Business Partner Security Standard

Responsible Office: Technology Services, Information Security Office
Initial Standard Approved: 03/2016
Current Revision Approved: 06/01/2017

Standard Statement and Purpose

The Business Partner Security Standard contains the information security requirements for the collection, storage, processing, transmission and handling of VCU data/information by third party business partners.

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 2
Definitions 2
Contacts 6
Standard Specifics and Procedures 6
Forms 10
Related Documents 10
Revision History 11
FAQs 11

Who Should Know This Standard

All VCU persons and Business Partners responsible for the processing, storage, transmission, and handing of VCU data/information should read and this Standard and familiarizing themselves with its contents and provisions.

Definitions

Acceptable Use Agreement (AUA)
An Acceptable Use Agreement in general covers the use of information a business partner collects, processes, transmits, or stores on behalf of VCU. If the AUA does not cover security requirements related to the storage, transmission and handling of VCU information, then an additional security agreement(s) should be put in place to ensure information security requirements are clearly communicated and agreed upon.

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.

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 "business associate" is a person or entity that performs certain functions or activities that involve the use or disclosure of protected health information on behalf of, or provides services to, a covered entity. A member of the covered entity's workforce is not a business associate. A covered health care provider, health plan, or health care clearinghouse can be a business associate of another covered entity. The Privacy Rule lists some of the functions or activities, as well as the particular services that make a person or entity a business associate, if the activity or service involves the use or disclosure of protected health information. The types of functions or activities that may make a person or entity a business associate include payment or health care operations activities, as well as other functions or activities regulated by the Administrative Simplification Rules.

Business Associate's Agreement (BAA)
BAA is a mutually executed agreement between a HIPAA covered entity with one of its business partners that may collect, process, transmit, or store data on its behalf.

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.

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 Provider
A Data provider is a third party business partner that is providing its data to VCU. Examples may include Department of Health and Human Services and a private computer contracting with VCU to conduct research.

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.

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.

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.

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.

Contacts

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

Standard Specifics and Procedures

The following section contains the requirements for this Standard.

A. Category II Systems

This section contains the requirements for Category II data/information. This section applies to all third party business partners that collects, processes, transmits, or stores Category II information on behalf of VCU.

1. Formal contract with third party business partner with access to data.
Third party business partners with requirements to access data or collect data on VCU's behalf must execute formal contracts before access is granted. Agreements include, but are not limited to, the following:

- Acceptable Use Agreement with the following minimum components:
  - Data use restrictions
  - Data retention requirements
  - Data transmission requirements
  - Data re-disclosure restrictions or a separate Non-disclosure Agreement

- Data responsibilities
- Data security requirements (N2, N3, N4)

2. Non-disclosure agreement with third party.
Third parties with requirements to collect and / or access VCU information must agree to specific terms related to authorized disclosure of such information. A non-disclosure agreement is

needed with the third party business partner to ensure the privacy and security of this information. (N2)

B. Category I Systems

This section contains the requirements for Category I data/information. Information covered in this section must also abide by the requirements for Category II information. See the Data Classification Standard for information on classifying data. This section applies to all third party business partners that collect, processes, transmits, or stores Category I information on behalf of VCU.

1. Third party must formally accept and agree to abide by governing regulations.
All governing regulations for applicable data must apply to data hosted by third parties. Third parties must agree to abide through formal written acceptance. (O1)

2. Must complete a third party business partner security assessment.
All vendors handling data on behalf of VCU must undergo a formal comprehensive security assessment by the Information Security Office (ISO). Assessment must include, but is not limited to:

- Data security policies and practices
- Infrastructure management architecture
- Change management processes
- Personnel authorization and clearance processes
- Security attestation documents (SOC 1 type II or SOC 2 type II)
- Site and area physical security review (O3)

3. Require annual review of security attestation documents.
Applicable vendor attestation documents such as SOC 1 type II or SOC 2 type II must be submitted to VCU for verification on an annual basis. The Information Security Office must complete the review process with assistance from the VCU Procurement Office and VCU Controller's Office. Deficiencies identified must be remediated as required by the Information Security Office. (O4)

4. Require security vulnerability scan / remediation or review of recent results.
All third party business partners handling applicable data must undergo security vulnerability scans either internally or via an outside vulnerability scanning provider. Written confirmation that scans were conducted and all remediation was completed successfully must be provided to the VCU Information Security Office. Proof of these actions should be provided in the form of an SSAE-16 type report in conjunction with a copy of their current security policy. At a minimum, scans must occur annually, or more frequently as dictated by applicable data security regulations. (O5)

5. Must execute formal data management / acceptable use contract.
All vendors handling applicable data must execute formal data management and acceptable use contracts with VCU. Contracts must include, but are not limited to:

- Data ownership
- Data transmission requirements
- Data storage, retention and deletion
- Data security and privacy
- Data acceptable use
- Liability
- Indemnification
- Termination and return of information (O7)

6. Third party business partner must agree to report security breaches to VCU.
All vendors must define security breach details. All security breach details must be reported to VCU without unreasonable delay. (O8)

