Data Handling and Storage Standard

Responsible Office: Technology Services
Initial Standard Approved: 04/10/2017
Current Revision Approved: 02/06/2024

Standard Statement and Purpose

Proper handling and storage of information is the cornerstone of an effective information security management program, as it helps to prevent theft, loss, and misuse of information, and helps to reinforce trust among the University and its students, employees, business partners and the community. This standard establishes the expectations and requirements for the secure handling and storage of VCU information.

This Standard should be used in conjunction with the other 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, business associates, affiliates, and contractors are responsible for knowing this standard and familiarizing themselves with its contents and provisions.

Definitions

Adequate Physical Protection
Protection of VCU information that meets or exceeds the protections provided by the University Computer Center (UCC). UCC required protections are 24x7 monitoring, security staff on premises, keycard access and auditing of access to location and server room, identification, sign-in and escort of visitors, and video surveillance.

Business Associate

A “business associate” is a person or entity that performs certain functions or activities that involve the use or disclosure of protected health information (PHI) on behalf of, or provides services to, a covered entity as defined by the Health Insurance Portability and Accountability Act (HIPAA) and the Virginia Consumer Data Protection Act, § 59.1-575 of the Code of Virginia (Virginia Code). A member of the covered entity’s workforce is not a business associate. A covered healthcare provider, health plan, or healthcare clearinghouse can be a business associate of another covered entity. The Privacy Rule lists some of the functions or activities, as well as the particular services that make a person or entity a business associate if the activity or service involves the use or disclosure of protected health information. The types of functions or activities that may make a person or entity a business associate include payment or health care operations activities, as well as other functions or activities regulated by the Administrative Simplification Rules.

Category I Information/Data (Confidential and Regulated)
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/Data (Sensitive)
All proprietary information that, if improperly released, has the potential to cause harm to the institution, its mission, or its reputation but **does 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 documentation, contractual information, intellectual property, internal memorandums, salary information, and all

other information releasable in accordance with the *Virginia Freedom of Information Act (Virginia Code §2.2-3700 et. seq.)*. More information on data and information classification can be found in the VCU Data Classification Standard.

Category III Information/Data (Public)
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 all individuals and entities external to the University community. Such data can make up public website information, public press releases, public marketing information, directory information, and public research information.

Centrally Managed Network Storage Devices
Redundant electronic storage devices that are not native or directly connected to an individual's desktop, laptop, or other computing device. The network storage device is physically hosted and managed in a data center(s) which has appropriate physical access protection, monitoring, and access management controls. Locally hosted servers and storage devices, regardless of its networking capability or redundancy, will not be considered as a centrally managed network storage device.

21 C.F.R. Part 11 (FDA) covered Information
This federal regulation provides guidance for the creation and storage of electronic records from the U.S. Food and Drug Administration (FDA), and data and information obtained, maintained, or accessed through sponsored research projects or protocols are covered under this regulation.

Contracted Site
There is no formal State definition of a "Contracted Site". In the absence of a state standard definition this standard includes any contracted site having a written agreement with the university to perform a scope-of-work.

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.

Criminal Justice Information (CJI)
Information regulated under the FBI Criminal Justice Information Services (CJIS) Security Standard; this includes any information provided by the FBI CJIS necessary for law enforcement and civil agencies to perform their missions including, but are not limited to biometric, identity history,

biographic, property, and case / incident history data. Like many other regulations, CJIS Security Standards also carries a transient property, where whether an organization receives the data directly or indirectly from a third party, such data will be regulated by the security standards. The VCU Police Department and certain research projects may have access or store these data.

Data Custodian

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 Handling

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

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.

dbGaP (database of Genotypes and Phenotypes)

National Institute of Health (NIH) database which was created to archive and distribute data on genotype and phenotype type studies and research. Maintained by the National Center for Biotechnology Information, this database is regulated under the dbGaP Security Best Practices.

