

SOUTHSIDE VIRGINIA COMMUNITY COLLEGE INFORMATION TECHNOLOGY SECURITY PLAN

IT Systems Security – *Application Security*

Application Security

Purpose

Application security requirements define the [high-level](#) specifications for securely developing and deploying Commonwealth applications.

Requirements

Each agency ISO is accountable for ensuring the following steps are [documented](#) and [followed](#):

Application Planning:

The SVCC IT Network administrator will be responsible for satisfying the following requirements and maintaining auditable documentation for the same:

1. Data Classification - Data used, processed or stored by the proposed application shall be classified according to the sensitivity of the data.
2. Risk Assessment – If the data classification identifies the system as sensitive, a risk assessment shall be [conducted before](#) development begins and after planning is complete.
3. Security Requirements – Identify and document the security requirements of the application early in the development lifecycle. For a sensitive system, this shall be done after a risk assessment is completed and before development begins.
4. Security Design – Use the results of the Data Classification process to assess and finalize any encryption, authentication and access control, and logging requirements. [When an application is planned to use, process or store sensitive information, agencies must address the following design criteria: \(Jan 2010 Revision\)](#)
 - a. [Secure communications channels shall be established for the transmission of sensitive information.](#)
 - b. [Sensitive information shall not be visibly transmitted between the client and the application. \(i.e. Do not include sensitive information in HTTP GET statements.\)](#)
 - c. [Sensitive information shall not be stored in hidden fields that are part of the application interface.](#)

SOUTHSIDE VIRGINIA COMMUNITY COLLEGE INFORMATION TECHNOLOGY SECURITY PLAN

IT Systems Security – *Application Security*

Application Development

The following requirements represent a minimal set of coding practices, which shall be applied to all applications. The SVCC IT Network administrator will be responsible for satisfying the following requirements and maintaining auditable documentation for the same:

5. Authentication – Application based authentication and authorization shall be performed for access to data that is available through the application but not considered publicly accessible. (Jan 2010 Revision)
6. Session Timeout - Any user sessions created by an application shall have an automatic timeout function set not longer than 30 minutes and less depending on sensitivity and risk. (Jan 2010 Revision)
7. Data storage shall be hosted separately from the application interface (i.e., design two or three tier architectures where possible). (Jan 2010 Revision)
8. Input Validation – All application input shall be validated irrespective of source. Input validation should always consider both expected and unexpected input, and not block input based on arbitrary criteria. (Jan 2010 Revision)
9. Default deny – Application access control shall implement a default deny policy, with access explicitly granted. (Jan 2010 Revision)
10. Principle of Least Privilege – All processing shall be performed with the least set of privileges required.
11. Quality Assurance – Internal testing shall include at least one of the following: penetration testing, fuzz testing, or a source code auditing technique. Third party source code auditing and/or penetration testing should be conducted commensurate with sensitivity and risk.

SOUTHSIDE VIRGINIA COMMUNITY COLLEGE INFORMATION TECHNOLOGY SECURITY PLAN

IT Systems Security – *Application Security*

Note: Source code auditing techniques include, but are not limited to: (Jan 2010 Revision)

- a. Manual code review can identify vulnerabilities as well as functional flaws, but most agencies do not have the skilled security resources or time available within the software life cycle that a manual code review requires, and therefore many agencies who decide to perform manual code reviews can only analyze a small portion of their applications.
 - b. Application penetration testing tries to identify vulnerabilities in software by launching as many known attack techniques as possible on likely access points in an attempt to bring down the application or the entire system.
 - c. Automated source code analysis tools make the process of manual code review more efficient, affordable, and achievable. This technique of code audit results in significant reduction of analysis time, actionable metrics, significant cost savings, and can be integrated into all points of the development life cycle.
12. Configure applications to clear the cached data and temporary files upon exit of the application or logoff of the system. (Jan 2010 Revision)

Production and Maintenance

The SVCC IT Network administrator will be responsible for satisfying the following requirements and maintaining auditable documentation for the same:

13. Production applications shall be hosted on servers compliant with the Commonwealth Security requirements for IT system hardening.
14. Applications classified as sensitive shall have at a minimum; a quarterly vulnerability scan run against the applications and supporting server infrastructure, and when any significant change to the environment or application has been made. Any remotely exploitable vulnerability shall be remediated immediately. Other vulnerabilities should be remediated without undue delay. (Jan 2010 Revision)

43 **Note:** The Code of Virginia § 2.2-3803 (B) requires every public body in the COV that has an Internet website to develop an Internet privacy policy and an Internet privacy policy statement that explains the policy to the public and is consistent with the

**SOUTHSIDE VIRGINIA COMMUNITY COLLEGE
INFORMATION TECHNOLOGY
SECURITY PLAN**

IT Systems Security – *Application Security*

requirements of the Code and is displayed on the public body's website in a conspicuous manner. (Jan 2010 Revision)