System Security Standard

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

Standard Statement and Purpose

The System Security Standard contains mandatory requirements applicable to security controls implemented on VCU managed IT Systems. These requirements are designed to provide a reasonable and risk based set of protections for IT systems. These requirements also support the enforcement of the VCU Information Security Policy and other related policies and standards.

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 1
Definitions 2
Contacts 6
Standard Specifics and Procedures 7
Forms 14
Related Documents 15
Revision History 15
FAQs 15

Who Should Know This Standard

All persons responsible for the technical and management support of VCU Managed IT systems should read this Standard and familiarize 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 guard on premises, keycard access and auditing of access to location and server room, identification, sign-in and escort of visitors, and video surveillance.

Administrative Privileges
Within the context of this document, administrative privileges refer to the highest level of permission that is granted to a computer user. In business and networked systems, this level of permission normally allows the user to install software, and change configuration settings.

Application Inventory Database
The application inventory database contains a list of all the known applications that the University has created and manages in-house or utilizes via a third party partner. Access to the application inventory database can be requested via an IT Services Request ticket.

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.

Business Associate
A person or entity other than a member of the covered entity's (VCU-ACE) workforce, who performs a function for or assists a covered entity with a function that involves the use or disclosure of individually identifiable health information (sensitive information).

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.

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 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 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)
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.

Department Contact
This is the field in the server inventory that is usually associated with the System Owner. This is the person who has responsibility over how the system is managed and by whom.

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).

Handling of Data
Refers to when a person views, uses, updates, deletes or destroys data. It also relates to the transfer of data from one location to another.

Health Insurance Portability and Accountability Act (HIPPA)
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.

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.

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.

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 and Mac OS.

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.

Primary User Account
Within the context of this document, a primary user account is the account used by an individual to conduct day to day business operations; such as word processing, access to a file share, and access to enterprise applications, etc. This account that will be used by individuals most of the time, and will not have administrative privileges.

Secondary User Account
Within the context of this document, a secondary user account refers to an account that is used by the computer user for a specific function, and is not used for day to day operations. The secondary user account can be used for administrative functions, such as the installation and maintenance of software.

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.

Server Inventory Database

This database contains data on all University servers and related infrastructure equipment such as storage and networking devices.

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).

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 in 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 Policy and its associated baseline.

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
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 Standard. The Information Security Office is responsible for obtaining approval for any revisions as required by the appropriate governance structures. Questions regarding this Standard should be directed to the Information Security Office (infosec@vcu.edu).

Standard Specifics and Procedures

The following section includes the standard requirements.

A. General and Category III Information/Data Requirements.

These requirements apply to all VCU systems.

1. Registration of server or server-like devices in the VCU server inventory database.
All servers and server-like devices handling VCU data/information must be registered in the VCU server inventory database. Registration data must include at a minimum:

- the description of the device
- category of data as defined by the VCU Data Classification Standard
- system specifications (IP Address, MAC Address, etc.)
- network location and configuration
- primary and secondary technician contact information
- department contact information (e.g. system owner, data custodian, and data steward)

Servers and server-like devices not in the server inventory may have network access suspended immediately upon discovery. The Department Contact/System Owner is responsible for the annual review and update in the server inventory database of the data associated with the system. Approval of access to the server inventory database is required and is obtained by contacting uccnoc@vcu.edu. (F20)

2. Application registration.
All applications running on VCU systems or 3rd party systems used to handle University Data and Information must be registered in the application inventory database. Information for these applications must be reviewed and updated periodically.

3. Remove or Rename default administrative accounts.
All default administrative accounts must be removed or renamed prior to production system deployment. (H1)

4. Change all default passwords on IT systems and applications.
All default passwords must be changed on all Information Technology (IT) systems and applications prior to production system deployment. (H2)

5. Disable Guest accounts.
All guest accounts on systems that transmit, process, and store data must be disabled or removed prior to production system deployment. (H5)

6. Inactivity lock-out for device containing data after 30 minutes or less.

All devices used to access or store data must automatically lock the user session after 30 minutes of inactivity. All users must re-authenticate to unlock the session. (H11)

7. Login banner.
All systems must display a login click-thru banner prior to authentication informing the user of the following terms and conditions for acceptable system use:

- Acceptable behavior on the system including subsequent use of network resources
- Rules, processes, and procedures regulating use
- VCU right to monitor all activities on local machines, including ingress and egress network traffic components
- Consequences for non-compliant activity initiation or involvement

