Policy Title: Information System Backup

Policy Type: Administrative

Policy Number: ADMINISTRATIVE POLICY # 32 – 8 – 609 (2014) Information System Backup

Approval Date: 05/28/2014 Revised

Responsible Office: Office of Information Technology

Responsible Executive: CIO

Applies to: Office of Information Technology

POLICY STATEMENT

Regular backups of user-level information contained in the information system are an integral process that assist in achieving recovery time and recovery point objectives in the event of a hazardous event compromising normal operational ability.

TABLE OF CONTENTS

<table>
<thead>
<tr>
<th>CONTACT(S)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Office of Information Technology – (757)823-2869</td>
</tr>
</tbody>
</table>

<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>4</td>
</tr>
<tr>
<td>Interpretation</td>
<td>4</td>
</tr>
<tr>
<td>Publication</td>
<td>4</td>
</tr>
<tr>
<td>Review Schedule</td>
<td>4</td>
</tr>
<tr>
<td>Related Documents</td>
<td>4</td>
</tr>
</tbody>
</table>
STAKEHOLDER(S)

University Faculty & Staff
Office of Information Technology

PURPOSE

This control establishes the University’s policy for backing up and maintaining user-level data for use in the event of hazardous occurrences that might result in disruption of normal operations.

REQUIREMENTS

NSU:

1. Conducts backups of user-level information contained in the information system within the University-defined frequency consistent with recovery time and recovery point objectives;

2. Conducts backups of system-level information contained in the information system in accordance with University-defined frequency consistent with recovery time and recovery point objectives;

3. Conducts backups of information system documentation including security-related documentation in accordance with University-defined frequency consistent with recovery time and recovery point objectives; and

4. Protects the confidentiality and integrity of backup information at the storage location.

Supplemental Guidance: System-level information includes, for example, system-state information, operating system and application software, and licenses. Digital signatures and cryptographic hashes are examples of mechanisms that can be employed by the University to protect the integrity of information system backups. A University assessment of risk guides the use of encryption for protecting backup information. The protection of system backup information while in transit is beyond the scope of this control.

Controls Enhancement for Sensitive Systems:

1. NSU tests backup information at least every 30-days to verify media reliability and information integrity.

2. NSU uses a sample of backup information in the restoration of selected information system functions as part of contingency plan testing.
3. NSU stores backup copies of the operating system and other critical information system software, as well as copies of the information system inventory (including hardware, software, and firmware components) in a separate facility or in a fire-rated container that is not collocated with the operational system.

For every IT system identified as sensitive relative to availability, NSU shall or shall require that its service provider implement backup and restoration plans to support restoration of systems, data and applications in accordance with agency requirements. At a minimum, these plans shall address the following:

1. Secure off-site storage for backup media.

2. Store off-site backup media in an off-site location that is geographically separate and distinct from the primary location.

3. Performance of backups only by authorized personnel.

4. Review of backup logs after the completion of each backup job to verify successful completion.

5. Approval of backup schedules of a system by the System Owner.

6. Approval of emergency backup and operations restoration plans by the System Owner.

7. Protection of any backup media that is sent off-site (physically or electronically), or shipped by the United States Postal Service or any commercial carrier, in accordance with agency requirements.

8. Authorization and logging of deposits and withdrawals of all media that is stored off-site.

9. Retention of the data handled by an IT system in accordance with the agency’s records retention policy.

10. Management of electronic information in such a way that it can be produced in a timely and complete manner when necessary, such as during a legal discovery proceeding.

11. Document and exercise a strategy for testing that IT system and data backups are functioning as expected and the data is present in a usable form.

12. For systems that are sensitive relative to availability, document and exercise a strategy for testing disaster recovery procedures, in accordance with NSU’s Continuity of Operations Plan.
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 62.8.609 Information System Backup

RELATED DOCUMENTS

Virginia Commonwealth State policy SEC501-08 Information Security Standard