Virginia Commonwealth University
Technology Services

Security Standard for Electronic Academic Research Data and Intellectual Property

Effective Date: *August 2007*
Compliance Date: *January 2008*
Scheduled Review: January 2009

Revision History:

Version	Date	Revision Issuance
1	April 06	Initial draft to the VCU Security Web Page
2	Jan 07	Clarification of standard and addition of guidelines
3	July 2007	Modified wording and layout
4	December 2007	Modifications of various components
5	January 2008	Various edits

Authority:
VCU Chief Information Officer
VCU Vice President of Research
VCU Information Security Officer

In Compliance with:
VCU Academic Policy: Security of Electronic Sensitive Information
VCU Academic Policy: Information Security Policy
COV ITRM Information Technology Security Management Standard SEC501-01
COV ITRM Information Technology Security Management Policy SEC500-02 – 7.2.3.
VCU-Affiliated Covered Entity Security Policies
Strategic Plan for Information Technology at VCU
VCU Office of Research Policy on Research Data
VCU Office of Research Intellectual Properties Policy

Purpose:

This standard focuses on the planning, implementation and enforcement of information security safeguards that are designed to secure the confidentiality, integrity and availability of University owned research program outcome data classified as “confidential information” and created, received, maintained, used and transmitted in electronic format. This standard also applies to University owned intellectual property maintained in electronic format

The **standard** is a statement that *defines the performance expectations or processes* that *must be in place* in order for the University to maintain a secure and protected electronic environment for research data and intellectual property.

Applied Industry Best Practices:

National Institute of Standards Technology (NIST).
ISO IEC 17799 Information Security Controls and Objectives.

Regulatory Compliance References:

Health Insurance Portability and Accountability Act (HIPAA Privacy and Security).
Office of Human Research Subjects Protections 45 CFR, Part 46. Common Rule.
FDA CFR 21, Part 50 (Informed Consent); Part 56 (IRB).
JCAHO-SBHC, Ethics, Rights and Responsibilities.

Scope:

This standard is applicable to all University owned research data and intellectual property. While academic instruction and research systems are exempt from the Virginia Information Technologies Agency’s Information Technology Security Policy and Standard (SEC500-02 and SEC501-01), the best practices components of SEC 501-01 have been used as a model for the requirements outlined below. The rationale for using the SEC501-01 Security Standard is that the components of this standard are comprehensive, and compliance will most often fulfill the requirements of other applicable standards.

Requirements of Standard:

R1. Risk Management

- **R1.1 Data Sensitivity Classification** – each data owner shall identify the sensitivity requirements of all types of data being handled using the criteria of confidentiality, integrity and availability (see VCU’s Data Classification Guidelines) and determine whether each type of data may also be subject to other regulatory requirements. It is assumed that research data has a high degree of integrity and availability. A sensitivity rating of high on the criteria of confidentiality should be used to classify the data as sensitive.

R2. Contingency Planning

- **R2.1 Data Backup and Restoration –** Systems housing confidential data must ensure that the following backup procedures are followed:
    - The University's current solution for secure off-site storage for backup media
    - Performance of backups only by personnel who are authorized by the data owner.
    - Review of backup logs after the completion of each backup job
    - Approval of backup schedules of a system by the system owner
    - Protection of any backup media that is sent off site in accordance with University requirements
    - The retention policy for academic and research data should be set at a reasonable limit that both fulfills the retention requirements for this data and addresses the resource limitations involved in handling such data. The Library of Virginia's Records Retention and Disposition Schedule General Schedule No. 111 has the following requirements:
        - Research accounting records (101168), research contract or grant administration records (101198), research final reports (101169) and research notes, work papers and technical data - contract or grant funded (101170) be retained for 5 years after the end of research or in accordance with contract/grant stipulations and/or college or university policy, whichever is greater, then offered to archives, special collections or the library. Archives, special collections or the library may selectively retain all or part of the records for their collections; the balance is to be destroyed.
        - Research notes, work papers and technical data - college or university sponsored (101171) are required to be retained for 3 years after the end of research or in accordance with college or university intellectual property or retention policy, whichever is greater, then offered to archives, special collections or the library. Archives, special collections or the library may selectively retain all or part of the records for their collections; the balance is to be destroyed.

R3. System Security

- **R3.1 System Hardening –** systems housing confidential data must have more restrictive security configurations such as those prescribed in VCU's Computer Security Checklists based on the Center for Internet Security's Benchmarks.
    - System owners of confidential IT systems must document an IT Security Plan that includes:
        - All existing and planned security controls for the system, including a schedule for implementing planned controls

        - Submit the Security Plan to the VCU Information Security Officer.
        - Update the Security Plan every three years or more often if necessary and resubmit for approval.
    - The **Security Plan template**, which is posted on the VCU security website, should be used for each IT system containing confidential data.

