POLICY STATEMENT

Contingency Planning is a necessary component in the practical strategies to recover essential business functions or dependent business functions in the case of an event that causes a moderate to severe impact on daily operations. Contingency planning addresses both information system restoration and implementation of alternative mission/business processes when systems are compromised.

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>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 is intended to establish the policy and procedures that are required for the effective implementation of selected security controls and control enhancements in the contingency planning family.

REQUIREMENTS

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

1. A formal, documented contingency planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

2. Formal, documented procedures to facilitate the implementation of the contingency planning policy and associated contingency planning controls.

NSU shall:

1. Designate an employee to collaborate with the agency Continuity of Operations Plan (COOP) coordinator as the focal point for IT aspects of COOP and related Disaster Recovery (DR) planning activities.

2. Based on BIA and RA results, develop IT disaster components of the agency COOP which identifies:

   a. Each IT system that is necessary to recover essential business functions or dependent business functions and the Recovery Time Objective (RTO) and Recovery Point Objective (RPO) for each; and

   b. Personnel contact information and incident notification procedures.

   Note: If the COOP contains sensitive data, those components with sensitive data should be protected and stored at a secure off-site location.

3. Require an annual exercise (or more often as necessary) of IT DR components to assess their adequacy and effectiveness.
4. Require review and revision of IT DR components following the exercise (and at other times as necessary).

5. Based on the COOP, develop and maintain an IT DRP, which supports the restoration of essential business functions and dependent business functions.

6. Require approval of the IT DRP by the Agency Head.

7. Require periodic review, reassessment, testing, and revision of the IT DRP to reflect changes in essential business functions, services, IT system hardware and software, and personnel.

8. Establish communication methods to support IT system users’ local and remote access to IT systems, as necessary.

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 62.8.601 Contingency Planning Policy and Procedures

RELATED DOCUMENTS

Virginia Commonwealth State policy SEC501-08 Information Security Standard