**Purpose**

This Sensitive IT Systems Inventory and Definition 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 and the University. The purpose of this policy is to ensure that VSU will list and mark the boundaries of all its IT systems that contain sensitive data.

**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.

1. 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. System Owners**

Systems Owners or their designees are responsible for having an information system operated and maintained in support of business functions for which they are accountable.

**B. Data Owners**

Data Owners must:

1. Identify the types of data handled by each IT system that he/she is responsible for
2. Determine the regulatory requirements for each data type,
3. Determine the potential damages to the University if data is compromised.
4. Classify the data according to the sensitivity:
    - Confidentiality- addresses sensitivity to unauthorized disclosure
    - Integrity- addresses sensitivity to unauthorized modifications
    - Availability - addresses sensitivity to outages

    This information will be used in the development and continuous assessment of the risks surrounding the data.
5. Validate that all systems have been reviewed and classified properly
6. Review IT system and data classifications with the System Owners or designee for final approval.
7. Ensure that no sensitive system is posted on a public website, stored on an ftp server, bulletin board or drive share without the written permission of the System Owner.

**C. University Executives and Senior Management**

University Executives and Senior Management in Academic and Business units of the University are responsible for and must participate in the development of the University's Sensitive IT Systems Inventory and Definition policy based on the Business Impact Analysis. These individuals are also responsible for approving the final Sensitivity IT System Inventory.

**Roles and Responsibilities**

The VSU ISO will:

1. Identify or assign the Data Owner the responsibility of identifying the types of data Owned and managed for each IT system
2. 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. Document each sensitive IT system owned including its ownership and boundaries.
    a. Update documentation as changes occur.
    b. Maintain updated network diagrams on each sensitive IT system.

2. 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).

3. 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.

Title: Sensitivity IT System Inventory Policy Policy: 6150

**References**

Virginia Information Technology Agency (VITA):
Information Security Standards (SEC501-09, 02/20/2015)
IT Security Audit Standard (SEC502-02.2, 01/06/2013)

NIST Special Publications

Contingency Planning Guide for Information Technology Systems SP 800-34 Revel, 05/2010

Recommend Security Controls for Federal Information Systems and Organizations SP 800-53 A Rev.4

Computer Security Incident Handling Guide SP 800-61 Rev.2 08/2012

Information Security Handbook A Guide for Managers SP 800-100.

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