Purpose

This policy reflects Virginia State University's (VSU) commitment to define steps to identify, analyze, prioritize, and mitigate risks that could compromise VSU's IT systems and data. It reflects VSU's commitment to select and implement security measures to reduce the risks to its information systems containing sensitive information to a reasonable and appropriate level. It further classifies all IT systems and data according to sensitivity for confidentiality, integrity and availability.

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 interests. Refer to Information Security Policy 6110 for roles and responsibilities.

A. VSU lnformation Security Officer (ISO)

1. The VSU ISO shall
    a. In collaboration with system owners and data owners, conduct and document Risk Assessment (RAs) of each university-owned sensitive IT system every 3 years or as needed depending on changes to the system or environment.
    b. Conduct and document an annual self-assessment to determine continued of validity of Risk Assessment.
    c. Prepare an executive level report on each Risk Assessment including major findings and risk mitigation recommendations and distribute the report to the appropriate personnel.

2. The VSU ISO will also verify that all systems have been reviewed and classified as appropriate for sensitivity, obtain University President approval, and communicate approved IT system and data classifications to Systems Owners, Data owners and end-users.

3. VSU ISO will also ensure that controls are in place to prohibit posting any data classified as sensitive with respect to confidentiality on the University's public website, File Transfer Protocol (ftp) servers, drive shares, bulletin boards or any other publically accessible medium unless a written exception identifying the business case, risks, mitigating controls and all residual risks is approved by the University President.

B. Data Owners

Data Owner must identify the types of data handled by each IT system they are responsible for and will also determine whether each type of data is subject to additional regulatory

Requirements. They must also determine the potential damages to the University that comprise Of confidentiality, integrity, or availability of each type of data handled by the IT system, classify the sensitivity of the data accordingly and use that information to inform the Risk Assessment processes.

C. Systems Owners

Systems Owners, as the University business managers responsible for having an information system operated and maintained in support of (essential) business functions for which they are accountable, will actively participate in the process to classify all IT systems and data according to their sensitivity for confidentiality, integrity and availability. Additional responsibilities include:

1. Classify their IT applications annually.
2. Review Risk Assessment policy and procedures annually (or more if required to address changes/modifications to the sensitive applications)
3. Perform at least every three years a Risk Assessment for each sensitive application.
4. Determine the vulnerabilities for each of their sensitive applications.
5. Ensure (require) that vulnerability scans are run against applications and supporting server infrastructure quarterly and when significant change to the environment or application have been made as part of continuing Risk Assessment efforts.

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.viwinia.gov/librarv.

Policy Statements

This policy applies to all University employees (permanent, temporary, contractual, faculty, administrators and students) who use VSU information technology resources to conduct University business and to transmit sensitive data or personally identifiable information (PIT) in the performance of their jobs, and all VSU information systems that store or process PII or other sensitive data.

1. It is the policy of the University that the information Risk Management program is established to determine risks to sensitive VSU IT systems, prioritize those risks, and plan and respond to those risks that could result in material or significant negative impacts on essential business functions and the mission of the University. The VSU information risk management program elements addressed in this policy include IT System and Data Sensitivity Classification, and Risk Assessment (RA).

2. IT Systems and Data Classification- all systems will be classified with respect to

a. Confidentiality- to address sensitivity to unauthorized disclosure;
b. Integrity- to address sensitivity to unauthorized modification; and
c. Availability- to address sensitivity to outages (unavailability).

3. The following steps are necessary to classify data sensitivity:
   a. Identify type(s) of data handled by each IT application;
   b. Determine whether each type of data is also subject to other regulatory requirements;
   c. Determine potential damages to University from a compromise of confidentiality, integrity, or availability of each type of data handled by the IT application and classify sensitivity of the data accordingly;
   d. Classify IT application as sensitive if any type of data it processes has a sensitivity of high for confidentiality, integrity, or availability; and
   e. Classify IT system as sensitive if any sensitive University IT applications or type of data processed by it has a sensitivity of high for confidentiality, integrity, or availability.

4. Risk Assessment steps shall include:
   a. Identify potential threats to each IT application, IT infrastructure, and environment in which it operates;
   b. Assess the likelihood that threats shall materialize;
   c. Identify and evaluate vulnerabilities;
   d. Determine potential risk treatments (avoidance, reduction, retention, transfer);
   e. Determine loss impact if one or more vulnerabilities are exploited by a potential threat;
   f. Develop risk treatment plans;
   g. Implement mitigation (plans) strategy; and
   h. Review and evaluate.

5. 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.

6. 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).

References

Virginia Department of Human Resources Management:
Policy 1.60 Standards of Conduct (4116/08, 6/1111)
Policy 1.75 Uses of Electronic Communication and Social Media (8/01101, 3117/11)

Virginia Information Technology Agency (VITA):
Information Security Standards (SEC501-09) (02/20/2015)
IT Security Audit Standard (SEC502-02.2) (01/06/2013)
IT Systems Security Guideline (SEC515-00) (07117/2008)
IT Risk Management Standard (SEC520-00) 02112/2014

NIST Special Publications

- Recommend Security Controls for Federal Information Systems and Organizations SP 800-53
- Information Security Handbook: A Guide for Managers SP 800-100.

Approval By: _____ Date: 5/10/16
President