Office of Computing and Communications Services

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.

<table>
<thead>
<tr>
<th>Information Technology Standard:</th>
<th>IT Security Awareness Guideline</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reference Number:</td>
<td>3.1.0</td>
</tr>
<tr>
<td>Date of Current Revision or Creation:</td>
<td>December 2012</td>
</tr>
</tbody>
</table>

A. PURPOSE
The purpose of this guideline is to describe the information security awareness, training, and education program for Old Dominion University.

B. DEFINITIONS
None

C. STANDARDS STATEMENT

The focus of security awareness at Old Dominion University is aimed at creating an attitude towards a commitment to good security practices and facilitating a climate that sees security rules as beneficial to the protection of the University environment. The Information Security Officer (ISO) has been designated as the individual who is responsible for all aspects of an agency's security awareness and training program including development, implementation, testing, training, monitoring attendance, and periodic updates.

**Information Security Awareness Training Program**
The IT security awareness program blends formal training with periodic reminders and promotional materials to increase the understanding of vulnerabilities and threats to the University’s information systems. Information security training is directed on improving the security skills and competencies of users.

**User Training Requirements**
All users must participate in the security awareness program through training sessions that correspond to role, responsibilities and use of information technology resources. This requirement is a condition of use.
IT Training Courses
Formal courses with specific content designed to address specific IT Security Roles. The courses are repeated annually at a minimum. Course content is reviewed annually to reflect changes in the IT security environment. Attendance at these courses is recorded.

General Security Awareness/Initial Account Training
This course is expected to increase user understanding and sensitivity to threats, vulnerabilities, and the need to protect University and personal information. All users are required to receive this training. This training is usually delivered on-line and is tied to account creation process.

Account Refresher Training
This course is expected to refresh user understanding and sensitivity to threats, vulnerabilities, and the need to protect University and personal information. All users are required to receive refresher training and it is tied to account renewal process. Users may also elect to receive refresher training as desired.

Employee Security Awareness Training
This course provides an overview of compliance and is designed to explain employee responsibilities to security. Attention to IT Security policy and standards is provided with special focus on handling of sensitive data. This training is usually delivered on-line and is tied to account management process.

Remote Users Security Training
This course provides an overview of employee responsibilities when connecting to information resources from a remote location. Attention to IT Security policy and standards, securing the workstation, handling of sensitive data and incident reporting is provided. This training is usually delivered on-line and is tied to VPN account management process.

Disaster Recovery Team Training
This course provides instruction on the policies and procedures related to the IT Disaster Recovery plan. It is designed to prepare the members of the Disaster Recover Team to effectively function in that role by having a good understanding of the ODU IT Disaster Recovery Plan (DRP), the purpose of it and their role in it.

IT Security Administrator Training
Training for those who manage, administer, operate, and design IT systems, is provided annually as practicable and necessary.

Instructor-led Topical Training
Special topic presentations designed to address a specific security training need are provided. Sessions are voluntary and are focused on a narrow topic, such as Internet Safety, Social Networking Security or Cyber Self Defense.

New Employee Orientation
Basic information and training materials are provided to new employees as a part of their orientation to the University.
New Student Orientation
Basic information and training materials are provided to new students as a part of their orientation to the University.

Specialized User Communication
Formal distribution lists, listservs or other communication methods are used to dispense information to special user populations. Information is focused on policies, standards, procedures, skills, tools, etc. needed to perform their specific role or function. Specialized populations include Campus Residents, Data Stewards, System Administrators, Data Owners, System Owners and the Information Technology Advisory Council.

Security Review and Consultation
Staff from the IT Security office is available to consult with campus users on risk assessments, application reviews, vulnerability scans, rights managements and information on security best practices.

General Community Awareness
General awareness will be broadly available through a variety of methods and media channels. Awareness is provided through guidelines and best practices on the Office of Computing and Communications Services website, posting of notices of virus alerts and other advisories, through awareness messages in posters, brochures, email, newsletters, flyers, giveaways, on mouse pads in computer laboratories and by videos and telecasts on Monarch TV. Efforts to increase awareness using social media (Facebook, Twitter, and YouTube) are ongoing. Security policies and standards are published. An online knowledgebase shares best practices. Security staff provides presentations to groups upon requests. The Technical Support Center staff incorporates security information into routine contacts with customers.

Cyber Security Event
Along with other institutions, each October, Old Dominion University participates in the National Cyber Security Alliance’s National Cyber Security Awareness Month campaign to raise awareness about cyber security and online safety by highlighting precautions users can take to help protect themselves online.

B. PROCEDURES, GUIDELINES & OTHER RELATED INFORMATION

References:

Policy 3500 – Policy on the Use of Computing Resources
Policy 3505 - Information Security Policy
Policy 3505 - Information Technology Security Program

C. 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>March 2012</td>
<td>ITAC/CIO</td>
<td>Reaffirmed</td>
</tr>
</tbody>
</table>