



## OIT 62.402: IT System Security Plans

**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 System Security Plans defines the steps necessary to provide adequate and effective protection for University systems.

### II. Purpose

The IT System Security Plans policy documents the security controls required to demonstrate adequate protection of information systems against security risks.

### III. Scope

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

### IV. Requirements

Each System Owner of a sensitive IT system shall:

1. Document an IT System Security Plan for the IT system based on the results of the risk assessment. This documentation shall include a description of:
  - a. All existing and planned security controls for the IT system, including a schedule for implementing planned controls;
  - b. How these controls provide adequate mitigation of risks to which the IT system is subject.
2. Submit the IT System Security Plan to the Agency Head or designated ISO for approval.
3. Plan, document and implement additional security controls for the IT system if the Agency Head or designated ISO disapproves the IT System Security Plan, and resubmit the IT System Security Plan to the Agency Head or designated ISO for approval.

4. Update the IT System Security Plan every three years, or more often if necessary (i.e., due to material change), and resubmit the IT System Security Plan to the Agency Head or designated ISO for approval.

## **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.