**Security Awareness and Training Policy Template**

### Security Awareness & Training Policy TEMPLATE

### 

**EFFECTIVE DATE: 07/01/2014**

# PURPOSE

The purpose of this policy is to create a prescriptive set of process and procedures, aligned with applicable COV IT security policy and standard, to ensure that “YOUR AGENCY” develops, disseminates, and updates the Security Awareness and Training policy. This policy and procedure establishes the minimum requirements for the Security Awareness and Training controls.

This policy is intended to meet the control requirements outlined in SEC501, Section 8.2 Security Awareness and Training Family, Controls AT-1 through AT-5, to include specific requirements for the Commonwealth of Virginia in AT-2-COV.

# SCOPE

All “YOUR AGENCY” employees (classified, hourly, or business partners) who require access to “YOUR AGENCY”’s IT systems

# ACRONYMS

CIO: Chief Information Officer

COV: Commonwealth of Virginia

ISO: Information Security Officer

COV: Commonwealth of Virginia

CSRM: Commonwealth Security and Risk Management

IT: Information Technology

ITRM: Information Technology Resource Management

SEC501: Information Security Standard 501

“YOUR AGENCY”: “YOUR AGENCY”

# DEFINITIONS

[See COV ITRM Glossary](http://www.vita.virginia.gov/uploadedFiles/Library/PSGs/EA_PSG_update_011510/ITRMGlossary_011510.pdf)

# BACKGROUND

The security awareness program at “YOUR AGENCY” is intended to educate users on the security policy of the agency. In addition to education, the program is also intended to help foster an understanding of how the policy protects the agency business, its employees and customers. This policy directs that “YOUR AGENCY” meet the requirements as stipulated by COV ITRM Security Standard SEC501 and security best practices.

# ROLES & RESPONSIBILITY

This section will provide summary of the roles and responsibilities as described in the Statement of Policy section. The following Roles and Responsibility Matrix describe 4 activities:

1. Responsible (R) – Person working on activity
2. Accountable (A) – Person with decision authority and one who delegates the work
3. Consulted (C) – Key stakeholder or subject matter expert who should be included in decision or work activity
4. Informed (I) – Person who needs to know of decision or action

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Roles** | User | User Manager | System Owner | System Admin | Information Security Officer |
| **Tasks** |  |  |  |  |  |
| Complete security awareness training | R | R |  |  | A |
| Develop and update the security awareness and training program |  |  | R |  | A |
| User acceptance of security policies | R | A |  |  |  |
| Create role-based security related training materials |  |  | R | R | A |
| Document and monitor system security training |  |  |  |  | A |
| Relations with security groups and associations |  |  |  |  | A |
| Complete role-based security related training | R | A |  | R | I |
| Security training records |  |  |  |  | A/R |

# STATEMENT OF POLICY

In accordance with SEC501, AT-2 and AT-2-COV, AT-3, AT-4, and AT-5, “YOUR AGENCY” will provide Security Awareness and Training for all “YOUR AGENCY” employees and business partners accessing “YOUR AGENCY” IT systems (including managers, senior executives, and contractors). “YOUR AGENCY”’s Security Awareness and Training addresses roles, responsibilities, management commitment, coordination among organizational entities, and compliance. The training also includes general information security training, role based training, system specific training and general awareness.

