Policy Title: Incident Reporting

Policy Type: Administrative

Policy Number: ADMINISTRATIVE POLICY # 32 – 8 – 806 (2014) Incident Reporting

Approval Date: 05/28/2014 Revised

Responsible Office: Office of Information Technology

Responsible Executive: CIO

Applies to: Office of Information Technology

POLICY STATEMENT

Incident reporting is required in order to alert the appropriate authorities to events that have the potential to compromise 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 policy and procedures for formal incident reporting requirements with regard to the University information system.

REQUIREMENTS

NSU:

1. Requires personnel to report suspected security incidents to the University incident response capability within 24 hours from when the agency discovered or should have discovered their occurrence; and

2. Reports security incident information to designated authorities.

NSU shall:

1. Provide quarterly summary reports of IDS and IPS events to Commonwealth Security.

2. Establish a process for reporting IT security incidents to the CISO. Users must report security incidents within 24 hours from when they are discovered.

3. Report information security incidents only through channels that have not been compromised.

   Supplemental Guidance: The types of security incidents reported, the content and timeliness of the reports, and the list of designated reporting authorities are consistent with applicable laws, directives, policies, regulations, standards, and guidance.

Control Enhancements for Sensitive Systems:

NSU reports information system weaknesses, deficiencies, and/or vulnerabilities associated with reported security incidents to appropriate University officials.

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 62.8.806 Incident Reporting

RELATED DOCUMENTS

Virginia Commonwealth State policy SEC501-08 Information Security Standard