Policy Title: Media Protection Policy and Procedures

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

Media protection addresses the storage and protection of any data or medium for storing data, whether sensitive or otherwise, and is subsequently necessary to assist in maintaining security within the University’s 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>2</td>
</tr>
<tr>
<td>Purpose</td>
<td>2</td>
</tr>
<tr>
<td>Requirements</td>
<td>2</td>
</tr>
<tr>
<td>Violations</td>
<td>3</td>
</tr>
<tr>
<td>Interpretation</td>
<td>3</td>
</tr>
<tr>
<td>Publication</td>
<td>3</td>
</tr>
<tr>
<td>Review Schedule</td>
<td>3</td>
</tr>
<tr>
<td>Related Documents</td>
<td>4</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 produce the policy and procedures that are required for the effective implementation of selected security controls and control enhancements in the media protection family.

REQUIREMENTS

NSU develops, disseminates, and reviews/updates at least annually:

1. A formal, documented media protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among University entities, and compliance; and

2. Formal, documented procedures to facilitate the implementation of the media protection policy and associated media protection controls.

NSU shall document and implement Data Storage Media protection practices. At a minimum, these practices must include the following components:

1. Define protection of stored sensitive data as the responsibility of Data Owner.

2. Prohibit the storage of sensitive data on any non-network storage device or media, except for backup media, unless the data is encrypted and there is a written exception approved by the Agency Head accepting all residual risks. The exception shall include following elements:
   a. The business or technical justification;
   b. The scope, including quantification and duration (not to exceed one year);
   c. A description of all associated risks;
   d. Identification of controls to mitigate the risks, one of which must be encryption; and
   e. Identification of any residual risks.

3. Prohibit the storage of any Commonwealth or NSU data on IT systems that are not under the contractual control of NSU. The owner of the IT System must adhere to the latest Commonwealth of Virginia and NSU information security policies and standards as well as the latest Commonwealth of Virginia and NSU auditing policies and standards.
4. Prohibit the connection of any non-University owned or leased data storage media or device to a University-owned or leased resource, unless connecting to a guest network or guest resources. This prohibition, at the University’s discretion need not apply to an approved vendor providing operational IT support services under contract.

Prohibit the auto forwarding of emails to external accounts to prevent data leakage unless there is a documented business case disclosing residual risk approved in writing by the Agency Head.

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 62.8.1001 Media Protection Policy and Procedures

RELATED DOCUMENTS

Virginia Commonwealth State policy SEC501-08 Information Security Standard