Encryption Security Standard

Responsible Office: VCU Technology Services, Information Security
Initial Approved: 02/22/2012
Current Revision Approved: 11/14/2016

Standard Statement and Purpose

This document provides the encryption requirements for all University data and information generated, processed, stored, and transmitted on behalf of VCU. This document is intended for use by VCU Data Trustees, Data Stewards, and Data Custodians to determine the need and applicability of encryption for the data managed by these individuals. This document is not intended to be used with data that is personally owned by individual employees, where if lost or stolen, has no negative impact on VCU.

Any unauthorized access or loss of University data and information or equipment containing University data and information are expected to be reported according to the instructions defined in this standard.

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 individuals who generate, store, process, transmit, or use VCU data are expected to read, understand and agree to the responsibilities defined in this standard and any published revisions of this standard.

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.

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.

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 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.

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.

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

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 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.

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 that meet the FIPS 140-2 requirements. At a minimum, symmetric encryption algorithms should utilize AES-128 or better and asymmetric encryption algorithms should use RSA-2048 or better. Encryption using SSL versions should be avoided. Encryption using TLS V1.0 or higher is acceptable. Digital signatures shall be used to verify the integrity of the data.

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).

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.

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.

Contacts

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

Standard Specifics and Procedures

A. Responsibilities

1. VCU Technology Services is responsible for the implementation and maintenance of an enterprise encryption solution that includes disk or file based encryption for desktops and laptops and encryption technology for email. The implemented solution shall include a secure centralized management system for administration and distribution of encryption software, keys, and key escrow.

3. Data Trustees are responsible to adhere to the storage and transmission requirements delineated in this standard, and provide oversight to applicable data stewards in ensuring the encryption of any applicable data.

4. Data Stewards are responsible to adhere to the storage and transmission requirements delineated in this standard, and collaborate with data trustees and data custodians on the

encryption of any applicable data.

5. Data Custodians are responsible to adhere to the storage and transmission requirements delineated in this standard, and implement the encryption solution on all IT systems used to store and transmit any applicable data.

B. General Encryption Related Storage and Transmission Requirements

The following section delineates the encryption requirements for the storage of electronic data and information generated, processed, stored, transmitted, or used by VCU.

1. **All fixed storage devices on University owned laptop computers must be encrypted with the VCU enterprise encryption solution. Store keys used to encrypt and decrypt data in protected forms.**

2. **All keys used to encrypt data must be stored in encrypted form, and stored separate from the data they encrypt. (G29)**

C. Category II Information Requirements

In addition to the general encryption requirements from the section above, the following requirements apply to Category II information.

1. Transmission encryption over untrusted networks.

All data transmitted over untrusted networks between IT systems or between IT systems and end users must be encrypted. Transmission methods include, but are not limited to:

- Web Access
- EMail Access
- File Upload
- Video Conferencing
- Remote System Access (RDP, VNC)
- Remote Application Access
- Voice Over IP (VoIP)
- Surveillance Video Streaming (G19)

D. Category I Information Requirements

The following section delineates the requirements for the storage and transmission of VCU owned Category I information. Requirements for the storage and transmission of such information are defined by data categories. For more information on data categories and classification, review the VCU Data Classification Standard. In addition to the requirements in this section, all Category I information must also follow the requirements noted in the Category II Information section.

1. **All emails containing Category I information must be encrypted using the University centrally managed email encryption tool. Attachments containing Category I information must be encrypted before it is sent, and bulk transfer of Category I information should utilize**

University managed bulk file transfer tools.

2. **Transmission encryption**
   All data transmitted between IT systems or between IT systems and end users must be encrypted. Transmission methods include, but are not limited to:
   - Web Access
   - EMail Access
   - File Upload
   - Video Conferencing
   - Remote System Access (RDP, VNC)
   - Remote Application Access
   - Voice Over IP (VoIP)
   - Surveillance Video Streaming (G19)

3. **Storage encryption when data is not stored in location with adequate physical protection.**
   All data stored on servers, desktops, and laptops must be encrypted when not stored in locations with adequate physical security. Encryption keys must be maintained and documented In accordance with VCU policies. (G17, G18)

D. Special Requirements

The following requirements apply to remote access to systems used to handle specific data 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 Requirements section.

1. **Digital signatures shall be used to verify the integrity of data.**
   All data and software applications that access data must be integrity verified through use of digital signatures. All digital signatures must be stored on a fault tolerant system, including fully enabled audit and monitoring functionality. Applicable to CUI, FISMA (mod + high), and CFR Title 21 Part 11 regulated information. (G28)

E. Reporting Loss or Theft of Equipment or Data

In the event a server or computer workstation is stolen, the theft must be reported immediately to the VCU police at 828-1196. In the event that Category I or II data is suspected to be improperly accessed, lost, or stolen, the theft or loss must be reported immediately to the VCU Information Security Office at infosec@vcu.edu.

Forms

1. VCU Information Security Exception Form

Related Documents

VCU Information Technology Policies are located in the University's Policy Library. The Information Technology Policy Framework contains VCU Information Technology Policies, Standards and Baseline requirements.

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. **Guideline on Data Storage Tools**

Revision History

This standard supersedes the following archived standard:

Approval/Revision Date	
February 2012	Encryption Security Standard

FAQs

There are no FAQs associated with this standard.