Policy Title: Life Cycle Support

Policy Type: Administrative


Approval Date: 05/28/2014 Revised

Responsible Office: Office of Information Technology

Responsible Executive: CIO

Applies to: Office of Information Technology

POLICY STATEMENT

Life cycle support addresses the analysis of the University’s information system to determine necessary processes, continued development, and system device management to ensure the continued security and functionality of the information system.

TABLE OF CONTENTS

<table>
<thead>
<tr>
<th>TABLE OF CONTENTS</th>
<th>PAGE NUMBER</th>
</tr>
</thead>
<tbody>
<tr>
<td>Contacts</td>
<td>1</td>
</tr>
<tr>
<td>Stakeholder(s)</td>
<td>1</td>
</tr>
<tr>
<td>Purpose</td>
<td>2</td>
</tr>
<tr>
<td>Requirements</td>
<td>2</td>
</tr>
<tr>
<td>Violations</td>
<td>5</td>
</tr>
<tr>
<td>Interpretation</td>
<td>5</td>
</tr>
<tr>
<td>Publication</td>
<td>5</td>
</tr>
<tr>
<td>Review Schedule</td>
<td>6</td>
</tr>
<tr>
<td>Related Documents</td>
<td>6</td>
</tr>
</tbody>
</table>

CONTACT(S)

Office of Information Technology – (757)823-2869

STAKEHOLDER(S)

University Faculty & Staff
Office of Information Technology
PURPOSE

This control is intended to establish the policy and procedures for assessing life cycle support development for the University’s information systems.

REQUIREMENTS

NSU:

1. Manages the information system using a system development life cycle methodology that includes information security considerations;

2. Defines and documents information system security roles and responsibilities throughout the system development life cycle; and

3. Identifies individuals having information system security roles and responsibilities.

NSU shall:

1. Project Initiation
   a. Perform an initial risk analysis based on the known requirements and the business objectives to provide high-level security guidelines for the system developers.

   b. Classify the types of data (see IT System and Data Sensitivity Classification) that the IT system will process and the sensitivity of the proposed IT system.

   c. Assess the need for collection and maintenance of sensitive data before incorporating such collection and maintenance in IT system requirements.

   d. Develop an initial IT System Security Plan (see IT System Security Plans) that documents the IT security controls that the IT system will enforce to provide adequate protection against IT security risks.

2. Project Definition
   a. Identify, develop, and document IT security requirements for the IT system during the Project Definition phase.

   b. Incorporate IT security requirements in IT system design specifications.

   c. Verify that the IT system development process designs, develops, and implements IT security controls that meet information security requirements in the design specifications.
d. Update the initial IT System Security Plan to document the IT security controls included in the design of the IT system to provide adequate protection against IT security risks.

e. Develop IT security evaluation procedures to validate that IT security controls developed for a new IT system are working properly and are effective.

3. Implementation

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

b. Conduct a Risk Assessment (see Risk Assessment) to assess the risk level of the IT application system.

c. Require that the system comply with all relevant Risk Management requirements in this Standard.

d. Update the IT System Security Plan to document the IT security controls included in the IT system as implemented to provide adequate protection against information security risks, and comply with the other requirements (see IT Systems Security Plans) of this document.

4. Disposition

a. Require retention of the data handled by an IT system in accordance with the agency’s records retention policy prior to disposing of the IT system.

b. Require that electronic media is sanitized prior to disposal, as documented (see Data Storage Media Protection), so that all data is removed from the IT system.

c. 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).

NSU’s ISO is accountable for ensuring the following steps are documented and followed:

1. Application Planning

   a. Data Classification - Data used, processed or stored by the proposed application shall be classified according to the sensitivity of the data.

   b. Risk Assessment – If the data classification identifies the system as sensitive, a risk assessment shall be conducted before development begins and after planning is complete.
c. Security Requirements – Identify and document the security requirements of the application early in the development life cycle. For a sensitive system, this shall be done after a risk assessment is completed and before development begins.

d. Security Design – Use the results of the Data Classification process to assess and finalize any encryption, authentication, access control, and logging requirements. When planning to use, process or store sensitive information in an application, agencies must address the following design criteria:

i. Encrypted communication channels shall be established for the transmission of sensitive information;

ii. Sensitive information shall not be visibly transmitted between the client and the application; and

iii. Sensitive information shall not be stored in hidden fields that are part of the application interface.

2. Application Development

The following requirements represent a minimal set of coding practices, which shall be applied to all applications under development.

a. Authentication – Application-based authentication and authorization shall be performed for access to data that is available through the application but is not considered publicly accessible.

b. Session Management - Any user sessions created by an application shall support an automatic inactivity timeout function.

c. Data storage shall be separated either logically or physically, from the application interface (i.e., design two or three tier architectures where possible).

d. Agencies shall not use or store sensitive data in non-production environments (i.e., a development or test environment that does not have security controls equivalent to the production environment).

e. Input Validation – All application input shall be validated irrespective of source. Input validation should always consider both expected and unexpected input, and not block input based on arbitrary criteria.

f. Default Deny – Application access control shall implement a default deny policy, with access explicitly granted

g. Principle of Least Privilege – All processing shall be performed with the least set of privileges required.
h. Quality Assurance – Internal testing shall include at least one of the following: penetration testing, fuzz testing, or a source code auditing technique. Third party source code auditing and/or penetration testing should be conducted commensurate with sensitivity and risk.

i. Configure applications to clear the cached data and temporary files upon exit of the application or logoff of the system.

3. Production and Maintenance

   a. Production applications shall be hosted on servers compliant with NSU Security requirements for IT system hardening.

   b. Internet-facing applications classified as sensitive shall have periodic, not to exceed 90 days, vulnerability scans run against the applications and supporting server infrastructure, and always when any significant change to the environment or application has been made. Any remotely exploitable vulnerability shall be remediated immediately. Other vulnerabilities should be remediated without undue delay.

VIOLATIONS

Violations of this policy will be addressed in accordance relevant University and Commonwealth of Virginia policies, including University Policy 32-01 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.

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.

PUBLICATION

This policy shall be widely published and distributed to the University community. To ensure timely publication and distribution thereof, the Responsible Office will make every effort to:

1. Communicate the policy in writing, electronic or otherwise, to the University community within 14 days of approval;

2. Submit the policy for inclusion in the online Policy Library within 14 days of approval;

3. Post the policy on the appropriate SharePoint Site and/or Website; and
4. Educate and train all stakeholders and appropriate audiences on the policy’s content, as necessary. Failure to meet the publication requirements does not invalidate this policy.

REVIEW SCHEDULE

- Next Scheduled Review: 05/28/2015
- Approval by, date: Office of Information Technology and 05/28/2014
- Revision History:
  - Supersedes (previous policy): OIT 62.8.1503 Life Cycle Support

RELATED DOCUMENTS

Virginia Commonwealth State policy SEC501-08 Information Security Standard