Policy Title: Contingency Plan

Policy Type: Administrative

Policy Number: ADMINISTRATIVE POLICY # 32 – 8 – 602 (2014) Contingency Plan

Approval Date: 05/20/2014 Revised

Responsible Office: Office of Information Technology

Responsible Executive: CIO

Applies to: Office of Information Technology

POLICY STATEMENT

Contingency planning for information systems is part of an overall University plan for achieving continuity of operations for mission/business 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>1</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>

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 necessary for developing, maintaining, and effectively communicating the Contingency plan for NSU.

REQUIREMENTS

NSU:

1. Develops a contingency plan for the information system that:
   a. Identifies essential missions and business functions and associated contingency requirements;
   b. Provides recovery objectives, restoration priorities, and metrics;
   c. Addresses contingency roles, responsibilities, assigned individuals with contact information;
   d. Addresses maintaining essential missions and business functions despite an information system disruption, compromise, or failure;
   e. Addresses eventual, full information system restoration without deterioration of the security measures originally planned and implemented; and
   f. Is reviewed and approved by designated officials within the University OIT team;

2. Distributes copies of the contingency plan to an University-defined list of key contingency personnel (identified by name and/or by role) and University elements;

3. Coordinates contingency planning activities with incident handling activities;

4. Reviews the contingency plan for the information system at least annually;

5. Revises the contingency plan to address changes to the University, information system, or environment of operation and problems encountered during contingency plan implementation, execution, or testing; and

6. Communicates contingency plan changes to the University-defined list of key contingency personnel (identified by name and/or by role) and University elements.

Supplemental Guidance: Information system recovery objectives are consistent with applicable laws, directives, policies, standards, or regulations. In addition to information system availability, contingency plans also address other security-related events resulting in a reduction in
mission/business effectiveness, such as malicious attacks compromising the confidentiality or integrity of the information system. Examples of actions to call out in contingency plans include, for example, graceful degradation, information system shutdown, fall back to a manual mode, alternate information flows, or operating in a mode that is reserved solely for when the system is under attack.

**Controls Enhancement for Sensitive Systems:**

1. NSU coordinates contingency plan development with University elements responsible for related plans.


2. NSU conducts capacity planning so that necessary capacity for information processing, telecommunications, and environmental support exists during contingency operations.

3. NSU plans for the resumption of essential missions and business functions within the University-defined time period of contingency plan activation.

**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 62.8.602 Contingency Planning

RELATED DOCUMENTS

Virginia Commonwealth State policy SEC501-08 Information Security Standard