Purpose

The University is committed to upholding the integrity of its Information Technology Environment. As such, the University will continuously assess its IT architectural structure to ensure that weaknesses are located and corrected as the pace of technology continues to change.

Authority, Responsibility, and Duties

The IT Security Program roles and responsibilities are assigned to individuals, and may differ from the actual role title 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 interest.

A. Chief Information Security Officer (CIO)

The CIO is responsible for ensuring that technology on campus is assessed for potential threats and provides management innovative solutions that protect university data and technology assets.

B. Technology Services Team

Assists management on staying abreast of technology advancement, constantly monitors the control environment, and identifies potential weaknesses.

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.

General Requirements

The University will:

a. Authorize connections from the information system to other information systems through the use of Interconnection Security Agreements;

b. Document, for each interconnection, the interface characteristics, security requirements, and the nature of the information communicated; and

c. Review and update Interconnection Security Agreements an annual basis or more frequently if required to address an environmental change

d. Ensure that System Owners, in consultation with the Data Owner, document IT systems with which data is shared. This documentation must include:

   1. The types of shared data; b. The direction(s) of data flow; and

   2. 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.

e. Ensure that System Owners of interconnected systems inform one another of connections with other systems.

f. Ensure that System Owners of interconnected systems notify each other prior to establishing connections to other systems.

g. Provide the written agreement that specifies if and how the shared data will be stored on each IT system.

h. Provide the written agreement that specifies that System Owners of the IT systems 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 in this Standard.

i. Provide the written agreement which specifies each Data Owner's authority to approve access to the shared data.

j. Ensure that System Owners approve and enforce the written agreements.

k. Assign a senior-level executive or manager as the authorizing official for the information system;

l. Ensure that the authorizing official authorizes the information system for processing before commencing operations;

m. Update the security authorization on an annual basis or more frequently if required to address an environmental change.

n. Continuous monitor strategy and implement a continuous monitoring program that includes:

   1. Establishment of organization-defined metrics to be monitored;
   2. Establishment of organization-defined frequencies for monitoring and organization-defined frequencies for assessments supporting such monitoring;
   3. Ongoing security control assessments in accordance with the organizational continuous monitoring strategy;
   4. Ongoing security status monitoring of organization-defined metrics in accordance with the organizational continuous monitoring strategy;
   5. Correlation and analysis of security-related information generated by assessments and monitoring;
   6. Response actions to address results of the analysis of security-related information; and
   7. Reporting the security status of organization and the information system to appropriate organizational officials at least every 120-days

References

Virginia Information Technology Agency (VITA):
Information Security Standards (SEC501-09) (05/01/2015)
IT Systems Security Guideline (SEC515-00) (07/17/2008)

Library of Virginia Records Retention and Disposition Schedule for Administrative Records GS-101 located at: http://www.lva.virginia.gov/agencies/records/sched_state/GS-101.pdf

Library of Virginia Records Retention and Disposition Schedule for State Agencies: College and University located at: http://www.lva.virginia.gov/agencies/records/sched_state/GS-111.pdf

Approval By: ________________________________ **Date: 10/4/17**
President