Purpose

The University acknowledges its responsibility to protect its information technology resources and environment whether information is on site, in-transit or hosted off-site. As such, this policy provides the overarching methodology to safeguard the university's information technology acquisition processes.

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 Technology Service Team direct to ensure the criteria and methodology to protect university systems and data are both valid and feasible.

B. Information Security Officer (ISO)

The ISO will identify all information technology processes designed to protect systems and data and ensure that procedures maintain appropriate levels of security to maintain system and data integrity.

C. Enterprise Manager

The Enterprise Manager is responsible for ensuring that the enterprise management team is trained and educated on the details of the Physical and Environmental Protection Policy and Procedure to ensure that the process is fully understood and implemented.

D. Applications Team

The Applications team is responsible for providing their expertise in what is required for functionality, maintenance and testing of potentially acquired software applications. The applications team will need to make assignments of system ownership when a new system is acquired.

E. Project Management Team

The Project Management Team is responsible for ensuring that the project management process includes controls to safeguard the acquisition process and align with the "System and Services Acquisition Process Policy" and the University's Project Management Policies and Procedures.

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

A. Allocation of Resources

The ISO and security team will:

a. Determine information security requirements for the information system or information system service in mission/business process planning; and
b. Determine, document, and allocate the resources required to protect the information system or information system service as part of its capital planning and investment control process;

B. Life Cycle Support

The Applications team and the Project Management team will (as specified in SEC525-02; SA-3-COV-1 and SA-3-COV-2):

a. Manage the information system using system development life cycle methodology that incorporates information security considerations;
b. Define and documents information security roles and responsibilities throughout the system development life cycle;
c. Identify individuals having information security roles and responsibilities; and
d. Integrate the organizational information security risk management process into system development life cycle activities.

C. Acquisitions

The CIO and the Technology Services team will:

a. Include the following requirements, descriptions, and criteria, explicitly or by reference, in the acquisition contract for the information system, system component, or information system service in accordance with applicable commonwealth laws, Executive Orders, directives, policies, regulations, standards, guidelines, and organizational mission/business needs:

   i. Security functional requirements;
   ii. Security strength requirements;
   iii. Security assurance requirements;
   iv. Security-related documentation requirements;
   v. Requirements for protecting security-related documentation;
   vi. Description of the information system development environment and environment in which the system is intended to operate; and
   vii. Acceptance criteria.

b. Limit the use of commercially provided information assurance (IA) and IA-enabled information technology products to those products that have been successfully evaluated against Commonwealth security processed and standards; and

c. Requires, if no Commonwealth approved Protection Profile exists for a specific technology type but a commercially provided information technology product relies on cryptographic functionality to enforce its security policy, that the cryptographic module is FIPS-validated.

D. Information Systems Documentation

The Technology Services team will:

a. Obtain administrator documentation for the information system, system component, or information system service that describes:
   1) Secure configuration, installation, and operation of the system, component, or service;
   2) Effective use and maintenance of security functions/mechanisms; and
   3) Known vulnerabilities regarding configuration and use of administrative (i.e., privileged) functions;

b. Obtains user documentation for the information system, system component, or information system service that describes:
   1) User-accessible security functions/mechanisms and how to effectively use those security functions/mechanisms;
   2) Methods for user interaction, which enables individuals to use the system, component, or service in a more secure manner; and
   3) User responsibilities in maintaining the security of the system, component, or service;

c. Document attempts to obtain information system, system component, or information system service documentation when such documentation is either unavailable or nonexistent and implements the appropriate organization-defined actions in response;

d. Protect documentation as required, in accordance with the risk management strategy; and

e. Distribute documentation to the appropriate organization-defined personnel.

f. Require the use of only agency approved software and service provider approved systems management software on IT systems.

g. Assess periodically whether all software is used in accordance with license agreements.

E. Security Engineering Principles

The Technology Services team will apply information system security engineering principles in the specification, design, development, implementation, and modification of the information system. For example:

i. Developing layered protections;
ii. Establishing sound security policy, architecture, and controls as the foundation for design;
iii. Incorporating security requirements into the system development life cycle;
iv. Delineating physical and logical security boundaries;
v. Ensuring that system developers are trained on how to build secure software;
vi. Tailoring security controls to meet organizational and operational needs;
vii. Performing threat modeling to identify use cases, threat agents, attack vectors, and attack patterns as well as compensating controls and design patterns needed to mitigate risk; and
viii. Reducing risk to acceptable levels, thus enabling informed risk management decisions.