The current version of the official VCU Long Banner Text is available at https://www.ucc.vcu.edu/intranet/security/doc.aspx?id=128. Access to this document is via the IT Professionals Intranet baseline section. Contact uccnoc@vcu.edu for approved access. (H15)

8. System firewall must be enabled (desktop / laptop).
All desktops and laptops must have an operating system firewall enabled and configured for default deny permissions. Network traffic exceptions requiring passage through the firewall will only be permitted for approved applications and ports. (H31)

9. Periodic scan of critical system files to reduce the risk of infection.
Critical system files must be periodically scanned to ensure they are free from infection. University approved and centrally managed antivirus and anti-malware software must be used to scan in real-time as files are modified or added. Additionally, full scan of the system must be conducted at least weekly. (H32)

10. System and applications must be patched on regular schedule.
All systems and applications must be patched on a regular basis. All patches must be thoroughly tested prior to deployment. Patch application priority is based on the severity of the vulnerability and criticality of the system being addressed. (H33)

11. University servers must be dedicated to specific functions.
All University servers that handle applicable data must be dedicated to specific function(s) in accordance to documented system security plans. Each server must be deployed and secured according to its originally described function(s). Using the device for unintended functions circumvents the security controls deployed to protect this device and its associated data; therefore any functional change of the server must be approved by the Information Security Office via changes to the system security plan prior to deployment or reconfiguration. (K4)

12. System configuration must meet applicable VCU configuration baseline.
All devices used to transmit, access, and store data must meet the VCU configuration baseline for operating systems, applications, databases and other forms of technology. (H34)

13. Up-to-date antivirus / anti-malware protection is needed (desktop / laptop).

All desktops and laptops must have University approved antivirus and anti-malware installed and active. Software subscriptions and definitions must be current at all times. (H30)

14. System configuration must meet regulatory or contractual requirements if provided by data provider.
All systems used to transmit, access, and store data must meet specific regulatory or contractual requirements. If conflicts exist between VCU baseline and the regulatory or contractual requirements, the most stringent requirements take precedence. (H35)

15. Removal of administrative privileges for all users.
Administrative privileges must be removed from all primary user accounts prior to production system deployment. With approval of system owner, users requiring administrative privileges may receive such privileges through a secondary user account. If used, these accounts must be limited to administrative functions only. Any provisioning of administrative privileges on a primary user account requires a formal exception request and approval from the system owner. All exception requests, including dispositions, must be documented, filed and approved by the Information Security Office. (H3)

16. Servers require protection mechanism against malicious code
All University servers must be protected from malicious code infection from web traffic, hacking, intrusion, and external media. The following proactive and reactive layers of protection must be used:

- Antivirus / anti-spyware
- Firewalls
- Intrusion Detection System
- Intrusion Prevention System (K3)

B. Category II Information/Data Requirements.

The requirements delineated in this section are applicable to systems having VCU information/data that are classified as Category II. In addition to the requirements from the General Requirements Section, systems having Category II information/data must also adhere to the following requirements:

1. Log out of IT system when finished.
All users must log out of IT systems when their work is completed. This action returns the screen to a login prompt. (G21)

2. Disable automatic logon features to systems.
All systems that access, transmit, process, and store data must disable all automatic logon functionality. At no time will systems cache credentials and bypass authentication prompts. If specific functionality is required during system restart, that functionality must exist as a service or daemon that does not require system logon. (H16)

3. Implement only one dedicated primary function per server.
Segregate server functions that require different security levels; For example, a web server should not also be a database server or file server. These functions must be segregated. (K11)

B. Category I Information/Data Requirements.

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

1. VCU centrally managed real-time logging and monitoring of authentication / system and alerting of security events.

All devices used to access or store data must have authentication, system, and security events centrally logged in real-time. (H10)

2. Logging and auditing of account / data creation, access, modification, and deletion.

All account and data creation, access, modification, and deletion activities must be documented in human readable form. Information must contain:

- **Who** – e.g., username, email address, employee number
- **System** – e.g., hostname, IP Address, database, directory location
- **Action** – e.g., account creation, account access, account modification, account deletion, record creation, record access, record modification, record deletion
- **When** – e.g., 7/7/2014 at 3:54 PM EST, 7/7/2014 at 21:54 UTC (G14)

