The purpose of an Information Technology Standard is to specify requirements for compliance with Old Dominion University Information Technology policies, other University policies, as well as applicable laws and regulations. Standards may include business principles, best practices, technical standards, migration and implementation strategies, that direct the design, deployment and management of information technology.

Information Technology Standard: Data Breach Notification Standard
Reference Number: 05.2.0
Date of Current Revision or Creation: December 2012

A. PURPOSE

The purpose of this standard is to specify the data breach notification requirements for Old Dominion University by identifying the triggering factors and necessary responses to unauthorized release of unencrypted sensitive information.

B. DEFINITIONS

Data Breach is an incident in which sensitive, protected or confidential data has potentially been viewed, stolen and/or used by an individual unauthorized to do so.

Personal Information is any piece of data that can potentially be used to identify a single person. Generally, NAME and one or more personal information data elements are necessary to place identity at serious risk.

C. STANDARDS STATEMENT

ODU will identify all University systems, processes, and logical and physical data storage locations, including those held by third parties, which contain personal Information. The personal information of import that is most likely to place identity at risk is defined as NAME and one or more of the following:

a. Social Security Number
b. Driver’s license or University identification card number
c. Financial account number, credit or debit card number
d. Other personal identifying information, such as insurance data or date of birth.
ODU will 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 both to participate in the investigation of incidents and exercise control over decisions regarding external reporting.

ODU will provide appropriate notice to affected individuals upon the unauthorized release of any unencrypted personal information by any mechanism, including, but not limited to:

a. Theft or loss of digital media including laptops, desktops, flash drives, smart phones, tablets, CD’s, DVD’s, tapes, etc.;
b. Theft or loss of physical hardcopy; or
c. Security compromise of any system containing personal information.

ODU will provide this notice without undue delay as soon as verification of the unauthorized release is confirmed, except as delineated below.

ODU will provide notification that consists of:

a. A general description of what occurred and when;
b. The type of personal information was involved;
c. What actions have been taken to protect the individual’s personal information from further unauthorized disclosure?
d. What, if anything, ODU will do to assist affected individuals, including contact information for more information and assistance; and
e. What actions ODU recommends that the individual take.

ODU will provide this notification by one or more of the following methodologies, listed in order of preference:

a. Standard mailing to any affected individuals whose mailing addresses are available.
b. Electronic mail to any affected individuals whose email address has been provided to the agency as a contact mechanism.
c. In the case of large scale breaches or data breaches where neither form of communication listed above is available or feasible, public communications channels, including:

i. Conspicuous notification on the agency website; and
ii. Notification by statewide public media, including newspaper, radio, and television).

ODU will not provide notification immediately following verification of unauthorized data disclosure only if requested by:

a. Law Enforcement entities where it would interfere with an ongoing investigation; or
b. CIO, ISO or designee where it would interfere with a determination of the scope of the data breach or investigation of root cause.

D. PROCEDURES, GUIDELINES & OTHER RELATED INFORMATION

Federal and State Law

Policy 3505 Security Policy

Security Awareness Training

E. HISTORY

<table>
<thead>
<tr>
<th>Date</th>
<th>Responsible Party</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>October 2008</td>
<td>ITAC/CIO</td>
<td>Created</td>
</tr>
<tr>
<td>October 2009</td>
<td>ITAC/CIO</td>
<td>Reaffirmed</td>
</tr>
<tr>
<td>October 2010</td>
<td>ITAC/CIO</td>
<td>Reaffirmed</td>
</tr>
<tr>
<td>October 2011</td>
<td>ITAC/CIO</td>
<td>Reaffirmed</td>
</tr>
<tr>
<td>October 2012</td>
<td>ITAC/CIO</td>
<td>Reaffirmed</td>
</tr>
<tr>
<td>December 2012</td>
<td>IT Policy Office</td>
<td>Minor rewording for clarity</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Link updated</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Numbering revision</td>
</tr>
</tbody>
</table>