Policy Title: Information Security Roles and Responsibilities

Policy Type: Administrative


Approval Date: 05/28/2014 Revised

Responsible Office: Office of Information Technology

Responsible Executive: CIO

Applies to: Office of Information Technology

POLICY STATEMENT

The Information Security Roles and Responsibilities Policy delineates the steps necessary to identify, analyze, prioritize, and mitigate risks that could compromise IT systems and data.

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>Roles and Responsibilities</td>
<td>2</td>
</tr>
<tr>
<td>Violations</td>
<td>8</td>
</tr>
<tr>
<td>Interpretation</td>
<td>8</td>
</tr>
<tr>
<td>Publication</td>
<td>8</td>
</tr>
<tr>
<td>Review Schedule</td>
<td>9</td>
</tr>
<tr>
<td>Related Documents</td>
<td>9</td>
</tr>
</tbody>
</table>

CONTACT(S)

Office of Information Technology – (757)823-2869

STAKEHOLDER(S)

University Faculty & Staff
PURPOSE

This Policy defines the key IT security roles and responsibilities included in the Commonwealth’s Information Security Program. These roles and responsibilities are assigned to individuals, and may differ from the COV role title or working title of the individual’s position. Individuals may be assigned multiple roles, as long as the multiple role assignments provide adequate separation of duties, provide adequate protection against the possibility of fraud, and do not lead to a conflict of interests.

ROLES AND RESPONSIBILITIES

Chief Information Officer of the Commonwealth (CIO)

The Code of Virginia §2-2.2009 states that “the CIO shall direct the development of policies, procedures and standards for assessing security risks, determining the appropriate security measures and performing security audits of government electronic information.”

Chief Information Security Officer (CISO)

The CISO is responsible for development and coordination of the COV Information Security Program and, as such, performs the following duties:

1. Administers the COV Information Security Program and periodically assesses whether the program is implemented in accordance with COV Information Security Policies and Standards.


3. Provides solutions, guidance, and expertise in IT security.

4. Maintains awareness of the security status of sensitive IT systems.

5. Facilitates effective implementation of the COV Information Security Program, by:
   a. Preparing, disseminating, and maintaining information security, policies, standards, guidelines and procedures as appropriate;
   b. Collecting data relative to the state of IT security in the COV and communicating as needed;
c. Providing consultation on balancing an effective information security program with business needs.

6. Provides networking and liaison opportunities to Information Security Officers (ISOs).

**Agency Head**

The Agency Head is responsible for the security of the agency's IT systems and data. The Agency Head’s IT security responsibilities include the following:

1. Designate an Information Security Officer (ISO) for the agency, no less than biennially:
   
   **Note:** Acceptable methods of communicating the designation to the CISO, include:
   
   a. An email directly from the agency head, or
   
   b. An email from the agency which copies the agency head, or
   
   c. A hard-copy letter or facsimile transmission signed by the agency head.
   
   d. This designation must include the following information:
      
      i. ISO’s name
      
      ii. ISO’s title
      
      iii. ISO’s contact information
      
      **Note:** The ISO should report directly to the Agency Head where practical and should not report to the CIO. The ISO is responsible for developing and managing the agency’s information security program. The Agency Head is strongly encouraged to designate at least one backup for the ISO. Agencies with multiple geographic locations or specialized business units should also consider designating deputy ISOs as needed.

2. Ensure that an agency information security program is maintained, that is sufficient to protect the agency’s IT systems, and that is documented and effectively communicated. Managers in all agencies and at all levels shall 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.

3. Review and approve the agency’s Business Impact Analyses (BIAs), Risk Assessments (RAs), and Continuity of Operations Plan (COOP), to include an IT Disaster Recovery Plan, if applicable.
4. Review or have the designated ISO review the System Security Plans for all agency IT systems classified as sensitive, and:
   a. Approve System Security Plans that provide adequate protections against security risks; or
   b. 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.

5. Ensure compliance is maintained with the current version of the IT Security Audit Standard (COV ITRM Standard SEC502). This compliance must include, but is not limited to:
   a. Requiring development and implementation of an agency plan for IT security audits, and submitting this plan to the CISO;
   b. Requiring that the planned IT security audits are conducted;
   c. Receiving reports of the results of IT security audits;
   d. Requiring development of Corrective Action Plans to address findings of IT security audits; and
   e. Reporting to the CISO all IT security audit findings and progress in implementing corrective actions in response to IT security audit findings.

   Note: If the IT security audit shows no findings, this is to be reported to the CISO as well.

6. Ensure a program of information security safeguards is established.

7. Ensure an information security awareness and training program is established.

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

9. Identify a System Owner who is generally the Business Owner for each agency sensitive system. Each System Owner shall assign a Data Owner(s), Data Custodian(s) and System Administrator(s) for each agency sensitive IT system.