F. External Information System Services

The Technology Services team will:

a. Require that providers of external information system services comply with organizational information security requirements and employ appropriate security controls in accordance with applicable Commonwealth laws, Executive Orders, directives, policies, regulations, standards, and guidance;
b. Define and documents government oversight and user roles and responsibilities with regard to external information system services; and
c. Employ appropriate processes, methods, and techniques to monitor security control compliance by external service providers on an ongoing basis.
d. Establish the exact geographically location of all data if not stored within the Commonwealth. The Commonwealth will define the parameters and costs for data location options prior to making any contractual commitments.
e. Confirm the exact geographically location of the sensitive data on a monthly basis and report the location to the appropriate regulatory authority every 90 days.
f. Establish a Data Escrow policy to address the data recovery process in case of system failure or facility issues and ensure all copies of data are returned to the Commonwealth at the end of contract.
g. Establish a validated copy of any data elements classified as sensitive with respect to integrity or availability or are considered components in a system of record for the Commonwealth. The validated copy must be stored within a secured environment maintained by the Commonwealth.
h. Perform an annual security audit of the environment or review the annual audit report of the environment conducted by an independent, third-party audit firm on an annual basis
i. Perform a monthly review of activity logs related to the operation of the service. At a minimum, the activity review must include the access time and action of each individual using the system during the review period.
j. Receive reports from the vendor on vulnerability scans of the operating system and supporting software at least once every 90-days
k. Ensure that the vendor conduct an independent vulnerability scan of the service at least once every 90-days and provide the results to Agency within 10-business days
l. Submit a summary of all findings from the monthly activity log review once every 90-days to the appropriate regulatory authority
m. Submit the vulnerability scan information within 30-days of receipt from the vendor to the appropriate regulatory authority
n. Submit the results from the Data Owning Agency vulnerability scan of the service within 30 days of scan completion.

G. Developer Configuration Management

The Project Management team and Applications team will:

a. Perform configuration management during information system design, development, implementation, and operation;
b. Document, manage, and control the integrity of changes to the configuration items under configuration management;
c. Implement only organization-approved changes to the system, component, or service;
d. Document approved changes to the system, component, or service and the potential security impacts of such changes; and
e. Track security flaws and flaw resolution within the system, component, or service and report findings to the appropriate organization-defined personnel.

H. Developer Security Testing

The Applications and Project Management teams will:

a. Create and implement a security assessment plan;
b. Perform unit, integration, system, and regression testing/evaluation at the appropriate depth and coverage;
c. Produce evidence of the execution of the security assessment plan and the results of the security testing/evaluation;
d. Implement a verifiable flaw remediation process; and
e. Correct flaws identified during security testing/evaluation.

I. Development Process, Standards & Tools

The CIO and Applications Manager will:

a. Require the developer of the information system, system component, or information system service to follow a documented development process that:
    1) Explicitly addresses security requirements;
    2) Identifies the standards and tools used in the development process;
    3) Documents the specific tool options and tool configurations used in the development process; and
    4) Documents, manages, and ensures the integrity of changes to the process and/or tools used in development
b. Review the development process, standards, tools, and tool options/configurations on an annual basis or more frequently if required to address an environmental change to determine if the process, standards, tools, and tool options/configurations selected and employed can satisfy organization-defined security requirements.

J. Developer-Provided Training

The University requires the developer (or trainer) of the information system, system component, or information system service to provide organization-defined training on the correct use and operation of the implemented security functions, controls, and/or mechanisms.

K. Developer Security Architecture and Design

The University requires the developer (or trainer) of the information system, system component, or information system service to produce a design specification and security architecture that:

a. Is consistent with and supportive of the University’s security architecture which is established within and is an integrated part of the University’s enterprise architecture;
b. Accurately and completely describes the required security functionality, and the allocation of security controls among physical and logical components; and
c. Expresses how individual security functions, mechanisms, and services work together to provide required security capabilities and a unified approach to protection.

L. Unsupported System Components

The Technology Services Team will:

a. Replace information system components when support for the components is no longer available from the developer, vendor, or manufacturer; and
b. Provide justification and documents approval for the continued use of unsupported system components required to satisfy mission/business needs.

References

Virginia Information Technology Agency (VITA):
Information Security Standards (SEC501-09.1) (12/08/2016)
Hosted Environment Information Security Standard (SEC525-02) (12/08/2016)

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