3. Log and monitoring of local events on data and program usage.

All systems that transmit, process, and store data must log all local system events pertaining to data, program, and server usage. System owners are expected to assure the maintenance and execution of application and server log review activities. (H14)

4. Audit system and security events.

All systems that transmit, process, and store data must maintain the following system and security event information for audit purposes:

- Successful and failed logon events
- Successful and failed privileged escalation events
- Successful and failed use of privileged accounts
- User account creation and removal (H25)

5. Backup audit logs for systems to central syslog server.

All audit logs, including but not limited to system, security, syslogs, and application logs, must write to a central syslog server and local log. Audit log information transmitted over a network must be encrypted. (H28)

6. Spam protection for electronic communication channels required.

All electronic communications channels must incorporate the following spam protection methods:

- Mail user agent (MUA) filters
- Spam filters
- Anti-phishing tools (K5)

7. Device must be synchronized with authoritative NTP server (VCU or NIST).
All systems that transmit, process, and store data must use network time protocol (NTP) for system clock synchronization. At a minimum, 2 authoritative NTP sources must be configured for redundancy. (H26)

8. Disable unneeded services or protocols on system.
All systems that transmit, process, and store data must enable only the applications, protocols, and services specified in the system security plan. All other applications, protocols, and services must be disabled prior to production system deployment. Exceptions require formal system owner approval, and must be documented as amendments to the existing system security plan. All exceptions must be documented and filed with the Information Security Office. (H4)

C. Special Requirements.

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

1. Must complete periodic penetration testing at least annually.
Applicable systems and networks must receive annual or more frequent internal and external penetration testing. All identified vulnerabilities and misconfigurations must be documented and reviewed with system owners. Appropriate steps to mitigate exposures must be taken if possible. If mitigation options do not exist, the vulnerabilities must be addressed as exceptions requiring approval from the Information Security Office. Required for PCI-DSS, FISMA (mod). (F6)

2. Review security events and logs for servers / system components daily.
All systems that transmit, process, and store data must have their logs and security events reviewed daily. System owners must maintain a record document of manual security event and log review activities. Required for PCI-DSS. (G33)

3. System logs documenting all authentication, modification, addition, and deletion activities must be retained for a minimum of 1 year.
The most recent 90 days of log activities must be readily available and in searchable format. System owners must maintain a record document of all audit trail log review activities. Required for CJI and PCI-DSS data. (G34)

4. Deploy change detection mechanism to identify unauthorized changes to critical files.
All applicable systems containing data must deploy change detection tools to monitor system files, application files, configuration files, and all audit and / or log files for unauthorized changes. System owners must report all detected unauthorized change activities to Information Security Office and follow appropriate incident handling procedures. Required by PCI-DSS. (H52)

5. Limit access to audit logs for data to only privileged users and record access attempts.
All access to audit logs must be restricted to those with business justification. All attempts to access audit logs must be documented for success and failure results. Information must include audit log name, source address, username, timestamp, and access result. Audit access information must not be stored in the local environment. Required by PCI-DSS, FISMA (mod),

CUI, and CFR Title 21 Part 11 (FDA) covered information. (G22)

6. Prevent the use of unauthorized / personally owned writable / removable media.
Storage of data using unauthorized or personally owned removable media is strictly prohibited. With proper justification, end users will be provided with approved devices that meet VCU compliance requirements. Required by PCI-DSS, FISMA (mod), and CUI. (H9)

7. Inactivity lock-out for device containing data after 15 minutes or less.
All devices used to access or store data must automatically lock the user session after 15 minutes of inactivity. All users must re-authenticate to unlock the session. Required by CJI, PCI-DSS, dbGaP, and TCGA. (H12)

8. Purge data on mobile device after 10 failed logon attempts.
All mobile devices must be configured to automatically clear organizational data following 10 consecutive failed logon attempts. Mobile devices automatically cleared and not physically recovered must be identified to the Information Security Office for breach exposure analysis. Required by CJI, PCI-DSS, FISMA (mod), and CUI. (H24)

9. Encrypt audit logs for systems.
All audit logs, including but not limited to system, security, and syslogs, must be encrypted during transit across the network. All encryption keys must be maintained and stored in accordance with VCU polices. Required by CJI and FISMA (mod). (H27)

10. Backup audit logs to separate media than data.
All audit logs, including but not limited to system, security, and syslogs, must be backed up using media separate from data backups. Data stored on this media should be encrypted if physical security cannot be guaranteed. Required by PCI-DSS, FISMA (low+mod), and CUI. (H29)

