POLICY STATEMENT

In the event of an incident that has the potential to disrupt normal daily operations, a secondary site for information and data processing is required as pursuant to achieve recovery time and recovery point objectives.

TABLE OF CONTENTS

<table>
<thead>
<tr>
<th>CONTACT(S)</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 establishes the University’s policy for obtaining and maintaining an alternate site for the purpose of information systems and data processing in the event of hazardous occurrences that might result in disruption of normal operations.

REQUIREMENTS

NSU:

1. Establishes an alternate processing site including necessary agreements to permit the resumption of information system operations for essential missions and business functions within the University-defined time period consistent with recovery time objectives when the primary processing capabilities are unavailable; and

2. Ensures that equipment and supplies required to resume operations are available at the alternate site or contracts are in place to support delivery to the site in time to support the University-defined time period for resumption.

Controls Enhancement for Sensitive Systems:

1. NSU identifies an alternate processing site that is separated from the primary processing site so as not to be susceptible to the same hazards.

   Enhancement Supplemental Guidance: Hazards that might affect the information system are typically defined in the risk assessment.

2. NSU identifies potential accessibility problems to the alternate processing site in the event of an area-wide disruption or disaster and outlines explicit mitigation actions.

3. NSU develops alternate processing site agreements that contain priority-of-service provisions in accordance with the University’s availability requirements.

4. NSU configures the alternate processing site so that it is ready to be used as the operational site supporting essential missions and business functions.

5. NSU ensures that the alternate processing site provides information security measures equivalent to that of the primary site.

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 62.8.607 Alternate Processing Site

**RELATED DOCUMENTS**

Virginia Commonwealth State policy SEC501-08 Information Security Standard