Virginia State University
Policies Manual

Title: IT Security Plan Policy Policy: 6150

Purpose

The University recognizes its responsibility to safeguard the Information Technology and data it collects and maintains. As such, the University is responsible for ensuring that a plan to protect these assets is consistently implemented and maintain for all platforms. This policy reflects the University's commitment to fulfill its obligation to list and mark the boundaries of all its sensitive IT systems in order to provide cost-effective, risk-based security protections for its IT systems.

Authority, Responsibilities and Duties

This Sensitive IT Systems Inventory and Definition 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. Refer to Information Security Policy 6110 for roles and responsibilities.

A. Data Owners

Data Owner must identify the types of data handled by each IT system that he/she is assigned, determine the regulatory requirements for each data type, and determine the potential damages to the University if data is compromised. The data must also be classified according to the sensitivity (i.e. confidentiality, integrity, and availability). This information will be used in the development and continuous assessment of the risks surrounding the data.

B. Systems Owners

Systems Owners, as well as, the University business managers are responsible for having an information system operated and maintained in support of business functions for which they are accountable, and will participate in the process to list and mark the boundaries of all their IT systems.

C. Information Security Officer (ISO)

The ISO will verify that all sensitive systems are listed, system boundaries are marked and have been reviewed and classified as appropriate for sensitivity, and obtain University President approval. The approved Sensitive IT Systems Inventory and Definitions and data classifications will be communicated to the Systems Owners, Data owners, Data Custodians, and end-users.

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

1. The University is committed to developing and maintaining a security plan (based on a risk assessment) that:
    a. Is consistent with the organization's enterprise architecture;
    b. Explicitly defines the authorization boundary for the system;
    c. Describes the operational context of the information system in terms of missions and business processes;
    d. Provides the security categorization of the information system including supporting rationale;
    e. Describes the operational environment for the information system and relationships with or connections to other information systems;
    f. Provides an overview of the security requirements for the system;
    g. Identifies any relevant overlays, if applicable;
    h. Describes the security controls in place or planned for meeting those requirements including a rationale for the tailoring and supplementation decisions; and
    i. Is reviewed and approved by the authorizing official or designated representative prior to plan implementation;
    j. Distributes copies of the security plan and communicates subsequent changes to the plan to the appropriate organization-defined personnel;
    k. Reviews the security plan for the information system on an annual basis or more frequently if required to address an environmental change;
    l. Updates the plan to address changes to the information system/environment of operation or problems identified during plan implementation or security control assessments; and
    m. Protects the security plan from unauthorized disclosure and modification.
    n. Includes documentation of the adoption and user agreement to the use policy. Executive branch agencies must adhere to Virginia Department of Human Resource Management (DHRM) Policy 1.75 – Use of Electronic Communications and Social Media.

2. Users are prohibited from:
    a. Installing or using proprietary encryption hardware/software on Commonwealth systems;
    b. Tampering with security controls configured on COV workstations;
    c. Installing personal software on a Commonwealth system;
    d. Adding hardware to, removing hardware from, or modifying hardware on a COV system;
    e. Connecting non-COV-owned devices to a COV IT system or network, such as personal computers, laptops, or hand held devices, except in accordance with the current version of the Use of non-Commonwealth

Computing Devices to Telework Standard (COV ITRM Standard SEC511). Violations of Policy; and

f. The storage, use or transmission of copyrighted and licensed materials on COV systems unless the COV owns the materials or COV has otherwise complied with licensing and copyright laws governing the materials.

3. Violation of this policy may result in disciplinary action under the Virginia Department of Human Resources Policy 1.60, Standards of Conduct (4/16/08, 6/1/11)

4. 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 confidentiality, integrity and availability of the Active Directory environment. Refer to Information Security Policy 6110 for the requirements and process to file an exception.

References

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

Approval By: ______________________________ **Date:** 9/6/17
President