VIRGINIA COMMONWEALTH UNIVERSITY

VCU

Physical Security Standard

Responsible Office: Technology Services
Initial Standard Approved: 12/08/2016
Current Revision Approved: 05/25/2017

Standard Statement and Purpose

This Standard delineates physical security requirements associated with physical space that is used to house VCU information in both physical and electronic format. Adequate security controls applied to physical space is imperative to the security of University information, as it can help to prevent the theft of equipment and documents containing sensitive 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 and this Standard and familiarizing themselves with its contents and provisions.

Definitions

Authoritative Unit Head
The Authoritative Unit Head is a role held by a Vice President, Dean, Department Chair, and in some cases a Director of a department or unit. This is usually the person who has responsibility and is accountable for a major work unit.

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.

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 requires the protection delineated under the NIST SP800-171 standards. These 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

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
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, viewing, 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.

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.

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 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)

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.

Contacts

VCU Technology Services officially interprets this Standard. The Information Security Office is responsible for obtaining approval for any revisions as required by the appropriate governance structures. Direct questions regarding this Standard to the Information Security Office (infosec@vcu.edu).

Standard Specifics and Procedures

The following sections contain the requirements of this standard.

A. General Requirements applicable to Category III Data/Information.

The following general requirements apply to physical space containing Category III information

1. Use of keys and / or keycards for access to physical space is optional.

In order to prevent unauthorized access to physical space, keys and / or keycards should be considered for implementation for physical space, including buildings, rooms, drawers or cabinets. For physical space containing only Category III information, this control is optional and at the discretion of the individuals or department occupying the space.

2. Lock physical space containing information when it is not occupied.

If key and / or keycard is used to control access to physical space, then the space must be locked when it is not occupied by authorized personnel.

B. Category II Data/Information requirements.

In addition to the requirements from the General requirements section, the physical security of Category II data must also adhere to the following requirements:

1. Periodically inspect facility entrance and exit to detect physical tampering.

Entrance and exit locations for facilities containing Category II information must be periodically inspected for physical tampering. The following items should be examined:

- Propped open doors
- Evidence of tampered locks
- Broken or propped up windows
- Physical damage or modification to doors or windows
- Physical damage or modification to surveillance equipment

All findings must be reported to Information Security Office without unreasonable delay. This is the responsibility of the Authoritative Unit head or their designee. (L15)

2. Expectations for physical security applicable to data must be set by Data Stewards.

Design and Implementation of physical security controls, including provisioning and de-provisioning of physical or electronic assets is the responsibility of Data Stewards and can be

implemented with the assistance of System Administrators in conjunction with the System Owners.

3. **Consider the use of electronic keycards for physical access.**
   Areas containing data should consider the use of electronic keycard for access. If electronic key cards are used, individual identification such as a unique ID (examples: Prox Card number, VCU Card Number) that can be associated with an individual person must be included as part of the keycard access profile. (L1)

4. **Ensure secured data center utility services and environmental controls.**

   Datacenter utilities services and environmental conditions (e.g., water, power, temperature and humidity controls, telecommunications, and internet connectivity) shall be secured, monitored, maintained, and tested for continual effectiveness at planned intervals to ensure protection from unauthorized interception or damage. (K12)

5. **Ensure redundancy of critical infrastructure services and environmental controls.**

   Ensure data center utility services and environmental controls such as water, power, temperature, humidity, Internet connection, and telecomm, etc. are designed with automated fail-over or other redundancies in the event of planned or unplanned disruptions. (K13)

6. **Ensure adequate physical protection to protect asset against natural and man-made disasters**

   Anticipate and develop plans for countermeasures against damages caused by natural and man-made disasters, such as fire, flood, wind, earthquake, civil unrest, biological hazard, etc. (K14)

C. Category I Data/Information Requirements.

In addition to the requirements from the General and Category II and III Requirements Section, the physical security of Category I data must also adhere to the following requirements:

1. **Access to physical space containing data requires key or electronic keycard (electronic or paper).**
   At a minimum, all areas containing electronic or paper data must use a key and lock for access when not occupied. Where applicable, electronic keycard access is preferred for physical entry to these areas. A key and lock may be used to control access to the following area types:

   - Room
   - Drawer

- Cabinet
- Cage
- Data center (L2)

2. **Documents containing data must be locked away when not needed.**
   All printed documents containing sensitive data must be stored in a secure location when unattended or not in use. Acceptable locations include locked cabinets, locked file drawers, inside an office with a locked door, or other locations with comparable physical security controls. (G26)

3. **Remove documents containing data from printers, fax, and copiers.**
   All printed documents containing sensitive data must be removed without unreasonable delay from copiers, fax machines, and printers. (G27)

4. **Develop and maintain list of individuals with physical access to data.**
   All individuals with physical access to data must be documented. All records must be periodically reviewed and maintained. This policy applies to individuals with permanent and visitor access authorizations (L8)

5. **Review and revise physical access authorization periodically.**
   A physical access authorizations provided to individuals must be reviewed periodically. Individuals no longer requiring physical access to an area must be removed from the physical access list as soon as is reasonably possible. (L10)

6. **Only authorized maintenance personnel can access infrastructure devices.**
   Access to HVAC, structured cabling, and wiring closets is allowed only for authorized maintenance personnel. All maintenance personnel must receive permission prior to conducting any service work that could potentially impact infrastructure operations. (L14)

D. Special Requirements.

The following physical requirements apply to all data types listed in this section. These data types are all considered Category I data and must also adhere to the requirements listed in the Category I Data/Information Requirements Section.