- **R3.2 Interoperability –** the following steps to protect confidential data shared with other IT systems must be taken:
    - System Owner and Data Owner must document IT systems with which data is shared and include the following:
        - Types of data shared
        - Direction of data flow
        - Contact information for the organization that owns the IT system with which data is shared including System Owner, Information Security Officer (or equivalent) and System Administrator
        - System Owners of IT systems which share data develop a written agreement that delineates IT security requirements for each interconnected IT system and for each type of data shared.
        - System Owners of IT systems that share data inform one another regarding other IT systems with which their IT systems interconnect or share data and inform one another prior to establishing any additional interconnections or data sharing.
        - The written agreement specifies if and how the shared data will be stored on each IT system.
        - The written agreement specify that System Owners of the IT systems that share data acknowledge and agree to abide with any legal requirements regarding handling, protection and disclosure of the shared data.
        - The written agreement maintains each Data Owner's authority to approve access to the shared data.
        - The System Owners approve and enforce the agreement.

R4. Logical Access Control

- **R4.1 Account Management** - Formal account management practices for requesting, granting, administering and terminating accounts that have access to confidential data to include the following:
    - Access is granted based on the principle of least privilege
    - Provide for annual review of all user accounts for confidential IT system to assess continued need for the accounts and access level and periodic review of user accounts for other IT systems

- Authentication and authorization requirements are based on sensitivity and risk. Use of passwords on confidential systems is required and additional authentication methods, such as tokens and biometrics, should be considered based on sensitivity and risk.
- Guest and shared accounts are prohibited
- Accounts that are not used for a predefined period are locked out automatically and unneeded accounts are disabled.

- **R4.2 Password Management**
  - Password is required on all accounts on systems classified as confidential including local, remote access and temporary accounts. Passwords are also required on mobile devices when storing confidential data.
  - Password length and complexity must follow strong password requirements as defined in VCU's Password Standard.
  - Default passwords must be changed immediately after installation
  - Transmission of identification and authentication data is prohibited without the use of encryption.
  - Group account IDs and shared passwords on confidential IT systems are prohibited.

- **R4.3 Remote Access (5.5.2)**
  - All remote access to confidential systems and data must be encrypted and this requirement applies to both session initiation and all exchanges containing confidential data.
  - The encryption technology used must be one that is authorized by the University. Exceptions should be submitted via the Security Standard Request for Exception form that is on the security website.
  - Remote access requirements to confidential data must be documented
  - Physical and logical hardening of remote access devices must be documented
  - All remote access must be audited and records must be maintained
  - Training to IT system users on remote access policies, standards, procedures and guidelines must be provided prior to granting remote access capabilities.

R5. Data Protection

- **R5.1 Data Storage Media Protection –** To protect data from compromise, the following are required:
  - Protection and identification of stored confidential data is the responsibility of the Data Owner
  - Confidential data must not be stored on mobile data storage media unless the data is encrypted and there a written exception approved by the VP of Research and the CIO.

    - All data storage media containing confidential data must have logical and physical protection commensurate with sensitivity and risk.
    - Only authorized personnel are allowed to pickup, receive, transfer and deliver data storage media containing confidential data.
    - Email transmission of electronic research data and intellectual property internally within the University network and externally from the University is secured with industry standard and Technology Services' approved mechanisms. If research data is attached to an email, the attachment must be transmitted in an encrypted format over the University network or externally over the Internet.
    - Data storage media containing confidential data must be sanitized before disposal or reuse.
- **R5.2 Encryption**
    - Transmission of confidential data must be encrypted commensurate with sensitivity and risk.

R6. Facilities Security

- IT systems containing confidential data must have safeguards to protect against human, natural and environmental risks
- There must be safeguards to protect against physical access by unauthorized personnel for all components of IT systems housing confidential data including computer hardware, wiring, displays and networks
- A system of monitoring and auditing of physical access to confidential IT systems must be in place.

R7. Personnel Security

- **R7.1 Access Determination and Control –** access determination and control practices for confidential systems and all third party systems with which confidential systems interconnect must be documented to include the following:
    - perform background investigations of employees based on access to confidential IT systems or data
    - restrict visitor access to facilities that house confidential systems or data
    - require non-disclosure and security agreements for access to confidential systems and data
    - establish termination and transfer practices that require return of logical and physical assets that provide access to confidential systems and data
- **R7.2 Security Awareness and Training**
    - Users of systems containing confidential data must receive security training so that each user is aware of and understands the following concepts:

        - Training and awareness programs are provided to research investigators on the role-based responsibilities for the confidentiality and security of research data and intellectual property. This training is documented and considered part of the research approval process
        - The University's policy for protecting IT systems and data
        - The concept of separation of duties.
        - Employee responsibilities in continuity of operations and incident detection and reporting
        - The IT system user responsibilities and best practices in prevention, detection and eradication of malicious code, proper disposal of data storage media and proper use of encryption products
        - Access controls including creating and changing passwords and the need to keep them confidential
        - The University's remote access policies
- **R7.3 Acceptable Use**
    - The following are prohibited for users:
        - installation or use of proprietary encryption hardware/software on University systems
        - tampering with security controls configured on their workstations
        - connecting unauthorized devices to a University system or network
    - Transmission of unencrypted confidential data over the Internet is prohibited

Implementation Guidelines:

- **Remote Access**
    - Secure remote access to confidential systems and data must be done via a University approved VPN technology. Requests to use other secure access technology may be submitted on the Security Standard Request for Exception form that is on the VCU Security website and sent to the VCU VP of Research and the CIO for approval.
- **Encryption**
    - Confidential data that is authorized to be stored on mobile devices such as laptops or USB drives must use a University approved encryption technology. See the **VCU security website** for information about the currently approved encryption products.

Enforcement:

IT systems housing research data classified as confidential will be periodically scanned and audited to ensure that the security safeguards specified in this standard are in place and that the systems and data are being appropriately protected. In cases where systems and data are not being properly secured and there exists a threat, Technology Services may act on behalf of the University to eliminate the threat by working with the relevant system and data owners or overseers to quickly close security holes and remediate any problems. In circumstances where these collaborative efforts fail or there is an urgent situation requiring immediate action and leaving no time for collaboration, the system may be disconnected from the network by Technology Services staff under the direction of the CIO or designee in order to prevent system compromise and/or data loss.

Exceptions:

Requests for exceptions to any of the requirements of this standard should be made using the Security Standard Request for Exception form that is on the VCU Security website and sent to the VCU VP of Research and the CIO.

General Responsibilities:

VCU Vice President of Research:

The Vice President of Research has the responsibility and right to exercise broad discretion necessary for the encouragement, development, *and protection* of inventions, patents and other intellectual property.

VCU Senior Research Investigator's Custodial Responsibility:

The senior VCU research investigator is charged with maintaining the custody of all research data on behalf of the University. The senior research investigator is responsible for the integrity, preservation and *security* of research data[1] and appropriate marking of all University intellectual property that may be included in research data. Senior members of the research investigation teams have the obligation to discus the responsibilities of data acquisition, use, management, access and retention with other members of a research team.

VCU Security Officer:

The VCU Security Officer has the duty and responsibility to develop, issue and maintain policies, procedures and standards for the security of University owned research data and intellectual property and to ensure that these standards are being practiced.

VCU Research Advisory Council:

[1] The preservation and *security* of research data is an allowable direct cost of conducting research and can be a budgeted item in a sponsored program agreement.

The Council of Research Deans works with the Vice President of Research to represent and serve the interests of the VCU research enterprise.

Ownership:
The University retains all rights, title and interest in any and all research data and intellectual property generated, created, or developed in facilities operated or controlled by the University, supported by funds administered by the University and performed in the course of regular duties by members of the workforce.

Definitions

Sensitive Information: Defined by the Commonwealth of Virginia, ITRM Information Security standards SEC501-01 as any data or information that has restrictions placed upon its access within the University or its disclosure outside of the University.

Confidential Data: A sensitivity rating of high on the criteria of Confidentialty (see the Guidelines for Data Classification). Confidentiality refers to the privacy of an asset and can be defined as which people, under what conditions, are authorized to access an asset. It refers to the protection of data from unauthorized disclosure to individuals or IT systems.

Research Data: As it applies to this standard is defined by the VCU Office of the Vice President of Research "Policy on Research Data" to mean recorded information, in electronic form or media in which it is recorded which constitute the original observations and methods of a study and the analysis of these original data that are necessary for reconstruction of the reports of a study made by one or more investigators. Research data is also inclusive of data gathered in anticipation of a report.

Intellectual Property: Defined by the Office of the Vice President of Research "Policy on Intellectual Property" to mean anything developed by anyone covered under the VCU research data or intellectual information policies that fit but are not limited to one or more of the following categories:

1) an invention;
2) an issued patent;
3) a copyrighted work;
4) a legal right inherent in a patent, copyright or trademark; or
5) know-how or trade secrets.

Data Owner: The person who is responsible for the policy and practice decisions regarding data and has the primary responsibility for determining the purpose and function of a data resource.

Data Custodian: An individual or organization in physical or logical possession of data on behalf of the data owner. Data custodians are responsible for protecting

the data in their possession from unauthorized access, alteration, destruction or usage and for providing, administering or overseeing the general controls, such as back-up and recovery systems.

Data Classification: See VCU Data Classification Guidelines