



OIT 62.404: IT Systems Interoperability Security

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 Interoperability Security defines the steps necessary to provide adequate and effective protection for University systems.

II. Purpose

The IT System Interoperability Security policy identifies steps to protect data shared with other IT systems.

III. Scope

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

IV. Requirements

For every sensitive University IT system that shares data with non-University entities, the University shall require or shall specify that its service provider require:

Note: Best practice dictates that Interoperability Agreements should be in place for sensitive IT system interoperability between Commonwealth agencies. However, this Policy currently only requires agreements between Commonwealth and non-Commonwealth entities.

1. The System Owner, in consultation with the Data Owner, shall document IT systems with which data is shared. This documentation must include:
 - a. The types of shared data;
 - b. The direction(s) of data flow; and
 - c. Contact information for the organization that owns the IT system with which data is shared, including the System Owner, the Information Security Officer (ISO), or equivalent, and the System Administrator.

2. The System Owners of the IT systems which share data shall develop a written agreement that delineates security requirements for each interconnected IT system and for each type of data shared.
3. The System Owners of the IT systems that share data shall inform one another regarding other IT systems with which their IT systems interconnect or share data, and shall inform one another prior to establishing any additional interconnections or data sharing.
4. The written agreement shall specify if and how the shared data will be stored on each IT system.
5. The written agreement shall specify that System Owners of the IT systems that share data acknowledge and agree to abide by any legal requirements (i.e., HIPAA) regarding handling, protection, and disclosure of the shared data.
6. The written agreement shall specify each Data Owner's authority to approve access to the shared data.
7. The System Owners shall approve and enforce the agreement.

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.