Encryption

The process or the means of transforming plain text readable information into scrambled information that can only be deciphered with a cryptographic key, usually protected by a passphrase. Encryption in this documentation refers to industry-accepted encryption techniques; preferably meeting the FIPS 140-2 requirements. At a minimum, symmetric encryption algorithms should utilize AES-128 or better and asymmetric encryption algorithms should use RSA-4096 or better. Encryption using SSL versions should be avoided. Encryption using TLS V1.2 or higher is acceptable. Digital signatures shall be used to verify the integrity of the data. More information on adequate encryption methods can be found in the Information Security Baselines - Transport Encryption Security Guideline for TLS.

Export Controlled Information
Information, usually intellectual property or research information, which can either be directly or indirectly used in military applications. Specific federal export control laws exist (including International Traffic in Arms Regulations (ITAR) and Export Administration Regulation (EAR)) that require the protection of and restrict access to this information. Research projects dealing with information in these fields may be subject to export control laws.

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.

Fixed Storage Device
Internal storage media used by a computer to store files. In a computer system, fixed storage devices are usually the computer's internal hard drive(s).

Health Insurance Portability and Accountability Act (HIPAA)
Federal law enacted to establish privacy and security standards for the protection of certain health information, including information stored and transmitted in electronic forms.

Information Storage and Handling
Within the context of this document, information storage and handling refers to actions that create, store, transmit, process, modify, destroy, and/or archive information. The storage and handling of information may involve both electronic and physical actions.

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.

Laptop Computer
A laptop computer is a battery or AC powered portable computing device that operates on traditional desktop operating systems such as Microsoft Windows, Mac OS, and GNU Linux.

Offsite location
Within the context of this document, offsite locations include physical space not owned, leased, or managed by VCU. Examples of offsite locations include an employee's home, the airport, a hotel, or a business partner's office.

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.

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).

University Data and Information
Information in paper, electronic or oral form 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 at VCU.

University Owned Equipment
Unless specified otherwise by the sponsoring funding source, any equipment purchased with funding allocated to the Virginia Commonwealth University, or its employees for the purpose of education, research, outreach, and administration.

Untrusted Networks
Untrusted network includes both untrusted internal networks and untrusted external networks. These networks generally include the majority of the Internet, the VCU public facing network,

RESNet, and any VCU guest networks. For more information on trusted and untrusted networks, please see the VCU Network Management and Security standard and its associated baseline.

VCU Managed IT System
An IT system that is administered by a VCU central or departmental IT 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
A VCU Network is a computer network that is registered to VCU and managed by VCU Technology Services.

Contacts

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

Standard Specifics and Procedures

The following section contains the standard requirements.

A. Roles and Responsibilities

Data trustees are university officials who have the ultimate authority over policies, procedures, standards, and guidelines regarding business definitions of data and the access and usage of that data within their delegated authority.

Data stewards are appointed by and accountable to the data trustees. Data stewards must have knowledge of and work in accordance with the policies, standards, and guidelines across the institution, including university policies on information security and privacy.

The data custodians are individuals or organizations (including third-party vendors) who are responsible for entering, modifying, and maintaining data in institutional or third-party-provided information systems. For more information regarding the roles and responsibilities of Data trustees, Data stewards, and Data custodians, please reference the Data and Information Governance policy here.

B. Requirements for Data Handling and Storage

The following sections of this document delineate the requirements for handling and storage of VCU data/information. Requirements for the handling and storage of such data/information are defined by data categories. For more information on data categories and classification, review the VCU Data Classification Standard.

1. General Requirements and Category III Information/Data Requirements.

a. **Access to information must be assigned by the Data Steward or a designee who is responsible for the overall management of the data; access to such information must follow defined processes from responsible data stewards.**

b. **Refer requests for information from media representatives (i.e., reporters, TV news crews, etc.) to the Office of University Public Affairs, Division of University Relations.** The Office of Public Affairs in the Division of University Relations is also responsible for managing all Freedom of Information Requests to university units. Requests should be forwarded to foiavcu@vcu.edu. Additional information is at https://marcom.vcu.edu/requests/foia/

c. **Ensure data access controls are consistent on all systems used to handle data.** All systems that transmit, process, and store data must employ consistent data access controls. Controls are determined by the sensitivity of the data being handled and subsequently applied to all systems. (G31)

d. **Unauthorized distribution and use of data/information is not allowed.** Distribution and use of data and information must follow all guidance provided by applicable data stewards or their designees. Distribution and use of information outside of the provided guidance is not permitted.

