Purpose

The University recognizes its responsibility to use its IT resources in an efficient and effective manner. As such, the Technology Service management is responsible for assessing IT risk across the University. This policy provides structure and consistency to the risk assessment process and reflects the University's commitment to fulfill its responsibilities in assessing and mitigating IT system risks.

Authority, Responsibilities, Duties and Scope

This policy applies to all University employees (permanent, temporary, contractual, faculty, administrators and students) who use VSU information technology resources to conduct University business.

These 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.

A. Chief Information Officer (CIO)

The CIO will give the ISO direction to ensure the criteria and methodology to evaluate the University's IT risk is based on sound business practices.

B. Information Security Officer (ISO)

The ISO will identify all information technology processes and assess risk accordingly. The Risk Assessment methodology used by the ISO will assist the University in understanding its information technology risk and understand the impact to the University's business. This risk assessment data should feed into the university business impact analysis (BIA). It is the ISO responsibility to ensure that the risk assessment is updated as needed and reviewed annually. The ISO will collaborate with the CIO to establish the appropriate risk assessment criteria to assess the University IT risk.

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 Statements

The University will:

a. Categorize information and the information system in accordance with applicable Commonwealth laws, Executive Orders, directives, policies, regulations, standards, and guidance;
b. Document the security categorization results (including supporting rationale) in the security plan for the information system;
c. Ensure that the security categorization decision is reviewed and approved by the authorizing official or authorizing official designated representative.
d. Conduct an assessment of risk, including the likelihood and magnitude of harm, from the unauthorized access, use, disclosure, disruption, modification, or destruction of the information system and the information it processes, stores, or transmits**;**
e. Document risk assessment results in a Risk Assessment Report;
f. Review risk assessment results on an annual basis or more frequently if required to address an environmental change;
g. Disseminate risk assessment results to the appropriate organization-defined personnel;
h. Update the risk assessment on an annual basis or whenever there are significant changes to the information system or environment of operation (including the identification of new threats and vulnerabilities), or other conditions that may impact the security state of the system.
i. Scan for vulnerabilities in the information system and hosted applications at least once every 90-days for publicly facing systems and when new vulnerabilities potentially affecting the system/applications are identified and reported;
j. Employ vulnerability scanning tools and techniques that facilitate interoperability among tools and automate parts of the vulnerability management process by using standards for:
    1. Enumerating platforms, software flaws, and improper configurations; Formatting checklists and test procedures; and
    2. Measuring vulnerability impact;
k. Analyze vulnerability scan reports and results from security control assessments;
l. Remediate legitimate vulnerabilities within 90-days in accordance with an organizational assessment of risk; and
m. Share information obtained from the vulnerability scanning process and security control assessments with the appropriate organization-defined personnel to help eliminate similar vulnerabilities in other information systems (i.e., systemic weaknesses or deficiencies).

References

Virginia Information Technology Agency (VITA):
Information Security Standards (SEC501-09.1) 12/08/2016)

Approval By: _____ **Date:** ____9/6/17_____

President