



## OIT 62.016 Systems Interoperability Security

**Responsible Executive:** Chief Information Officer (CIO)  
**Responsible Office:** Office of Information Technology  
**Related Policy:** NSU 60.201: Acceptable Use of Technological Resources  
COV IT Information Security Standard (SEC501-01)  
**Approved-On Date:** December 17, 2009  
**Effective Date:** December 17, 2009  
**Revision Date:** December 17, 2009

### Policy Statement

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

### Purpose

The purpose this policy is to define the steps necessary to provide adequate and effective protection for sensitive NSU IT systems and data.

### Requirements for internal systems

For every sensitive IT system, NSU shall require that:

1. The System Owner, in consultation with the Data Owner, document IT systems with which data is shared. This documentation shall include:
  - The types of shared data
  - The direction(s) of data flow
  - Contact information including the System Owner, the Information Security Officer (ISO) or equivalent, and the System Administrator for systems with which data is shared.
2. The systems be compliant with and follow NSU and OIT policies and procedures.

### Requirements for external systems

For every sensitive IT system, NSU shall require or shall specify that its service provider require:

3. The System Owner, in consultation with the Data Owner, document IT systems with which data is shared. This documentation shall include:

- The types of shared data
  - The direction(s) of data flow
  - Contact information for the organization that owns the IT system with which data is shared.
4. The System Owners of the IT systems which share data develop a IT Systems Interoperability Security Agreement ([www.nsu.edu/forms](http://www.nsu.edu/forms)) that delineates the following:
- The IT security requirements for each interconnected system and each type of data shared.
  - The System Owners of the IT systems that share data inform one another regarding other IT systems with which their systems interconnect or share data and inform one another prior to establishing any additional interconnections or data sharing.
  - If and how the shared data will be stored on each IT system.
  - That System Owners of the IT systems which share data acknowledge and agree to abide with any legal requirements (i.e., HIPAA, FERPA) regarding handling, protection, and disclosure of the shared data.
  - The Data Owner's authority to approve access to the shared data.
  - The System Owners approve and how the agreement shall be enforced.