Disaster Recovery Standard

Responsible Office: Technology Services
Initial Standard Approved: 05/31/2017
Current Revision Approved: 05/31/2017

Standard Statement and Purpose

This Standard addresses aspects of disaster recovery that are necessary to avoid and recover from an event or events that affect the confidentiality, integrity and availability of VCU's data, computer and network resources.

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 persons responsible for the technical and management support of systems should read and this Standard and familiarize themselves with its contents and provisions.

Definitions

Access to Data
In the context of this document, this term refers to the VCU data that is stored, processed or transmitted by an outside entity. This includes data that is collected on behalf of VCU.

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

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.

Controlled Unclassified Information (CUI)
Information from federal agencies that requires the protection delineated under the NIST SP800-171 standards. These types of information typically are received as a part of a research project, and are

required through the Federal Acquisition Regulation clauses. Although dubious at the moment, the U.S. National Archive is made the authoritative source for the definition of CUI, and the list of potentially covered information can be found at the National Archive CUI Registry: https://www.archives.gov/cui/registry/category-list.html.

Criminal Justice Information (CJI)
Information regulated under the FBI Criminal Justice Information Services (CJIS) Security Standard, this includes any information provided by the FBI CJIS necessary for law enforcement and civil agencies to perform their missions including, but are not limited to biometric, identity history, biographic, property, and case / incident history data. Like many other regulations, CJIS Security Standards also carries a transient property, where whether an organization receives the data directly or indirectly from a third party, such data will be regulated by the security standards. The VCU Police Department and certain research projects may have access or store these data.

Data Custodian
An individual or organization in physical or logical possession of data for data stewards. Data custodians are responsible for protecting the data in their possession from unauthorized access, alteration, destruction, or usage and for providing and administering general controls, such as back-up and recovery systems. The data custodians are directly responsible for the physical and logical security of the systems that are under their control.

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

Data Steward
The data steward is a University director or equivalent position who oversees the capture, maintenance and dissemination of data for a particular operation. The data steward is responsible to ensure data quality, develop consistent data definitions, sensitivity classifications, determine data aliases, develop standard calculations and derivations, define security requirements, document all appropriate "business rules" and monitor data quality within the source system and/or data warehouse. The data steward is also responsible for communicating data protection requirements to the data custodian; defining requirements for access to the data.

Data Trustee
Data Trustees will carry out plans and policies to implement guidance from the Data and Information Management Council. Data trustees are high-level employees (e.g., vice presidents, vice provosts, and deans) appointed by and reporting to the President, including but limited to Provost and Senior Vice President of Academic Affairs, Vice President of Finance, Vice President of Administration, Vice President of Research, or Senior Vice President of Health Sciences.

dbGaP (database of Genotypes and Phenotypes)
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.

Export Administration Regulation (EAR)

EAR regulates items designed for commercial purpose but which could have military applications (computers, civilian aircraft, pathogens). It covers both the goods and the technology. The licensing regime encourages balancing competing interests. It balances foreign availability, commercial and research objectives with national security.

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

Federal Information Security Management Act (FISMA)
Federal Information Security Management Act (FISMA) requires the use of the National Institute of Science and Technology (NIST) Special Publication (SP) 800-53 as a common security framework for the management of various information belonging to federal government. The framework outlines the expected security controls for information that are rated at the low, moderate, or high level, where each level requires additional controls to be implemented. This regulation can impact the research projects involving federal government data, or projects that are funded by federal government. The moderate and high level controls are a set of minimal baseline set to handle any data with medium to high sensitivity.

HIPPA Information
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. In order for Health or Medical information to qualify as PHI, the information must be collected from an existing HIPAA covered entity, or is received by a HIPAA covered entity. VCU designates several of its schools and departments as a part of the affiliated covered entity, which allows these organizations to share PHI without the execution of a Business Associate's Agreement. Any health or medical information that meets the HIPAA PHI definition will become PHI once it is sent into these organizations, and any such information coming from these organizations and other covered entities will also be considered as PHI.

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

Information Technology Baseline
An information technology baseline is a set of technical requirements that define the minimum required standard practices. Technology Baselines are used in conjunction with Technology Standards and Policies.

Information Technology Guideline
An information technology guideline is a recommended practice that allows some discretion or leeway in its interpretation, implementation, or use.

Information Technology Standard

An information technology standard is a formal document for an established norm of methods, criteria, and processes for technology subjects.

Information Under Non-disclosure Agreement (NDA)
Information maintained by the University on behalf of a third party individual or organization, where contractual agreement has been made that requires the University to maintain the security and / or privacy of the information, or limits the use and disclosure of this information. This information is regulated under specifically executed contract, and failure to meet obligations may result in breach of contract and potential legal liabilities.

International Traffic in Arms Regulations (ITAR)
The Department of State is responsible for the export and temporary import of defense articles and services governed by 22 U.S.C. 2778 of the Arms Export Control Act ("AECA"; see the AECA Web page) and Executive Order 13637. The International Traffic in Arms Regulations ("ITAR," 22 CFR 120-130) implements the Arms Export Control Act.

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

Payment Card Industry Data Security Standard (PCI-DSS)
Payment Card Industry Data Security Standard is a set of comprehensive requirements for enhancing payment card data security. Compliance with the PCI DSS helps to alleviate vulnerabilities that put cardholder data at risk.

System 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).

Third Party Business Partner
Within the context of this document, a third party business partner is a business entity, which does business with VCU. Some but not all of VCU's third party business partners will be handling VCU information. Some but not all of VCU's third party business partners will be involved in the collection of data on VCU's behalf or the storing, processing, and/or transmitting VCU information.