10. Prevent or have designee prevent conflict of interests and adhere to the security concept of separation of duties by assigning roles so that:
a. The ISO is not a System Owner or a Data Owner except in the case of compliance systems for information security;
b. The System Owner and the Data Owner are not System Administrators for IT systems or data they own; and
c. The ISO, System Owners, and Data Owners are COV employees.

Notes:

a. Other roles may be assigned to contractors. For roles assigned to contractors, the contract language must include specific responsibility and background check requirements.

b. A System Owner can own multiple IT systems.

c. A Data Owner can own data on multiple IT systems.

d. System Administrators can assume responsibility for multiple IT systems.

Information Security Officer (ISO)

The ISO is responsible for developing and managing the agency’s information security program. The ISO’s duties are as follows:

1. Develop and manage an agency information security program that meets or exceeds the requirements of COV IT security policies and standards in a manner commensurate with risk.

2. Verify and validate that all agency IT systems and data are classified for sensitivity.

3. Develop and maintain an information security awareness and training program for agency staff, including contractors and IT service providers. Require that all IT system users complete required IT security awareness and training activities prior to, or as soon as practicable after, receiving access to any system, and no less than annually, thereafter.

4. Implement and maintain the appropriate balance of preventative, detective and corrective controls for agency 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 VITA requirements and take appropriate actions to prevent recurrence.

6. Maintain liaison with the CISO.
7. Meet educational requirements necessary to maintain an information security program by meeting all of the following requirements:

a. Attending Information Security Orientation training,

b. Successfully completing at least 3 course hours per year of security courses authorized by the CISO.

c. Possessing a recognized professional IT Security Certification, i.e., CISSP, CISM, CISA, SANS, meeting all requirements of the certification body, may be substituted for two (2) courses.

d. Attending one mandatory ISOAG meeting per year, and

e. Obtaining an additional 20 hours of training in IT security related topics annually (ISOAG meetings count for up to 3 hours each!)

Note: Continuing Profession Education credits (CPE’s) for professional IT Security Certifications can be applied to this requirement.

Privacy Officer

An agency must have a Privacy Officer if required by law or regulation, such as the Health Insurance Portability and Accountability Act (HIPAA), and may choose to have one where not required. Otherwise, these responsibilities are carried out by the ISO. The Privacy Officer provides guidance on:

1. The requirements of state and federal Privacy laws.

2. Disclosure of and access to sensitive data.

3. Security and protection requirements in conjunction with IT systems when there is some overlap among sensitivity, disclosure, privacy, and security issues.

System Owner

The System Owner is the agency business manager responsible for having an IT system operated and maintained. With respect to IT security, the System Owner’s responsibilities include the following:

1. Require that the IT system users complete any system unique security training 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 information security policies and procedures required to protect the system in a manner commensurate with risk.
3. Maintain compliance with COV Information Security policies and standards in all IT system activities.

4. Maintain compliance with requirements specified by Data Owners for the handling of data processed by the system.

5. Designate a System Administrator for the system.

Note: Where more than one agency may own the IT system, and the agency or agencies cannot reach consensus on which should serve as System Owner, upon request, the CIO of the Commonwealth will determine the System Owner.

Data Owner

The Data Owner is the agency manager responsible for the policy and practice decisions regarding data, and is responsible for the following:

1. Evaluate and classify sensitivity of the data.

2. Define protection requirements for the data based on the sensitivity of the data, any legal or regulatory requirements, and business needs.

3. Communicate data protection requirements to the System Owner.

4. Define requirements for access to the data.

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 Custodian. The System Administrator assists agency management in the day-to-day administration of agency IT systems, and implements security controls and other requirements of the agency information security program on IT systems for which the System Administrator has been assigned responsibility.

Data Custodian

Data Custodians are individuals or organizations in physical or logical possession of data for Data Owners. Data Custodians are responsible for the following:

1. Protecting the data in their possession from unauthorized access, alteration, destruction, or usage.

2. Establishing, monitoring, and operating IT systems in a manner consistent with COV Information Security policies and standards.
3. Providing Data Owners with reports, when necessary and applicable.

**IT System Users**

All users of COV IT systems including employees and contractors are responsible for the following:

1. Reading and complying with agency information security program requirements.
2. Reporting breaches of IT security, actual or suspected, to their agency management and/or the CISO.
3. Taking reasonable and prudent steps to protect the security of IT systems and data to which they have access.

**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 62.2 Information Security Roles and Responsibilities

RELATED DOCUMENTS

Virginia Commonwealth State policy SEC501-08 Information Security Standard