



OIT 62.1002: IT Asset Control

Responsible Executive: Information Security Officer
Responsible Office: Office of Information Technology
Related Policy:
Approved-On Date: 2/28/2011
Effective Date: 7/1/2011
Revision Date: 2/1/2011

I. Policy Statement

IT Asset Control addresses protection of the components that comprise IT systems by managing them in a planned, organized, and secure fashion.

II. Purpose

The IT Asset Control policy identifies the steps necessary to control and collect information about IT assets.

III. Scope

This policy applies to all Commonwealth of Virginia (COV) systems and to the University IT network infrastructure.

IV. Requirements

Commensurate with sensitivity and risk, the University shall or shall require that its service provider document and implement inventory management practices that address the following components, at a minimum:

1. Identify whether IT assets may be removed from premises that house IT systems and data, and if so, identify the controls over such removal.
2. Identify whether personal IT assets are allowed onto premises that house IT systems and data, and if so, identify the controls necessary to protect these IT systems and data.
3. Remove data from IT assets prior to disposal in accordance with the current version of the Removal of Commonwealth Data from Surplus Computer Hard Drives and Electronic Media Standard (COV ITRM Standard SEC514).
4. Require creation and periodic review of a list of agency hardware and software assets.

V. Violations

Violations of this policy will be addressed in accordance relevant University and Commonwealth of Virginia policies, including University Policy 60.201 and Department of Human Resources Management Policy 1.75. The appropriate level of disciplinary action will be determined on an individual case basis by the appropriate Vice President or designee, with sanctions up to or including termination or expulsion depending upon the severity of the offense.

VI. Interpretation

The Information Security Officer is responsible for official interpretation of this policy. Questions regarding the application of this policy should be directed to the Office of Information Technology. The Information Security Officer reserves the right to revise or eliminate this policy.