

Virginia State University
Policies Manual

Title: Systems Security Plan and Systems Operability Agreement Policy

Policy: 6160

Purpose

This policy reflects the University's commitment to document information security controls, to develop Systems Security Plans and Systems Interoperability Agreements, as necessary and required, and to ensure and demonstrate responsibilities for adequate protection of IT system against IT security risks.

Authority, Responsibilities and Duties

1. These roles and responsibilities are assigned to individuals and may differ from the actual role or working title of the individual's position. Individuals may be assigned multiple roles, as long as, the multiple role assignments provide adequate separation of duties, provide adequate protection against the possibility of fraud, and do not lead to a conflict of interests. Refer to Information Security Policy 6110 for roles and responsibilities.

A. System Owner

The System Owner of each VSU Application System classified as sensitive shall:

1. Use the results of the Business Impact Assessment (BIA) and Risk Assessment (RA) of the System as primary inputs to develop a formal System Security Plan for the IT system that includes a description of:
 - a. All existing and planned security controls for the system, including a schedule for implementation of planned controls.
 - b. How those controls provide adequate mitigation of risk to which the system is subject.
2. Conduct an annual review to determine the continued validity of the System Security Plan for each system.
3. Independent audit conducted by Internal Audit or an independent firm on the system every three (3) years.
4. Update the System Security Plan for each system owned as needed as the environment changes.
5. Plan for and document additional IT security controls for the IT system if the University President, ISO, or CIO disapprove of the IT System Security Plan, and resubmit the IT System Security Plan to the University President, ISO, and CIO for approval.
6. Update the IT System Security Plan every three years or more often if necessary, and resubmit the IT System Security Plan to the designated VSU ISO for approval.
7. For the IT systems that share data, Systems Owners will also:
 - a. Specify and document all IT systems which data is shared
 - b. System owners of each system will inform one another regarding other IT systems with which their IT systems interconnect or share data, and inform one another prior to establishing any additional interconnections or data sharing.
 - c. Specify that the data and connection be managed through managed interfaces.

Virginia State University
Policies Manual

Title: Systems Security Plan and Systems Operability Agreement Policy Policy: 6160

- d. Develop written agreement that clearly delineates security requirements for each such Interconnected system and for each type of data shared, and
- e. Specify the Data owner's authority to approve access to the shared data.

8. For systems that share sensitive data with Non-Commonwealth of Virginia systems, the following additional documentation must be kept:

- a. The type of data being shared and the flow of same;
- b. Contact information for the organization that owns the IT system with which data is shared, including the System Owner, the Information Security Officer (ISO), or equivalent, and the System Administrator;

B. Data Owners

Data Owners maintain authority to approve access to the shared data.

C. VSU Information Security Officer

VSU ISO will establish a process to receive, review, and approve or disapprove systems security plans and systems interoperability agreements.

Definitions

The IT security definitions and terms can be found in the Commonwealth of Virginia (COV) Information Technology Resource Management (ITRM) Glossary. It is referenced on the ITRM Policies, Standards, and Guidelines web page on www.vita.virginia.gov/library.

Policy Statement

It is the policy of the VSU that System Security Plans and Interoperability Agreements for all sensitive IT systems will be based on the results of the risk assessments and will meet the requirements in the COV Information Security Guidelines (SEC501). Risk assessments are to be conducted and updated as sensitive IT systems progress through the system development lifecycle (SDLC), for example between the phases of development and before the production phase.

A. System Security Plans- at a minimum will include:

1. The plan documentation shall include a description of:
 - A. All IT existing and planned IT security controls for the IT system, including a schedule for implementing planned controls; and
 - b. How these controls provide adequate mitigation of risks to which the IT system is subject.
2. The plan must be submitted to the VSU ISO for review and approval.
 - a. If the ISO disapproves the plan, additional IT security controls will be planned and documented for the IT system.

Virginia State University
Policies Manual

Title: Systems Security Plan and Systems Operability Agreement Policy Policy: 6160

- b. The updated plan will be re-submitted for approval.
3. The plan must be reviewed and updated every three years or more often if necessary, and resubmitted to the ISO for approval.

B. System Interoperability Agreements- at a minimum will include:

1. For every VSU-owned sensitive IT system, the University shall require that the VSU system owners or VSU service provider specify and document all IT systems with which data is shared.
2. This documentation, in the form of a written agreement shall include:
 - a. The types of shared data;
 - b. The direction(s) of data flow,
 - c. Contact information for the organization that owns the IT system with which data is shared, including the System Owner, the Information Security Officer (ISO), or equivalent, and the System Administrator.
 - d. If and how the shared data will be stored on each IT system.
3. The written agreement shall also specify that System Owners of the IT systems that share data acknowledge and agree to abide by any legal requirements (i.e., HIPAA) regarding handling, protection, and disclosure of the shared data, including but not limited to Data Breach requirements.
4. The System Owners of interconnected systems must notify each other prior to establishing connections to other systems.
5. The written agreement shall specify if and how the shared data will be stored on each IT System.
6. The written agreement shall identify each Data Owner's authority to approve access to the shared data and the System Owners responsibility to approve and enforce the agreement.

C. Exceptions to this Policy

Exceptions to this policy will require a documented request that details the business case for the exception, specifically what requirement the exception is for, and what mitigating controls will be implemented to protect the University. Refer to Information Security Policy 6110 for the requirements and process to file an exception.

D. Violations of Policy

Violation of this policy may result in disciplinary action under the Virginia Department of Human Resources Policy 1.60, Standards of Conduct (4116/08, 6/1111).

Virginia State University
Policies Manual

Title: Systems Security Plan and Systems Operability Agreement Policy


Policy: 6160

References

Virginia Information Technology Agency (VITA):
Information Security Standard (SEC 501-09) (02/20/2015)

Virginia Information Technology Agency (VITA):
IT Security Audit Standard (SEC 502-02.2) (01/06/2013)

Approval By: _____


President

Date: _____

5/10/16