Policy Title: Incident Response Assistance

Policy Type: Administrative

Policy Number: ADMINISTRATIVE POLICY # 32 – 8 – 807 (2014) Incident Response Assistance

Approval Date: 05/28/2014 Revised

Responsible Office: Office of Information Technology

Responsible Executive: CIO

Applies to: Office of Information Technology

POLICY STATEMENT

An efficient and practiced incident response support resource can provide the necessary assistance with events deemed potential threats to 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>2</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 on the incident response support resources available to University staff.

REQUIREMENTS

NSU provides an incident response support resource, integral to the University incident response capability, which offers advice and assistance to users of the information system for the handling and reporting of security incidents.

Supplemental Guidance: Possible implementations of incident response support resources in the University include a help desk or an assistance group and access to forensics services, when required.

Control Enhancements for Sensitive Systems:

1. NSU:
   a. Establishes a direct, cooperative relationship between its incident response capability and external providers of information system protection capability; and
   b. Identifies University incident response team members to the external providers.

Enhancement Supplemental Guidance: External providers of information system protection capability include, for example, the Computer Network Defense program within the U.S. Department of Defense. External providers help to protect, monitor, analyze, detect, and respond to unauthorized activity within University information systems and networks.

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.
ADMINISTRATIVE POLICY # 32 – 8 – 807 (2014) Incident Response Assistance

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 62.8.807 Incident Response Assistance

RELATED DOCUMENTS

Virginia Commonwealth State policy SEC501-08 Information Security Standard