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: Information Security Program Review Standard

<table>
<thead>
<tr>
<th>Reference Number:</th>
<th>08.2.0</th>
</tr>
</thead>
<tbody>
<tr>
<td>Date of Current Revision or Creation:</td>
<td>March 21, 2013</td>
</tr>
</tbody>
</table>

### A. PURPOSE

The purpose of this standard is to establish the management responsibilities and define the elements to be examined in information security program reviews.

### B. DEFINITIONS

**Information Security Officer (ISO)** is responsible person for developing, reviewing, evaluating, and managing the University’s Information Security Program.

Information Security Program is the framework of general principles, guidelines and security controls and elements used to protect University data and assets and to satisfy the laws and regulations relevant to information security.

Information Security Review is a summary of security recommendations and safeguards to be developed by the University, the IT Security Team and the technical staff for the continued protection of information technology assets.

### C. POLICY STATEMENT

The Old Dominion University Information Security Program elements are reviewed on an annual cycle and when significant changes occur to ensure its continuing suitability, adequacy, and effectiveness.

The IT Security Program Reviews include assessing opportunities for improvement of information security policy and the approach to managing information security in response to...
changes to the organizational environment, business circumstances, legal conditions, or technical environment.

The ISO reviews should include information on these topics as appropriate:

- feedback from interested parties
- results of independent reviews
- status of preventive and corrective actions
- results of previous ISO reviews
- process performance and information security policy compliance
- changes to the organizational environment, business circumstances, available resources, contractual, regulatory and legal conditions, or to the technical environment.
- trends related to identified threats or vulnerabilities
- reported information security incidents
- recommendations provided by relevant authorities

ISO management reviews will document decisions and/or actions related to:

- improvement of the organization's approach to managing information security and its processes
- improvement of control objectives and controls
- improvement in the allocation of resources and/or responsibilities

Based on the results of the reviews, the ISO develops an IT Security Review outlining strategies and actions for the protection of the confidentiality, integrity, availability, and accountability of the University's information technology assets.

D. PROCEDURES, GUIDELINES & OTHER RELATED INFORMATION

Federal and State Law

- University IT Policies
- IT Standards and Guidelines

E. HISTORY

<table>
<thead>
<tr>
<th>Date</th>
<th>Responsible Party</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>April 20, 2010</td>
<td>CIO/ITAC</td>
<td>Approved</td>
</tr>
<tr>
<td>April 20, 2010</td>
<td>CIO/ITAC</td>
<td>Approved</td>
</tr>
<tr>
<td>October, 2011</td>
<td>CIO/ITAC</td>
<td>Reaffirmed</td>
</tr>
<tr>
<td>March 21, 2013</td>
<td>CIO/ITAC</td>
<td>Numbering, Security Office Revision</td>
</tr>
<tr>
<td>March 21, 2013</td>
<td>CIO/ITAC</td>
<td>Reaffirmed</td>
</tr>
</tbody>
</table>