



OIT 62.406: System Development Life Cycle 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

The Systems Development Life Cycle (SDLC) Security policy defines the steps necessary to provide adequate and effective protection for University systems.

II. Purpose

The Systems Development Life Cycle (SDLC) Security policy documents the security-related activities that must occur in each phase of the development life cycle (from project definition through disposal) for University IT application systems.

III. Scope

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

IV. Requirements

NSU shall:

1. Incorporate security requirements in each phase of the life cycle, as well as for each modification proposed for the IT application system in each stage of its life cycle.

Project Initiation

2. Perform an initial risk analysis based on the known requirements and the business objectives to provide high-level security guidelines for the system developers.
3. Classify the types of data (see IT System and Data Sensitivity Classification) that the system will process and the sensitivity of the proposed IT system.

4. Assess the need for collection and maintenance of sensitive data before incorporating such collection and maintenance in IT system requirements.
5. Develop an initial IT System Security Plan (see IT System Security Plans) that documents the security controls that the system will enforce to provide adequate protection against security risks.

Project Definition

6. Identify, develop, and document security requirements for the system during the Project Definition phase.
7. Incorporate security requirements in IT system design specifications.
8. Verify that the system development process designs, develops, and implements security controls that meet information security requirements in the design specifications.
9. Update the initial IT System Security Plan to document the security controls included in the design of the system to provide adequate protection against security risks.
10. Develop evaluation procedures to validate that security controls developed for a new system are working properly and are effective.

Note: Some security controls (primarily those controls of a non-technical nature) cannot be tested and evaluated until after deployment of the system.

Implementation

11. Execute the evaluation procedures to validate and verify that the functionality described in the specification is included in the product.

Note: Results should be documented in a report, including identification of controls that did not meet design specifications.
12. Conduct a Risk Assessment (see Risk Assessment) to assess the risk level of the system.
13. Require that the system comply with all relevant Risk Management requirements in this Standard.
14. Update the IT System Security Plan to document the security controls included in the system as implemented to provide adequate protection against

information security risks, and comply with the other requirements (see IT System Security Plans) of this document.

Disposition

15. Require retention of the data handled by a system takes place in accordance with the University's records retention policy prior to disposing of the system.
16. Require that electronic media is sanitized prior to disposal, as documented (see Policy 62.602 Data Storage Media Protection), so that all data is removed from the system.
17. Verify the disposal of hardware and software in accordance with the current version of the Removal of Commonwealth Data from Surplus Computer Hard Drives and Electronic Media Standard (COV ITRM Standard SEC514).

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.