



## OIT 62.207: IT Security Audits

**Responsible Executive:** Information Security Officer  
**Responsible Office:** Office of Information Technology  
**Related Policy:**  
**Approved-On Date:** 4/19/2011  
**Effective Date:** 7/1/2011  
**Revision Date:** 4/11/2011

### I. Policy Statement

IT Security Audit 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 IT Security Audit policy defines the steps necessary to assess whether IT security controls implemented to mitigate risks are adequate and effective.

**Note:** In accordance with the Code of Virginia § 2.2-2009, the requirements of this policy apply only to “all executive branch and independent agencies and institutions of higher education.”

### III. Scope

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

### IV. Requirements

For each IT system classified as sensitive, the data-owning unit shall:

1. Require that the IT systems undergo an IT Security Audit as required by and in accordance with the current version of the IT Security Audit Standard (COV ITRM Standard SEC502).
2. Assign an individual to be responsible for managing IT Security Audits.
3. IT Security Audits should only be performed by independent parties who are not associated with the processes or procedures of the system

### 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.