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.

Information Technology Standard: Information Technology Security Roles and Responsibilities
Reference Number: 1.2.0
Date of Current Revision or Creation: March 2012

A. PURPOSE

The purpose of this compliance standard is to clearly define the roles and responsibilities involved in the ODU Information Technology Security Program.

B. DEFINITIONS

Data Classification - In the context of information security, it is the classification of data based on its level of sensitivity and the impact to the University should that data be disclosed, altered or destroyed without authorization.

University Data - All data or information owned, used, created or maintained by the University whether individually controlled or shared, stand-alone or networked.

C. STANDARDS STATEMENT

This standard defines the roles and responsibilities included in the ODU Security Program. The roles are assigned to individuals and may differ from their official position title. Individuals may be assigned multiple roles as long as there is separation of duties, protection against fraud and conflicts of interest.

Agency Head

At Old Dominion University, the Agency Head is the University President. The Agency Head, or designee, is responsible for the security of the University’s IT systems and data.
The Agency Head’s IT security responsibilities include the following:

1. Designate and inform the Virginia Information Technology Agency (VITA), by way of an email or hard copy signed letter, to Chief Information Security Officer of the Commonwealth (CISO), the individual chosen as the Information Security Officer (ISO), including the person’s name, title, and contact information. The Agency head’s designee may email the information to VITA with a copy to the ODU Agency Head. The President may also designate a deputy ISO as needed.

2. Determine the optimal place of the IT security function within the University hierarchy with the shortest practicable reporting line to the President.

3. Maintain an IT security program that is sufficient to protect the University’s IT systems, and that is documented and effectively communicated.

4. Review and approve the Business Impact Analyses (BIAs), Risk Assessment (RAs) and Continuity of Operations Plan (COOP), to include an IT Disaster Recovery Plan.

5. Review (or have the designated ISO review) of System Security Plans (in the form of Risk Assessments) for all sensitive agency IT systems.

6. Review or have the designated ISO review the System Security Plans for all agency IT systems classified as sensitive, and approve System Security Plans that provide adequate protections against security risks; or disapprove System Security Plans that do not provide adequate protections against security risks, and require that the System Owner implement additional security controls on the IT system to provide adequate protections against security risks.

7. Maintain an IT Security audit program that includes, but is not limited to, requiring development and implementation of an plan for IT security audits; requiring that the planned IT security audits are conducted; receiving reports of the results of IT security audits; and requiring development of Corrective Action Plans to address findings of IT security audits.

8. Ensure a program of IT security safeguards.

9. Ensure an IT security awareness and training program.

10. Provide the resources to enable employees to carry out their responsibilities for securing IT systems and data.

11. Prevent, or have a designee prevent, conflict of interest and adhere to the security concept of separation of duties.

Information Security Officer (ISO)
The ISO is responsible for developing and managing Old Dominion University’s IT security program. At Old Dominion University, this role has been formally assigned to a position in the Office of Computing and Communications Services. The Information Security Officer must be an employee of the Commonwealth of Virginia. The ISO is restricted from holding the role of a System Owner and a Data Owner except in the case of compliance systems for information security.
The Information Security Officer is responsible for the following:

1. Develop and manage an IT security program that follows industry standards such as the International Standards Organization’s ISO-27000 series of standards, best practices and the practices of similar higher education institutions.
2. Verify and validate that all University systems and data are classified for sensitivity.
3. Develop and maintain an IT security awareness and training program for faculty, staff, and students, including contractors and IT service providers.
4. Implement and maintain the appropriate balance of protective, detective, and corrective controls for IT systems commensurate with data sensitivity, risk, and systems criticality.
5. Mitigate and report all IT security incidents in accordance with §2.2-603 of the Code of Virginia and take appropriate actions to prevent recurrence.

Privacy Officer
At Old Dominion University, a Privacy Officer has not been designated at this time. However, should a situation arise whereby the University must designate a Privacy Officer by law or regulation, such as the Health Insurance Portability and Accountability Act (HIPAA), the responsibilities are to be carried out by the Data Owner or their designee for the data that is subject to the law or regulation.

The Privacy Officer is responsible for providing guidance on the following:

1. The requirements of state and federal Privacy laws pertaining to the data involved.
2. Disclosure and access to sensitive data.
3. Security and protection requirements in conjunction with IT systems when there is overlap among sensitivity, disclosure, privacy, and security issues.

System Owner
The System Owner is the manager responsible for operation and maintenance of a University IT system. The System Owner is restricted from acting as System Administrator for systems or data they own. The System Owner must be an employee of the Commonwealth of Virginia and can own multiple systems.

