



## OIT 62.205: Sensitive IT System Inventory and Definition

**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

Sensitive IT System Inventory and Definition addresses protecting University information and IT systems commensurate with sensitivity and risk, including system availability needs. This is a central component of the University information security program and allows the University to determine how these factors apply to its IT systems and data.

### II. Purpose

The Sensitive IT System Inventory and Definition policy identifies the steps in listing and marking the boundaries of sensitive IT systems in order to provide cost-effective, risk-based security protection for IT systems, for the University as a whole.

### III. Scope

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

### IV. Requirements

The ISO or designated Sensitive System Owner(s) shall:

1. Document each sensitive IT system owned by the University, including its ownership and boundaries, and update the documentation as changes occur.

**Note:** Data and homogenous systems, belonging to the University, that have the same technical controls and account management procedures (i.e., Microsoft SharePoint, or PeopleSoft), may be classified and grouped as a single set of data or systems for the purpose of inventory, data classification, risk assessments, security audits, etc.

**Note:** Where more than one agency may own the IT system, and the agency or agencies cannot reach consensus on which should serve as System Owner for

the purposes of this Policy, upon request, the CIO of the Commonwealth will determine the System Owner.

**Note:** A sensitive IT system may have multiple Data Owners, and/or System Administrators, but must have a single System Owner.

2. Maintain or require that its service provider maintain updated network diagrams.

## **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 executive 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.