Virginia State University
Policies Manual

Title: IT Asset Management Policy Policy: 6800

Purpose

This policy reflects VSU's commitment to identify the steps necessary to control and collect information about IT assets and software licenses to protect against the use of computer software in violation of applicable laws.

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 and the IT Asset Management (ITAM) Program for specific asset management roles and responsibilities.

A. Faculty and Staff

Faculty and Staff members are required to adhere to the copyright protection of licensed software and documentation, contact his/her Supervisor, Dean/Director, or departmental Chairperson about departmental software acquisitions and purchases. They are to report any knowledge of unauthorized software use to their direct reports such as departmental Chairperson, Dean/Director, or Director of IT Services.

B. IT Asset Management

Director of IT Services is required to:

1. Establish IT Asset Management policies and procedures to govern the ITAM Program.
2. Assess periodically whether all software is used in accordance with license agreements.
3. Perform wall-to-wall inventory of physical IT assets every two years.
4. Have faculty and staff member complete the Software Approval form for software installation. Once approved, IT Service Desk team will assist in installing software on University IT equipment. Maintain a central location for all original copies of University software, software licensing agreements, and purchasing histories.
5. Maintain a software asset inventory management tool which contains software information such as a software inventory, software usage data, and summary of license compliance status.
6. Conduct periodic software review and maintain detailed records and results to ensure compliance with license agreements.

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

I. It is the policy of VSU that IT Asset Management (ITAM) Program processes and procedures for all University information systems will be consistent with best practices and comply with Commonwealth of Virginia (COV) Information Security Standards (SEC 501) and the ITAM Process Life Cycle as per the Information Technology Infrastructure Library (ITIL) Service Management practices.

2. Effective Asset Management and control will protect IT systems and data by managing the IT assets in a planned, organized, and secure fashion. VSU has adopted the ITAM Program to control and collect information about IT assets to document and implement inventory management processes that, at a minimum;

   A. Identify whether IT assets may be removed from the premises that house IT systems and data and identify and implement controls over such removal.

   B. Identify whether personal IT assets are allowed onto premises that house IT systems and data and identify controls necessary to protect these IT systems and data.

   C. Remove data from assets prior to disposal in accordance with ITRM Standard SEC-514, Removal of Commonwealth Data from Surplus Computer Hard Drives and Electronic Media.

   D. Requires creation and periodic review of a list of agency hardware and software assets.

3. Effective software license management process and procedures include, at a minimum, the following:

   A. *Prohibitions*- Students are not allowed to install, attempt to install, copy, or download any type of software onto University computers, unless the student is in an Academic Computing Lab specifically setup for the purpose of studying an IT related discipline and:

      I. installation of software is required as part of coursework,

      2. There is proof the software license belongs to the University, and

      3. The Lecturer has given his/her authorization.

   D. *Unauthorized Software*

      1. If unlicensed or unapproved software is found on campus, the employee will be requested to uninstall the software.

2. If the request is denied, the Technology Services department has the authority to uninstall any software which violates the practices set forth in this policy, the Acceptable Use Policy, or any federal and state laws.

F. *Data Software Removal*

1. Software licensing agreements must be followed when computer systems, are being surpluses, transferred, disposed of, traded-in, or reassigned within the University.

2. Copies of software and licensing agreements should be turned into the Asset Manager and properly disposed of.

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 (8/01/01, 3117/11)

Virginia Information Technology Agency (VITA):

Information Security Standards (SEC501-07) (1/28/2013)
IT Security Audit Standard (SEC502-02) (12/05/2011)
Removal of Commonwealth Data from Surplus Computer Hard Drives and Electronic Media (SEC514-03, 03/15/2008)

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.

Industry groups –best practices

Information Technology Infrastructure Library (ITIL)
Business Software Alliance (BSA)

Approval By: ______________________________ Date: 5/16/16
President