**A. GENERAL SECURITY AWARENESS TRAINING**

1. The ISO will oversee “YOUR AGENCY”’s Security Awareness and Training program, including development, implementation, and testing.
2. The ISO or designee will coordinate, monitor and track the completion of the Security Awareness Training for all “YOUR AGENCY” employees and business partners and report incomplete training to the respective managers.
3. Security Awareness and Training content will be regularly reviewed by ISO and updated as appropriate. Security Awareness and Training will include, at a minimum, contents described in the Information Security Standard (SEC501), such as the following:
   1. The agency’s policy for protecting IT systems and data, with a particular emphasis on sensitive IT systems and data;
   2. The concept of separation of duties;
   3. Prevention and detection of information security incidents, including those caused by malicious code;
   4. Proper disposal of data storage media;
   5. Proper use of encryption;
   6. Access controls, including creating and changing passwords and the need to keep them confidential;
   7. “YOUR AGENCY” Acceptable Use policies;
   8. “YOUR AGENCY” Remote Access policies;
   9. Intellectual property rights, including software licensing and copyright issues;
   10. Responsibility for the security of Commonwealth data;
   11. Phishing; and
   12. Social engineering.
4. The ISO or designee will ensure that current versions of the Security policies and procedures are included in the Security Awareness Training.
5. Each manager is responsible for ensuring that their respective employees and business partners complete mandatory Security Awareness Training.
6. All new “YOUR AGENCY” employees and business partners will complete a Security Awareness Training course within the first 30 days of commencing work and repeat the training at least on an annual basis afterward.
7. All “YOUR AGENCY” employees and business partners will acknowledge that they have read, understand and accept the “YOUR AGENCY” Information Security policies and procedures included in the training.
8. The ISO or designee may revoke account rights until mandatory Security Awareness Training is completed.

**B. ROLE-BASED TRAINING**

1. The ISO or designee shall identify opportunities to create the appropriate role-based information security training materials and communicate the training opportunities to managers.
2. Managers will ensure that “YOUR AGENCY” employees and business partners, who manage, administer, operate, or design IT systems, receive additional role-based information security training that is commensurate with their level of expertise.

**C. INFORMATION SECURITY AWARENESS**

1. A variety of methods will be used to deliver Security Awareness and Training to “YOUR AGENCY” employees and business partners regularly throughout the year. Methods of delivery include, but are not limited to, posters, newsletters, “YOUR AGENCY” Buzzes, contests and events consistent with the Information Security Standard (SEC501).

**D. SECURITY TRAINING RECORDS**

* + - 1. The ISO or designee will document and monitor individual information security training activities including basic awareness training and specific information system security training.
      2. Individual training records will be retained for defined by the agency’s records retention policy.

**E. CONTACTS WITH SECURITY GROUPS AND ASSOCIATIONS**

* + - * 1. The ISO will establish and institutionalize contact with selected groups and associations within the security community:

1. To facilitate ongoing security education and training for organizational personnel;
2. To stay up to date with the latest recommended security practices, techniques, and technologies; and
3. To share current security-related information including threats, vulnerabilities, and incidents.

# ASSOCIATED

**PROCEDURE** “YOUR AGENCY” Information Security Program Policy

**AUTHORITY**

**REFERENCE** [*Code of Virginia, §2.2-2005 et seq.*](http://leg1.state.va.us/cgi-bin/legp504.exe?000+cod+2.2-2005)

(Powers and duties of the Chief Information Officer “CIO”““YOUR AGENCY””)

**OTHER**

**REFERENCE** [ITRM Information Security Policy (SEC519)](http://www.vita.virginia.gov/uploadedFiles/Library/PSGs/Security_Policy_519_00_Final_0709.pdf)

[ITRM Information Security Standard (SEC501)](http://www.vita.virginia.gov/uploadedfiles/VITA_Main_Public/Library/PSGs/Information_Security_Standard_SEC501_06_07012011.pdf)

| Version History | | |
| --- | --- | --- |
| Version | Date | Change Summary |
| 1 | 01/13/2004 | Original document. |
| 2 | 09/28/2007 | Update policy to align with revised IT security policy (ITRM SEC500-02) and standard (ITRM SEC501-01) and required multimedia delivery of awareness training. |
| 3 | 04/30/2010 | Total replacement from previous version with formatting changes and updates to be in compliance with the ITRM Information Security Standard – SEC501 (Revision 5) dated 08/11/2009. |
| 3.1 | 02/03/2012 | Clarification wording under A. General Information Security Training, number 8 by adding “The ISO or designee reserves the right to revoke access until mandatory Information Security Awareness and Training is completed.” |
| 4 | 07/01/2014 | Complete rewrite from previous version in compliance with the ITRM Information Security Standard SEC501 Revision 8 with Role Matrix added. |
| 5 | 11/30/2021 | Formatting changes |