related documents and form; Add security awareness training and role based training for IT staff under CAT III data.

FAQ

There are no frequently asked questions associated with this Standard.