Application Security Standard

Responsible Office: Technology Services
Initial Standard Approved: 05/22/2017
Current Revision Approved: 05/22/2017

Standard Statement and Purpose

Security measures built into and around applications minimize the likelihood that unauthorized code will be able to manipulate applications to access, modify, or delete sensitive University data. They also minimizes the potential for attackers to further compromise other assets in the University environment. This standard outlines the security requirements for applications designed to handle University information; including both applications developed and / or hosted in house, and those created and / or hosted 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

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

Definitions

Application Owner

An application owner is an employee with the oversight responsibility for the management of an application within an IT system. The application owner is typically not the administrator managing the application, but rather the departmental business manager and sponsor of the application. The application owner holds the authority to provision, de-provision, or modify the application to address specific business needs. Application owner can sometime be system owners, but in certain cases, there may be multiple application owners within an IT system.

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.

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.

Category II Information

All proprietary data 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)*.

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.

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

dbGaP
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.

Data Custodian
The Data Custodians can have both a business and/or technical role, though it is typically considered a business role. The Data custodians are responsible for entering, modifying and maintaining data in the enterprise databases and information systems.

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

Data Steward
Data stewards are appointed by and report to the data trustees. Data stewards have knowledge of and work in accordance with numerous University rules and policies across the institution, including university policies on information security and privacy. Data stewards are essentially Executive Subject Matter Experts (ESMEs) for the business domains under their authority.

Data Trustee
Data Trustees will carry out plans and policies to implement appropriate data management practices as defined by industry regulations, federal and state statues, and University policies and procedures. Data trustees are high-level employees (e.g., vice presidents, vice provosts, and deans) appointed by and reporting to the President, Provost and Senior Vice President of Academic Affairs, Senior Vice President of Finance and Administration or Senior Vice President of Health Sciences.

Developed Applications

Applications which are developed within VCU or by a vendor on behalf of VCU are considered “developed applications”. Vendor supplied prepackaged applications are not considered developed applications. An example of a vendor supplied prepackaged application is Microsoft Office Suite.

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

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

Information Technology Standard
A technology standard is a formal document for an established norm of methods, criteria, and processes for technology subjects.

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.

PPRA regulated information
Protection of Pupil Rights Amendment grants the rights to parents of minors to inspect the instructional material provided by schools or programs funded by Department of Education, and requires written parental consent before a school or program funded by Department of Education collects data from minors including 1) Political affiliations; 2) Mental and psychological problems potentially embarrassing to the student and his/her family; 3)Sex behavior and attitudes; 4)Illegal, anti-social, self-incriminating and demeaning behavior; 5)Critical appraisals of other individuals with whom respondents have close family relationships; 6) Legally recognized privileged or analogous relationships, such as those of lawyers, physicians, and ministers; or 7)Income (other than that required by law to determine eligibility for participation in a program or for receiving financial assistance under such program).

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.

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 Application
Within the context of this document, a University application refers to a computer program designed to handle and / or store University information. Examples of a University application include an application hosted in the University Computer Center or a third party hosted web application managed by a third party, but are used by the University to store, process, and transmit its data.

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.

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
Computer network that is registered to VCU and managed by VCU Technology Services or Technology Services designated personnel.

Contacts

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

Standard Specifics and Procedures

This section contains the requirements of this Standard.

A. General (Category III Information) Requirements

The following requirements apply to all applications regardless of the system and information classification.

1. Use custom error messages that do not reveal unnecessary system information on all publically accessible systems/applications.

Where configurable, all publically accessible systems and applications must use custom error messages that do not disclose sensitive technical information. Custom error messages will be presented to users when they encounter a fault. Messages **must not contain** the following information:

- Database connection strings
- Internal error codes
- Faulting lines
- Server versions
- Application versions
- Private IP addressing and fully qualified domain names
- Passwords
- Usernames (I1)

2. Disable directory browsing feature on web application servers.
Where configurable, all web application servers must disable directory browsing. System and application owners should maintain records of analysis and compliance. (I4)

3. Developed applications must have proper input validation controls.
All developed applications must have proper input validation controls. Application owners should maintain records of analysis and compliance. At a minimum, mitigation techniques must be implemented to prevent the following attack vectors:

- SQL injections
- Buffer overflows
- Cross-site Scripting (XSS) attacks
- Invalid and Un-used HTTP request methods
- Insecure direct object access
- Internal URL access without authentication (I6)

4. Protect applications from session hijacking.
All sessions between applications and users must be secured from session hijacking. Application owners should maintain records of analysis and compliance. (I7)

5. Ensure encrypted authentication.
Where applicable, all systems containing data must encrypt user authentication traffic. Application owners should maintain records of analysis and compliance. (I9)

6. Physical or logical separation of application and database.
All application user interfaces must be logically or physically separated from their respective backend data. Applications and databases must never be co-located on the same logical or

physical server. System and application owners should detail traffic flow between applications and backend data prior to deployment. (I15)

