Policy Title: Media Sanitization

Policy Type: Administrative

Policy Number: ADMINISTRATIVE POLICY # 32 – 8 – 1006 (2014) Media Sanitization

Approval Date: 05/28/2014 Revised

Responsible Office: Office of Information Technology

Responsible Executive: CIO

Applies to: Office of Information Technology

POLICY STATEMENT

Media sanitization policies involve the appropriate disposal of any data or medium for storing data, whether sensitive or otherwise, and is accordingly necessary to assist in maintaining data 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>1</td>
</tr>
<tr>
<td>Purpose</td>
<td>2</td>
</tr>
<tr>
<td>Requirements</td>
<td>2</td>
</tr>
<tr>
<td>Violations</td>
<td>2</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>3</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 University’s policy and procedures for media sanitization or disposal.

REQUIREMENTS

NSU sanitizes information system media, both digital and non-digital, prior to disposal, release out of University control, or release for reuse.

NSU shall remove data from IT assets prior to disposal 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).

Control Enhancements for Sensitive Systems:

NSU:

1. Tracks, documents, and verifies media sanitization and disposal actions;

2. Tests sanitization equipment and procedures to verify correct performance 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);

3. Sanitizes portable, removable storage devices prior to connecting such devices to the information system; and

Enhancement Supplemental Guidance: Portable, removable storage devices (e.g., thumb drives, flash drives, external storage devices) can be the source of malicious code insertions into University information systems. Many of these devices are obtained from unknown sources and may contain various types of malicious code that can be readily transferred to the information system through USB ports or other entry portals. While scanning such devices is always recommended, sanitization provides additional assurance that the device is free of all malicious code to include code capable of initiating zero-day attacks. NSU considers sanitization of portable, removable storage devices, for example, when such devices are first purchased from the manufacturer or vendor prior to initial use or when the University loses a positive chain of custody for the device. The University’s assessment of risk guides the specific circumstances for employing the sanitization process.

4. Destroys information system media that cannot be sanitized

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 62.8.1006 Media Sanitization

RELATED DOCUMENTS

Virginia Commonwealth State policy SEC501-08 Information Security Standard