1. **Maintain access log to physical space.**
   All access to physical spaces containing or used to handle data must be accounted for by means of keycard access log or paper sign-in sheet. At a minimum, the following information must be recorded and retained in accordance with VCU retention requirements:

   - Names of individuals accessing physical space

- Companies individuals work for
- Entrance and exit dates and times
- Detailed reasons for visit
- Items removed from or added to area
- Authorizing signatures

Required by PCI-DSS, HIPPA, PII of Children Under 13, FISMA (mod), CUI, Export controlled information, and CFR Title 21 Part 11(FDA) covered information. (L3)

2. **Review physical access logs periodically.**
   All physical access logs must be periodically reviewed for suspicious entry. Any suspicious activity must be reported to Information Security Office or VCU Police without unreasonable delay. Required by CJI, PCI-DSS, FISMA (mod), CUI and Export Controlled Information. (L4)

3. **Video surveillance and / or keycard monitoring for physical space access.**
   Aside from areas excluded by the applicable regulation such as a cash register located in a public area, all physical space access must be monitored by video surveillance and / or use of individual electronic keycards. All access logs must be maintained in accordance with Control L3. All access logs must be reviewed in accordance with Control L4. Required by PCI-DSS. (L5).

4. **Restrict access to data environment from public network jacks.**
   All public network jacks must have their access restricted and should be considered untrusted. At a minimum, all access to the data environment must be denied. If the public network jack is not used, it should be disabled at the port level. Required by PCI-DSS, FISMA (mod), CUI and Export Controlled Information. (L11)

5. **Disallow access to area containing data from loading dock.**
   All access from loading docks to areas containing data must be authenticated, authorized, and accounted for. Required by PCI-DSS, HIPPA, PII of Children Under 13, and FISMA (mod). (L12)

6. **Register asset entering area containing data to asset inventory.**
   All assets entering an area containing data must be registered and inventoried upon entry. The following information must be documented and maintained:

   - Asset serial number
   - System owner
   - Asset description
   - Asset value
   - Asset facility destination details (i.e., floor, room, cage, rack)

- Data type contained in asset

Required by CJI, PCI-DSS, HIPPA, Donor Information, and FISMA (mod). (L13)

7. **Retain documentation of repairs and modifications to facility.**
   All repairs and modifications to security-related physical components of a facility used to handle or store data must be documented and maintained. This includes, but is not limited to:

   - Doors
   - Locks
   - Walls
   - Surveillance equipment
   - Electronic keycard systems

   All activities must be recorded with the facility management. Required by PCI-DSS and HIPPA. (L16)

8. **Require display of badge for employees and visitors.**
   Employees and visitors must display identification badges at all times when onsite at a location that handles or stores data. Individuals failing to comply must be denied entrance to the facility or be authenticated via an alternative mechanism. These specific Individuals should be issued a temporary badge. Required by PCI-DSS. (L17)

9. **Must implement process to issue and retrieve visitor badges.**
   All visitors must be issued a visitor badge upon arrival. Visitor badges are expected to include the following information:

   - Visitor name
   - Visitor company
   - Badge validity date
   - Employees they are visiting
   - Areas of building authorized to access
   - Visitor color code

   At conclusion of visitor activities, visitors must be escorted to the location of badge issuance and return their visitor badges. Required by PCI-DSS. (L18)

10. **Formal authorization needed for removal of data from on-site location.**
    All data and equipment containing data requiring removal from onsite locations must receive formal approval from management and the Information Security Office prior to relocation. Removal requests for data must contain the reason for removal, data custodian, data steward, system owner, data classification, and past / current / future disposition. Removal requests for equipment containing data must contain the reason for removal,

system owner, system serial number, asset tag, and past / current / future disposition. Required by PCI-DSS, dbGaP, TCGA, FISMA (mod), and CUI (F13).

11. **Escort visitors and identify them with a badge.**
    All visitors must display a badge at all times containing full individual identification and specific access authorizations. Visitors requiring access to areas containing applicable data must be accompanied by a VCU escort with adequate access permissions. Required by CJI, PCI-DSS, FISMA (mod), CUI and Export controlled information. (L9)

12. **Review \ revise physical access authorization at least annually.**
    At a minimum, all physical access authorizations provided to individuals must be reviewed annually. Individuals no longer requiring physical access to an area must be removed from the physical access list as soon as is reasonably possible. Required by PCI-DSS, FISMA (mod), CUI, and Export controlled information. (L10)

13. **Enforce physical safeguard measures at alternate worksites (e.g. telework).**

    Require reasonable assurance that alternative worksites are physically secure, and ensure that employees can maintain and certify the security of these sites. Applicable to FISMA (mod), CUI, and Export Controlled Information. (L20)

Forms

1. VCU Information Security Exception Form

Related Documents

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

Revision History

Approval/Revision Date	*Title*
12/08/2016	New Standard
05/25/2017	Minor revisions

FAQs

There are no FAQs associated with this Standard.