7. Remove any maintenance backdoors for application before deployment.
All maintenance backdoors that allow authentication bypass on systems and applications must be removed prior to production deployment. System and application owners should maintain records of removal as part of the production deployment process. (I3)

8. Ensure source code is not published with application.
Developed applications must not publish source code with applications. System and application owners should maintain records of compliance as part of the production deployment process. (I5)

9. Pre-production and quarterly vulnerability assessment and remediation required for publicly accessible applications.
All public facing applications must undergo a vulnerability assessment and when applicable, a static code review prior to deployment. Subsequently, these applications must undergo quarterly vulnerability scans. All critical and high level vulnerabilities identified must be addressed, with any remediation efforts verified by subsequent code reviews and / or assessments. Reviews should be coordinated by the Information Security Office or a designee. (I11)

10. Ensure developed application follows Application Security baseline.
All developed applications must follow the VCU Application Security baseline. Compliance to the baseline must be verified prior to application deployment. (I14)

11. Remove where applicable, any development / test or custom application accounts before deployment.
All custom application, development, and test accounts on systems and applications must be removed prior to production deployment. System and application owners must maintain records of the accounts used for pre-production assignments. (I2)

B. Category II Information Requirements

The following section delineates the requirements for applications used to transmit, process, or store Category II information. In addition to the requirements in this section, all Category II information must also follow the requirements noted in the General (Category III Information) Requirements.

1. Ensure encrypted session.
All applications must encrypt sessions between applications and users. Data transmitted before, during, and / or after authentication must be encrypted. Application owners should maintain records of analysis and compliance. (I10)

C. Category I Information Requirements

The following section delineates the requirements for Category I information. 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. Source code access must be strictly controlled.
All source code access must be strictly controlled and limited to authorized personnel only. Source code must not reside in the production application environment or be publicly accessible through the Internet. (I13)

2. Pre-production and quarterly vulnerability scan and remediation required for all applications used to transmit, process, or store Category I Information.
All applications, both public facing and internal, must undergo a vulnerability assessment, and where applicable a static code review prior to deployment. Subsequently, these applications must undergo quarterly vulnerability scans. All critical and high-level vulnerabilities identified must be addressed, with any remediation efforts verified by subsequent code reviews or assessments. Reviews should be coordinated by the Information Security Office or designee. (I12)

3. Data integrity controls must be built into applications.
All applications must employ data integrity controls. Application owners should maintain records of analysis and compliance. At a minimum, the following controls must be incorporated into applications:

- Protection against buffer overflows
- Prevent out of order program execution
- Prevent dirty reads, writes
- Validation of system generated data
- Output validation (I8)

D. 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 Information Requirements section.

1. Separation of test, development, and production system.
Development, Test, and Quality Assurance environments must not contain production data. User accounts for Development, Test, and Quality Assurance environments must not exist in the Production environment. All Development, Test, Quality Assurance, and Production domain administrator accounts must be documented and subject to annual audit. Accounts no longer necessary must be suspended. Required for PCI-DSS. (F17)

3. Must provide secure coding training to developers at least annually.
Provide verifiable training and record completion for all developers working on systems designed to process, transmit, or store affected data, training must be conducted at least annually. Required by PCI-DSS. (M18)

E. Exception Request

All requests for exception(s) to this policy are evaluated by the Information Security Office on a case-by-case basis. 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 Authoritative Unit Head listed in the request. After the Authoritative 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 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. **Application Security Baseline**
7. **Password, Authentication and Access Standard**
8. **Business Partner Security Standard**

Revision History

Approval/Revision Date	*Title*
None – New Standard	

FAQs

1. **In section A.8. of this Standard, it is mentioned that the source code cannot be published with the application. However, for certain languages used in the development space, the only way for the application to function is to have the application source code published. Examples of such languages include PHP, Python, ASP, and PowerShell. Does section A.8 apply to these languages?**

   No, interpreted languages such as those referenced in the question are not subject to this requirement, since the publication of the code is necessary for the application to function. However, when constructing an application used to handle sensitive information, the developer should consider using a compiled language (e.g. C# or Java) instead of an interpreted language for added protection against common cyberattacks.

2. **Can I use my VCU assigned personal account as an application account?**
   No, this item is covered in the Password, Authentication and Access Standard. An application account must be unique and dedicated to the application, and cannot be used for other purposes, such as day to day work activities of an individual, or the administration of a system.

3. **This standard covers many aspects of application development and security, but does this only apply to internal applications or does it apply to third party applications as well?**
   This standard applies to applications that are designed and used to handle University information; which includes both applications developed and / or hosted in house and applications developed and / or hosted by a third party business partner. In order to facilitate compliance to this standard and the Business Partner Security Standard for applications developed and / or hosted by business partners, it is imperative for application owners to convey these expectations and requirements to third party business partners before the purchase of any application suites.