2. Category II Information/Data Requirements.

The requirements delineated in this section are applicable to VCU information/data that are classified as Category II. In addition to the requirements in the Category III Section, the handling and storage of Category II information/data must also adhere to the following requirements:

a. Access to data must be protected.
Access to electronic data must be protected by a password or passcode and an acceptable MFA that meets or exceeds the requirements stated in the VCU Password, Authentication, and Access Standard. Access to paper data must be protected by physical protection mechanisms, such as locked offices or locked cabinets. Physical protection mechanisms used to protect information must meet the requirements delineated in the Physical Security Standard.

b. Disposal of information and media (paper and electronic) used to store such information must follow the requirements of the Media Sanitization Baseline and the University's Records Management Policy.
All paper and electronic media must be securely disposed of in accordance with VCU record retention and disposal policies and associated procedures. All paper and

electronic media must be identified and documented at the time of disposal. (H7)

c. Electronic storage media used to store University information must be reviewed and approved by the Information Security Office.
Refer to the Data Management System for acceptable information/data storage media. Requests for exceptions must be completed by the Data Custodian with the approval of the Data Steward or designee using the VCU Information Security Exception Request form.

d. Sharing by individual or group accounts only.
Unauthorized sharing of data/information with the public is prohibited. All data shared using collaboration tools must be shared with specific users or a defined group of users. Any data sharing beyond the originally defined scope must be approved by the Data Steward or designee. Public sharing of data/information is prohibited without the explicit approval of the Data Steward or designee. (G24)

e. Devices storing or accessing data must not be located on a publicly accessible network without any form of reasonable authentication and authorization.
The authentication and authorization method used must meet requirements delineated in the Password, Authentication, and Access standard. (H51)

3. Category I Information/Data Requirements.

The requirements delineated in this section are applicable to the handling and storage of VCU information/data that are classified as Category I. In addition to the requirements from the Category III and Category II Information/Data Requirements Sections, the handling and storage of Category I information/data must also adhere to the following requirements:

a. **Records of authorized users with access to Category I Information must be maintained by Data Stewards or their designee.**
The records must include, but are not limited to, the following:

- List of individuals with authorization to access Category I information
- Actions performed by accounts assigned to each of the individuals
- Formal authorization and approval documentation for individuals with access to information

b. The long-term storage of Category I data in voice mail is not recommended.
Deletion of this data from voicemail systems should be done as soon as is reasonable.

c. Report any disclosure or breach of Category I information as required in the University’s Exposure and Breach of Information Policy**.**

d. Faxing of Category I information should be done only when the physical security of the data can be assured at the sending and receiving ends.
Fax machines, such as those located in areas accessible by the public, must not be used to send and receive fax documents containing Category I information. Examples of such locations include the public areas of the libraries, student commons, public computer labs, classrooms, and any other areas that can be accessed by the general public without any reasonable form of prior authentication. This requirement does not apply to shared office space accessible only to authorized personnel. However, faxed and received documents containing Category I information should be retrieved and removed immediately from the fax machine following the successful transmission.

e. Secure sanitization of electronic media prior to re-use.
All electronic media suitable for re-use must be securely sanitized in accordance with the Media Sanitization Baseline prior to being re-deployed. (H8)

f. Media containing data and going to an offsite location must be encrypted.
All data contained on media transported offsite must be encrypted as defined in the Encryption Security Standard before transport occurs. All media used to store data must meet the VCU Encryption Security Standard and associated baseline requirements. This is applicable but not limited to the following media:

- USB drives
- CD/DVD-ROMs
- Laptops
- Desktops
- Servers
- Tablets
- Phones
- Any other electronic storage devices (H49).

g. Portable storage devices used to store data must be encrypted.
All data stored on portable media must be encrypted. All device types used to store data must meet the VCU Encryption Security Standard and associated baseline requirements. (H6)

h. Backup must be stored in a physically secured location.
All backup media must be stored in a physically secure location. Physical security controls comparable to those applied to the original data must be in place and maintained. Physical security requirements are delineated in the VCU Physical Security Standard, and specifics on data backup can be found in the Backup Baseline document. (K7)

i. Data access control policy and procedure.

