Policy Title: Incident Handling

Policy Type: Administrative

Policy Number: ADMINISTRATIVE POLICY # 32 – 8 – 804 (2014) Incident Handling

Approval Date: 05/28/2014 Revised

Responsible Office: Office of Information Technology

Responsible Executive: CIO

Applies to: Office of Information Technology

POLICY STATEMENT

Incident handling encompasses all procedures necessary for the appropriate approach to those events that pose security risks to the University. These procedures include, but are not limited to, the preparedness, detection, and reactive measures for such events. All aspects of incident handling are required in pursuance of adequate and effective incident responsiveness.

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>6</td>
</tr>
<tr>
<td>Interpretation</td>
<td>6</td>
</tr>
<tr>
<td>Publication</td>
<td>6</td>
</tr>
<tr>
<td>Review Schedule</td>
<td>6</td>
</tr>
<tr>
<td>Related Documents</td>
<td>6</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 incident handling policy and procedures for events that are considered to potentially compromise the University’s information system.

REQUIREMENTS

NSU:

1. Implements an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery;
2. Coordinates incident handling activities with contingency planning activities; and
3. Incorporates lessons learned from ongoing incident handling activities into incident response procedures, training, and testing/exercises, and implements the resulting changes accordingly.

Supplemental Guidance: Incident-related information can be obtained from a variety of sources including, but not limited to, audit monitoring, network monitoring, physical access monitoring, and user/administrator reports.

NSU shall:

1. Identify immediate mitigation procedures, including specific instructions, based on information security incident categorization level, on whether or not to shut down or disconnect affected IT systems.
2. Establish procedures for information security incident investigation, preservation of evidence, and forensic analysis.
3. Identify and document all agency systems, processes, and logical or physical data storage locations (whether held by the agency or a third party) that contain personal information or medical information.
   a. Personal information means the first name or first initial and last name in combination with and linked to any one or more of the following data elements that relate to a resident of the Commonwealth, when the data elements are neither encrypted nor redacted:
      i. Social security number;
      ii. Driver’s license number or state identification card number issued in lieu of a driver’s license number; or
iii. Financial account number, or credit card or debit card number, in combination with any required security code, access code, or password that would permit access to a resident’s financial accounts;

b. Medical information means the first name or first initial and last name in combination with and linked to any one or more of the following data elements that relate to a resident of the Commonwealth, when the data elements are neither encrypted nor redacted:

i. Any information regarding an individual's medical or mental health history, mental or physical condition, or medical treatment or diagnosis by a health care professional; or

ii. An individual's health insurance policy number or subscriber identification number, any unique identifier used by a health insurer to identify the individual, or any information in an individual's application and claims history, including any appeals records.

4. “Redact” for personal information means alteration or truncation of data such that no more than the following are accessible as part of the personal information:

a. Five digits of a social security number; or

b. Mental or physical condition; or

c. Medical treatment or diagnosis; or

d. No more than four digits of a health insurance policy number, subscriber number; or

e. Other unique identifier.

5. Include provisions in any third party contracts requiring that the third party and third party subcontractors:

a. Provide immediate notification to the agency of suspected breaches; and

b. Allow the agency to both participate in the investigation of incidents and exercise control over decisions regarding external reporting.

6. Provide appropriate notice to affected individuals upon the unauthorized release of unencrypted and/or un-redacted personal information or medical information by any mechanism, including, but not limited to:

a. Theft or loss of digital media including laptops, desktops, tablets, CDs, DVDs, tapes, USB drives, SD cards, etc.;
b. Theft or loss of physical hardcopy; and

c. Security compromise of any system containing personal or medical information (i.e., social security numbers, credit card numbers, medical records, insurance policy numbers, laboratory findings, pharmaceutical regimens, medical or mental diagnosis, medical claims history, medical appeals records, etc.)

7. An individual or entity shall disclose the breach of the security of the system if encrypted information is accessed and acquired in an unencrypted form, or if the security breach involves a person with access to the encryption key.

8. If a Data Custodian is the entity involved in the data breach, they must alert the Data Owner so that the Data Owner can notify the affected individuals.

9. NSU shall provide this notice without undue delay as soon as verification of the unauthorized release is confirmed, except as delineated in #10, below.

10. In the case of a computer found to be infected with malware that exposes data to unauthorized access, individuals that may have had their information exposed due to use of that computer must be alerted in accordance with data breach rules. Agencies shall notify the CISO when notification of affected individuals has been completed.

11. Provide notification that consists of:

   a. A general description of what occurred and when;

   b. The type of Personal Information that was involved;

   c. What actions have been taken to protect the individual’s Personal Information from further unauthorized access;

   d. A telephone number that the person may call for further information and assistance, if one exists; and

   e. What actions the agency recommends that the individual take. The actions recommended should include monitoring their credit report and reviewing their account statements (i.e., credit report, medical insurance Explanation of Benefits (EOB), etc.).

12. Provide this notification by one or more of the following methodologies, listed in order of preference:

   a. Written notice to the last known postal address in the records of the individual or entity;

   b. Telephone Notice;

   c. Electronic notice; or
d. Substitute Notice - if the individual or the entity required to provide notice demonstrates that the cost of providing notice will exceed $50,000, the affected class of Virginia residents to be notified exceeds 100,000 residents, or the individual or the entity does not have sufficient contact information or legal consent to provide notice. Substitute notice consists of all of the following:

i. Email notice if the individual or the entity has email addresses for the members of the affected class of residents;

ii. Conspicuous posting of the notice on the website of the individual or the entity if the individual or the entity maintains a website; and

iii. Notice to major statewide media.

13. Hold the release of notification immediately following verification of unauthorized data disclosure only if law enforcement is notified and the law enforcement agency determines and advises the individual or entity that the notice would impede a criminal or civil investigation, or homeland security or national security. Notice shall be made without unreasonable delay after the law enforcement agency determines that the notification will no long impede the investigation or jeopardize national or homeland security.

Control Enhancements for Sensitive Systems:

1. NSU identifies classes of incidents and defines appropriate actions to take in response to ensure continuation of University missions and business functions.

   Enhancement Supplemental Guidance: Classes of incidents include, for example, malfunctions due to design/implementation errors and omissions, targeted malicious attacks, and untargeted malicious attacks. Incident response actions that may be appropriate include, for example, graceful degradation, information system shutdown, fall back to manual mode or alternative technology whereby the system operates differently, employing deceptive measures (e.g., false data flows, false status measures), alternate information flows, or operating in a mode that is reserved solely for when a system is under attack.

2. NSU correlates incident information and individual incident responses to achieve a University-wide perspective on incident awareness and response.

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 62.8.804 Incident Handling

**RELATED DOCUMENTS**

Virginia Commonwealth State policy SEC501-08 Information Security Standard