7. Must complete security review before external party is given access to data.
All third party data collection and access requests must be reviewed and approved by the Information Security Office in conjunction with the applicable data steward, through the University third party security assessment process. The Information Security Office reviews submitted details and stipulates any additional conditions required prior to approval. (F10)

8. Maintain a list of third party business providers with access to data.
Data stewards have the responsibility to inform the VCU Information Security Office of all third party Business Partners who have access to VCU information and/or who are collecting information on behalf of VCU. VCU Information Security Office in conjunction with VCU Procurement Services are responsible for the maintenance of a list of all third party business partners with access to data and their responsibilities for the data. (O12)

9. Disable vendor access when not in use.
All vendor access must be disabled when not in use. This includes physical access (e.g., keycard systems) and IT accounts (e.g., Active Directory). Vendor access must only be enabled when authorized access is required. System administrators should work with the data stewards and data custodians to address this requirement. (O11)

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 data and must also adhere to the requirements listed in the Category I Systems Section.

1. e-Commerce arrangement agreement with third party business partner
All applicable e-Commerce arrangements with trading partners must have documented agreements. Documentation must include, but is not limited to:

- Commercial terms of use for partners and customers
- Security responsibilities and controls for e-Commerce systems
- Audit terms and requirements

Documentation must be periodically reviewed and updated. This is required by PCI-DSS. (N25)

2. Third party business partner is officially approved by the data provider to handle data.
All third party handling of applicable data must be approved by data provider. Data will not be shared without prior documented approval. This is required for dbGaP, TCGA, and CUI. (O2)

3. Must execute business associate agreements / contracts.
All applicable vendors must execute business associate agreement with VCU. This action can be accomplished via a standalone agreement or by addendum to an existing contract. This requirement is for HIPPA related data. (O6)

4. Periodic assessment of service provider is required.
All service providers with access to applicable data must be periodically assessed. The assessment is a collaborative effort between the department(s) using the service, the VCU Procurement Office, data stewards, the Information Security Office, and units responsible for accreditation and certification. Assessments must include, but are not limited to:

- Service Level Agreement (SLA) terms and performance
- Assurance terms and performance
- Currency and inclusiveness of accreditation documents

Required for PCI-DSS and FISMA (mod). (O9)

5. Third party business partner software development contract for software handling data.
All third party software development that will handle applicable data must be governed by contract. Contracts must include, but are not limited to:

- Licensing details
- Source code ownership
- Intellectual Property (IP) rights
- Expectations on source code quality
  - Adherence to industry standard development methodologies
  - Security expectations
  - Rights and access to audit source code

Required by FISMA (low+mod). (O10)

6. Annual request must be sent to data provider for renewal or termination of data access.
Access to data is exclusively limited to authorized users approved by the data provider. Any sharing of data with any unauthorized personnel is strictly prohibited. Individuals designated as project leads are responsible for the annual request for renewal or termination of data access. Data Custodians and Data Stewards should work collaboratively in address the requirement. Required by dbGaP, TCGA, ITAR and EAR. (Q7)

7. Data cannot be shared with any other party not explicitly approved by data provider.

Documents (electronic or physical) containing data that are signed, must ensure authenticity of the signature. It must contain the following elements: 1) Printed name of signer; 2) Date and time of signature execution; 3) The meaning of the signature (e.g. review, approval, responsibility, or authorship). Required for CFR Title 21 Part 11 (FDA) covered information. (Q8)

8. Business Associate's Agreement / Contract (Addendum)
Third party business partner with requirements to access data must execute a Business Associate's Agreement (BAA) before access is granted. Required by HIPPA. (N1)

9. Memo of Understanding (MOU) required with internal department before providing access.
A MOU must be executed with the internal department outlining the acceptable use of the data, need to know rationale, data access provisioning, de-provisioning, termination of access, ramifications of non-compliance etc. Required by CJI, PCI-DSS, HIPPA, PII of Children Under 13, FISMA (mod), PII of EU Citizens, and Export Control information. (Q2)

D. Exception Request

The Information Security Office on a case-by-case basis evaluates all requests for exception(s) to this policy. Exception requests should be made using the Information Security Exception Request Form found in Information Technology Professionals (ITPros) Intranet – IT Resources - Forms. Authorized access to the IT Pros Intranet can be requested by emailing uccnoc@vcu.edu. The completed exception request form is automatically emailed the authorized unit head listed in the request. After the authorized unit head approves the request, the Information Security Office will provide the secondary review and approval as appropriate. Evaluation criteria for exception include the requirement to which an exception is requested, the sensitivity of the information affected, compensating controls in place to mitigate additional risks, and business processes affected by the exception. The Information Security Office will send the exception request review decision and any additional correspondence to the requestor's and the authoritative unit head's email addresses.

Forms

1. VCU Information Security Standard Exception Form
2. University Third Party Security Assessment Request 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. Records Management Policy
7. Library of Virginia General Schedules

Revision History

Approval/Revision Date	Title
March 2006	Business Associates and Contracted Sites
June 1, 2017	Replaces the Business Associates and Contracted Sites Policy

FAQs

There are no FAQs associated with this Standard.