All data access control policies and procedures must be warehoused and maintained with examples and sample forms, readily available upon user request. Forms must include but are not limited to:

- Data access request procedures
- Data access revocation procedures
- Periodic data access review procedures
- Additional associated forms (N5)

j. Documented procedures for handling, processing, transmission, and storage of data.

Overall expectations for handling, processing, transmission, and storage of applicable data should be provided by the data steward or a designee. IT systems must have documented procedures for handling, processing, transmission, and storage of data. System owners, in conjunction with the system administrator, are responsible for defining, documenting, and implementing procedures related to IT systems. Procedures must include but are not limited to

- Physical and technical access restrictions based on data classification
- Handling and labeling of media based on data classification
- Administrative, physical, and technical controls
- Security monitoring and incident response

Documentation must be periodically reviewed and updated. (N24)

k. Assets and media containing data must be classified and inventoried.

All assets and media used to store data must be periodically inventoried and documented, including, at a minimum:

- Unique device ID
- Physical/logical location
- System owner

The Data Custodian, working in conjunction with the system owner, is responsible for the data classification and inventory functions. At a minimum, inventories should be reviewed annually. (H43)

l. Production data must not be used with test or development systems.

Original form production data must not be used under any circumstances for test or development functions. If this requirement is not viable, the referenced production data must be de-identified or obfuscated prior to introduction to any test or development environment. (G30)

m. Individuals with access to applicable data must not discuss or display data in an environment where it may be viewed or overheard by unauthorized individuals.

n. Sharing of applicable data with a third-party service provider/vendor requires a third-party assessment and approval by IT Governance.
A formal third-party vendor information security review is required for all third-party systems/service providers needing to collect, access, store, or otherwise handle VCU Category I data through the IT Governance process. Annual review and re-assessment of the third-party service providers used university-wide are needed to ensure the proper storage and handling of VCU information. Third-party service providers are required to be reviewed by the IT Governance Process. For questions regarding IT Governance or the procurement process, contact ITGov@vcu.edu.

o. Secure disposal of data and media when no longer needed.
All expired data must be securely destroyed regardless of storage medium. All data and medium must be securely disposed of in accordance with VCU record management and retention policies and applicable procedures. All data and media destruction events must be documented and available for audit review. Individual schools, departments, as well as the VCU central Technology Services unit, may leverage the VCU Computer and Media Decommissioning form to track the disposal and destruction of devices and media. (G12, F18)

4. Special Data Handling and Storage Requirements

The following requirements apply to personnel or systems used to handle specific data/information types; all data types listed in this section are considered Category I data and must also adhere to the requirements listed in the Category I Information/Data Requirements Section.

a. Periodic review and removal of unneeded data.
Data stewards and system owners must jointly review assigned processes per the established timetable. Upon review completion, processes must be internally certified to reflect current data management standards. All process shortfalls identified must be documented and remediated in accordance with VCU requirements. If mitigation options do not exist, the shortfalls must be addressed as exceptions requiring the Information Security Office approval. Required by FISMA (mod), CUI, CJI, PCI-DSS, and CFR Title 21 Part 11 (FDA). (F2)

b. Periodic review and removal of unneeded data.
Data custodians and data stewards must jointly review assigned stored data per the established timetable. Upon review completion, data must be purged or archived in accordance with VCU requirements. Required for FISMA (mod), and PCI-DSS. (F3)

c. Procedures should be established to prevent the re-identification of data.

Anonymized data must not be re-identified with the original information source for any purpose. No employee or contractor will attempt to re-identify data or contact original information sources. De-identified data must be assigned the classification of "anonymous" for the entirety of its lifecycle. Data stewards and data custodians must identify and document anonymized data under their charge, including formal education for all data handlers. Required by PCI-DSS, dbGaP, and TCGA. (F22)

d. Information flow enforcement.