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 Computer and Network Resources
All Information Technology (IT) resources, including wired and wireless networks, software or applications, servers, appliances, workstations, desktops, laptops, tablets and any mobile devices, that are used by Authorized Individuals in the course of their university responsibilities or are purchased with funding allocated to VCU. Free and open source software or applications used by University employees for the purpose of education, research, patient care or administration that relates to the University's mission and day to day operations are also considered VCU computer and network resources.

Contacts

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

Standard Specifics and Procedures

The following sections include the requirements for this standard.

A. Category III and Category II Information Requirements

The requirements delineated in this section are applicable to VCU information/data that are classified as Category II and III.

1. Disaster Recovery Plan.
All applicable IT systems must have a Disaster Recovery Plan (DRP). System and application owners must collaborate and document all required functionality, including procedures for successful restoration of service. DRPs must address different disaster scenarios, amount of time required for recovery, and resources required for recovery. All DRPs must be reviewed periodically to ensure all plan objectives are achievable. (N7)

2. Unit based Contingency Operations / Emergency Mode Ops / Business Continuity Plan.

System and application owners must collaborate and document all required functionality, including procedures for successful restoration of service. Business Continuity Plans (BCP) must address multiple and diverse disaster scenarios, amount of time required for recovery, and resources required for recovery. All BCPs must be reviewed periodically to ensure plan objectives are achievable. (N9)

3. Periodic testing of backup and recovery.
All Disaster Recovery Plans (DRP) for applicable IT systems must be periodically tested. System and application owners must collaborate and document all deficiencies found during testing. All deficiencies must be addressed in accordance with appropriate remediation plans. (N8)

4. Annual test of Contingency Operations / Business Continuity Plan.
All Contingency Operations / Business Continuity Plans must be tested annually. Acceptable testing methods include the following:

- Tabletop exercise with detailed review of scenarios and associated responses
- Simulated exercise with plan implementation; however, business unit does not suffer an outage
- True outage exercise with business unit shutdown, followed by continuity plan implementation

All deficiencies found during testing must be documented and treated to reflect requirements detailed in contingency operations and business continuity plans. (N11)

B. Category I Information Requirements

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

1. Secure data backup (w/ documented procedures).
All data must be securely backed up per an established schedule. All backed up data must retain its pre-backup security classification and access permissions. All backup, recovery, and security processes must be clearly documented. (G10)

2. Create a secure backup copy of data before movement of equipment.
All data must be securely backed up prior to moving equipment to another location. Backup, recovery, and security processes should be clearly documented prior to any equipment movement. (G11)

3. Periodic tiered data backup is required.
All data must be periodically backed up to a backup tier separate from where it is normally backed up. Data will fall into one of the following default classification tiers:

- **Mission critical data:** Stored on highly available (HA) systems with the ability to quickly recover data in event of a disaster.
- **Supporting data:** Not accessed as frequently as mission critical data, can be stored on normal backup systems with average recovery time.

- **Archived data:** Very rarely accessed and may use inexpensive offline storage for long term archival. (K6)

4. Periodic testing of backup media and restoration is required.
All media containing backup data must be periodically tested to ensure backup data can be properly restored in a disaster recovery scenario. Testing must include select data restoration followed by subsequent inspection and verification of the restored information. Documentation of all test events should be maintained by the system owner. (K8)

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/systems and must also adhere to the requirements listed in the Category I Information Requirements Section.

1. Designate alternative telecommunications services in case of disaster.
Data stewards, data custodians, and system owners must jointly identify mission critical data and systems, in conjunction with related telecommunications services used for daily operations. Alternative data processing locations and telecommunications services must be identified, procured, staged, and annually tested to ensure operational readiness when disaster strikes. Test results must be documented and reviewed, including detailed plans to remediate all shortfalls. Required for FISMA (low+mod). (F24)

2. Emergency Access Procedures.
All emergency data access procedures must include the following:

- Personnel authorized to access data. This list must mirror access authorizations established for non-emergency conditions.
- Complete access transaction accounting. All access transactions must be logged for subsequent business and security reviews.
- Defined authorized access methods. List all authorized alternate access methods for use when normal access channels are unavailable.

Required for HIPPA information. (N10)

3. VCU centrally managed backup.
Systems containing applicable data must utilize the backup solution offered by the University Computer Center for such data. Required for CUI and CFR Title 21 Part 11 (FDA) covered information. (G13)

4. Data Backup Plan and Contingency Operations Procedures.
All system and application owners must develop a plan with associated procedures for accessing and restoring data under DR (disaster recovery) and Emergency Mode conditions. This plan will also document specific timelines for data and service restoration. All associated plans and procedures must be reviewed periodically for accuracy. Data requiring backup must have a complete data backup plan. Plans must include, but are not limited to, the following information:

- Type of backup
  - ☐ Incremental
  - ☐ Differential
  - ☐ Full
  - ☐ Progressive
  - ☐ Continuous Data Protection (CDP)

- Frequency of backup
  - ☐ Daily
  - ☐ Weekly
  - ☐ Monthly
  - ☐ Yearly
  - ☐ Continuous

- Storage location of backup
  - ☐ Onsite
  - ☐ Offsite

- Storage media
  - ☐ Disk
  - ☐ Tape
  - ☐ Additional removable media

- Retention period of backup (regulatory requirements may require increased periods of retention)
  - ☐ D number of days
  - ☐ W number of weeks
  - ☐ Y number of years

- Destruction requirements following retention period
  - ☐ Media reuse may be prohibited
  - ☐ Secure wipe according to United States Department of Defense standard 5220.22-M.

Required by HIPPA, FISMA (mod), CUI, and CFR Title 21 Part 11 (FDA) covered Information (L6, N6)

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**

Revision History

Approval/Revision Date	*Title*
None – New Standard	

FAQs

There are no FAQs associated with this Standard.