The System Owner’s is responsible for the following:

1. Require that all IT system users complete IT security awareness and training activities prior to, or as soon as practicable after, receiving access to the system, and no less than annually, thereafter.
2. Manage system risk and developing any additional IT security policies and procedures required to protect the system in a manner commensurate with risk.
3. Follow industry standards such as the International Standards Organization’s ISO-27000 series of standards, best practices and the practices of similar higher education institutions.
4. Maintain compliance with requirements specified by Data Owners for the handling of data processed by the system.
5. Designate System Administrators for the system.
6. Participate in the development of the University’s Business Impact Analysis (BIA).
8. The System Owner, in consultation with the Data Owner, documents IT systems with which data is shared, including the types of shared data; the direction(s) of data flow; and the contact information for the organization that owns the IT system with which data is shared, including the System Owner, the Information Security Officer (ISO), or equivalent and the System Administrator.
9. The System Owner of the IT systems which share data develop a written agreement that delineates IT security requirements for each interconnected IT system and for each type of data shared and inform one another regarding other IT systems with which their IT systems interconnect or share data, and inform one another prior to establishing any additional interconnections or data sharing.
10. The written agreement must specify how the shared data will be stored on each IT system and specify the System Owner of the IT systems that share data acknowledge and agree to abide with any legal requirements regarding handling, protection, and disclosure of the shared data. The written agreement maintains each Data Owner’s authority to approve access to the shared data.
11. The System Owner approves and enforces the agreement.

Data Owner
The Data Owner is the manager responsible for the policy and practice decisions regarding data. The Data Owner must be an employee of the Commonwealth of Virginia and can own data in multiple systems. The Data Owner is restricted from acting as System Administrator for systems they own.

The Data Owner is responsible for the following:

1. Evaluate and classify sensitivity of the data.
2. Identify the type(s) of data handled by the University IT system and determine whether each type of data is also subject to other regulatory requirements.
3. Determine the potential damages to the University if the data was compromised.
4. Classify the IT system as sensitive if any type of data handled by the IT system has a sensitivity of high on any of the criteria of confidentiality, integrity, or availability.
5. Use the information documented in the data classification policy as a primary input to the Risk Assessment process.
6. Define protection requirements for the data based on the sensitivity of the data, any legal or regulatory requirements, and business needs.
7. Communicate data protection requirements to the System Owner.
8. Define requirements for access to the data.
9. Participate in the development of the University’s Business Impact Analysis (BIA).

**System Administrator**
The System Administrator is an analyst, engineer, or consultant who implements, manages, and/or operates a system or systems at the direction of the System Owner, Data Owner, and/or Data Administrator.

The System Administrator is responsible for the following:

1. Assists management in the day-to-day administration of IT systems.
2. Implements security controls and other requirements of the security program on IT systems for which assigned.
3. The System Administrator can administer multiple systems.

**Security Administrator**
The Security Administrator ensures that proper security software, controls, and configurations are in place to protect the assigned information technology resources. The Security Administrator is restricted from acting as System Administrator or System Owner on the same IT resource they administer.

The Security Administrator is responsible for the following:

1. Scan for vulnerabilities.
2. Propose, require, and oversee the implementation of security controls.
3. Monitor for violations or attempted violations of the security environment.
4. Perform forensics of compromised systems when needed.
5. Coordinate corrective actions for compromised systems.
6. Track and report security violations.

**Data Administrator**
Data Administrators are individuals or organizations in physical or logical possession of data for Data Owners. The Data Administrator must be an employee of the Commonwealth of Virginia and can own multiple systems.

The Data Administrator is responsible for the following:

1. Protect the data in their possession from unauthorized access, alteration, destruction, or usage.
2. Establish, monitor, and operate IT systems in a manner consistent with security policies and standards.
3. Provide Data Owners with reports, when necessary and applicable.
University Managers
Managers at all levels must provide for the IT security needs under their jurisdiction. They shall take all reasonable actions to provide adequate IT security and to escalate problems, requirements, and matters related to IT security to the highest level necessary for resolution.

Information Technology System Users
All users of IT systems, including faculty, staff, students, contractors and visitors, are responsible for the following:

1. Read and comply with IT security program requirements.
2. Report breaches of IT security, actual or suspected, to their University management and/or the Information Security Officer (ISO).
3. Take reasonable and prudent steps to protect the security of IT systems and data to which they have access.

Roles Assigned to Contractors
Roles may be assigned to contractors. In such circumstances, the contract language must include specific responsibility and background check requirements.

D. PROCEDURES, GUIDELINES & OTHER RELATED INFORMATION

Federal and State Law
University IT Policies
OCCS Policies and Standards

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>March 2012</td>
<td>ITAC/CIO</td>
<td>Replaced Standard 02.2.1 and 02.2.1 Numbering revision</td>
</tr>
</tbody>
</table>