11. Access to system utilities must be monitored and limited to administrators.
Access to system management tools must be restricted to system administrators. All access attempts must be logged, including source, destination, date, time, and username information. Users requiring access to system management tools must file a formal exception request with the system owner. All exception requests, including dispositions, must be documented and filed with the Information Security Office. Required by CJI, PCI-DSS, dbGaP, TCGA, FISMA (mod), CUI, and CFR Title 21 Part II (FDA) covered information. (H39)

12. Login time to system must be restricted to work hours only.
Users may only access systems during work hours. Hours of access are determined by user functional requirements. Administrators are excluded from this restriction. Required by FISMA (mod). (H40)

13. Examine device to detect tampering or substitution annually.
Applicable devices must receive periodic tampering and component substitution inspections. At a minimum, these inspections must be performed annually. All unauthorized actions identified must be documented and reviewed with system owners and Information Security Office. Appropriate steps must be taken to mitigate future device modifications. Required by PCI-DSS and CFR Title 21 Part II (FDA) Covered Information. (H44)

14. System maintenance tools must be inspected before used in environment.
All systems containing data must have applicable tools validated and approved prior to system installation or maintenance. Required by FISMA (mod) and CUI. (H45)

15. Restrict the execution of web-based mobile code (scripting code).
All applicable systems must execute the following scripting code from only trusted sources.

- JavaScript
- Java
- Flash
- ActiveX
- Shockwave
- Similar languages

If requirements exist to execute scripting code from a non-trusted source, the request must be made to Information Security Office for review. Required by FISMA (mod) and CUI. (H46)

16. System must not store sensitive authentication data once authentication and authorization is successful.
Systems must not store the following sensitive authentication data (SAD) following successful cardholder authentication and authorization:

- Full track data (mag stripe data or equivalent on chip)
- CAV2 / CVC2 / CVV2 / CID
- Pins and Pin Blocks

Required by PCI-DSS. (H47)

17. Prevent multiple concurrent sessions from the same user account.
All systems containing data must restrict user sessions to one per user account. Multiple concurrent connections from the same user account are prohibited. Required by CJI. (H53)

18. System troubleshooting procedures.
All system and application owners must document troubleshooting procedures for applicable systems. Procedures must include how to handle and recover from detected faults in IT systems. Procedures must be periodically reviewed and updated. Required by FISMA (low+mod). (N26)

19. System and information integrity procedures.
All applicable IT systems and data must document procedures to verify information and system integrity. Procedures must include methods to verify integrity while data is both at rest and in transit. System integrity verification must be ongoing via critical file system monitoring. Documentation must be periodically reviewed and updated. Required by PCI-DSS, CUI, PII of EU Citizens, and CFR Title 21 Part II (FDA) Covered Information. (N27)

20. Asset and media inventory must be kept for assets accessing / containing data.
All applicable assets that access data must be periodically inventoried and documented

including:

- unique device ID
- serial number
- physical / logical location
- manufacturer
- system owner

All applicable media containing data must be periodically inventoried and documented including:

- unique device ID
- serial number
- physical / logical location
- manufacturer
- data custodian
- data steward

All applicable asset and media location changes must be documented by the system owner following the relocation. Required by CJI, PCI-DSS, HIPPA, donor information, FISMA (mod) and CUI. (F11)

21. Retain audit trail logs for the lifetime of the data.
Audit log retention period must match the data retention period. Required by CFR Title 21 Part II (FDA) Covered Information. (G38)

22. Application whitelisting or blacklisting technology must be used on endpoints.
University approved application whitelisting or blacklisting technology must be used to control and monitor software used on endpoints accessing or storing data. Required by PCI-DSS, FISMA (Mod), and CUI. (H57)

23. 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
- Asset owner
- Asset description
- Asset value
- Asset facility destination details (i.e., floor, room, cage, rack)

Required by CJI, PCI-DSS, HIPAA, donor information, and FISMA (Mod). (L13)

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.

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. **Exposure and Breach of Information Policy**
4. **Data Classification Standard**
5. **Network Management and Security Policy**
6. **VCU Authentication Banner Text (Requires IT Professional Intranet Access)**
7. System Security Baseline

Revision History

Approval/Revision Date	*Title*
None – New Standard	

FAQs

There are no FAQs associated with this Standard.