All data flows for applicable data must be documented in detail, including source and destination addresses, port information, reasons for data flow, and data flow schedules. All data flows must be monitored to ensure compliance with data flow restrictions and timing. Data flows must be suspended when flows deviate from documented information. Required by FISMA (mod), CUI, CJI, and PCI-DSS. (G20)

e. Physical transfer of media containing data must use secured couriers with tracking.

All physical transfers of paper or electronic media containing applicable data between buildings within a site or involving offsite physical locations must use secured couriers with tracking capability. Required by FISMA (mod), CJI, and PCI-DSS. (H48)

f. Prevent copy, move, print & storage of data to local drives from remote locations.

Data from remote locations must not be copied, moved, printed, or stored locally. System and application owners must implement controls as applicable. If business needs exist for these functionalities, exception requests must be filed with the Information Security Office. Required by PCI-DSS, FISMA (mod). (J14)

g. Annual progress report on a project using data.

All project managers using provided data must provide annual progress reports to data providers. Data providers will be notified upon project completion or achieving a final project conclusion. Notifications must include data end state disposition statements. Required by dbGaP and TCGA. (N12)

h. Operating procedures for systems handling data (communicated with appropriate personnel).

All IT systems handling data must have operating procedures documented and communicated to appropriate personnel. Procedures must be periodically reviewed and updated. Required by PCI-DSS, FISMA (mod), CUI, and CFR Title 21 Part II (FDA). (N22)

i. Mask sensitive data elements when displayed.

Mask sensitive data elements so only a small portion of the data is showing when displayed to individuals. Only people with business needs can see the full information. Required by Social Security Number, Driver's License Number, PCI-DSS, and authentication (Log-in) credentials. (G35)

j. Must not store or record any full track data, verification code, and PIN.
System cannot store any full magnetic strip track data, PIN, or verification (CVV, CVC2) codes. This is required by PCI-DSS. (H54)

k. Limit use of organizational storage media on external information systems.
Limit or prevent the use of media containing data on external information systems. Require approval before these media can be used on other external systems. This is required by PCI-DSS, FISMA (mod), and CUI. (H56)

l. Data stored in shared systems must be logically separated from other, less sensitive data.
Data on shared systems must be logically separated. Data designated as "sensitive" must be segregated from data designated as "not sensitive." Storage access control lists must be implemented to restrict LUN, NAS, and SAN access to authorized employees and contractors. This restriction includes application of database access control lists to restrict specific field access within a given database. Required by CJI, PCI-DSS, FISMA (mod), CUI, and Export Controlled Information. (G8)

m. Label devices and media containing data.
Place physical labels on devices and media containing data to state the sensitivity of the system/media. Required by FISMA (mod), CUI, and Export Control Information. (L19)

o. Staff and faculty traveling internationally must not transport export-restricted data or software outside of the U.S. The Office of Research Programs can provide guidance (http://www.research.vcu.edu/export_control/index.htm). Store the minimum data necessary for travel. All other files should be securely deleted (old email, old files, etc.). An encrypted computer should be used.

p. Secure deletion of data (Department of Defense (DoD) deletion method).
All data must be securely deleted in accordance with DoD 5220.22-M/NIST SP 800-88 wipe methods. A minimum of three wipe passes must be made over the disk space to zero it out properly. Required by PCI-DSS, dbGaP, TCGA, and FISMA (mod). (G23)

q. Ensure adequate storage, transmission, and processing power is allocated.
All system and application owners must complete formal capacity planning prior to initial system provisioning. Future growth requirements are addressed through follow-up planning sessions conducted bi-annually at a minimum or when otherwise indicated. Planning processes should address a 12 to 24-month horizon. Required by FISMA (low+mod). (K1)

r. Daily incremental/differential and weekly full backups are needed.
At a minimum, all systems must adhere to the following backup strategy:

- Daily incremental or differential backup

- Weekly full backup

Required by FISMA (low+mod). (K10)

s. Computers/devices containing data must not be located in a public area.
All systems containing data must have physical access barriers that prevent unauthorized access. No devices containing data or with access to devices containing data will be located in public areas. Required by CJI, PCI-DSS, HIPAA, dbGaP, TCGA, PII of Children Under 13, FISMA (mod), CUI, and Export Controlled Information. (L7)

t. Must be a U.S. Person to handle data.
The person handling data must be a U.S. citizen, U.S. permanent resident, or U.S. political refugee. No other personnel with other nationalities can handle this data. Required by Export Controlled Information. (Q3)

u. Cannot use shared or group accounts to access data.
Shared or group accounts cannot be used to access the data. Each session accessing data must be uniquely tied back to an individual. Required by PCI-DSS, HIPAA, FISMA (mod), CUI, Export Controlled, and CFR Title 21 Part 11 (FDA) covered information. (Q4)

v. Annual request must be sent to data provider for renewal or termination of data access.
On an annual basis, requests must be sent to the data provider on renewal of a project involving data or close out of a project in which data is no longer needed. Required by dbGaP and TCGA. (Q6)

w. Prohibit the use of personally owned equipment from accessing this data.
All personal devices are prohibited from accessing applicable data and networks providing data transport. Personally owned computers meeting VCU requirements may be used for remote access. Required by CJI and FISMA (mod). (H41)

x. Any copies of or extracts from the original data must be tracked.
All copies and extracts generated from original data must be approved and tracked. Individuals receiving data must have formal authorization from the data steward or designee. Required tracking documentation includes the following:

- Named recipient of the copy or extract with applicable contact information
- Description of all agreements in place applicable to data handling
- The intended use of the copy or extract
- Requirements for protecting and securely destroying the copy or extract
- Granted duration of use

Required by dbGaP, TCGA, and FISMA (mod). (G32)

y. Store the data outside of the U.S.
Data may **not** be stored outside of the bounds of the United States (e.g., with global companies and international data centers) or with collaborative groups in other countries. Required by PCI-DSS. FISMA (mod), PII of EU Citizens, and Export Controlled data. (Q1)

z. Access to data using public equipment is prohibited.
All public use equipment, including but not limited to computers intended. for use in computer labs, Internet cafes, or hotel lounges, is prohibited from accessing applicable data. Required by Applicable to CJI, PCI, dbGAP, TCGA, and FISMA (mod). (H42)

aa. Offsite secure backup storage is required.
Backup media containing backup data must be transferred offsite to a physically secure location for safekeeping in case of an on-site disaster affecting the location. Required by PCI-DSS. (K9)

Tools

1. VCU Data Management System
2. VCU Data Classification Tool

Forms

1. VCU Information Security Exception Form
2. VCU Computer and Media Decommissioning Form
3. VCU IT Governance Submission 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.

Baseline documents can be found in the VCU University Computer Center IT Professionals Intranet under Security Baselines. Access to the IT Professionals Intranet requires approval. Requests for access can be made via email to uccnoc@vcu.edu.

1. Computer Network and Resources Use Policy

2. Information Security Policy
3. Data and Information Governance
4. VCU IT Governance
5. Exposure and Breach of Information Policy
6. Network Management and Security Policy
7. Records Management Policy
8. Data Classification Standard
9. Password, Authentication and Access Standard
10. Encryption Security Standard
11. Physical Security Standard
12. Transport Encryption Security Guideline for TLS
13. Media Sanitization Baseline
14. Data Storage Guideline

Revision History

This standard supersedes the following archived policies and standards:

Approval/Revision Date	***Title***
4/10/2017	Data Handling and Storage Standard
5/22/2017	Minor revisions
01/27/2022	Revisions: Added reference to Data and Information Governance policy. Revised responsibilities section to better align with the Data and Information Governance Policy. Reviewed for consistency and redundancy. Fixed broken links.
6/6/2022	Revisions: Added reference to Information Security Baselines - Transport Encryption Security Guideline for TLS, Data and Information Governance, reference to record management and IT-Governance Process. Fixed broken links.
11/3/2023	Revisions: Updated definitions. Fixed broken links

FAQs

There are no FAQs associated with this standard.