**Information Security Roles and Responsibilities Policy Template**

# PURPOSE

The purpose of this policy is to create a prescriptive set of process and procedures, aligned with applicable COV IT security policy and standards, to ensure that “YOUR AGENCY NAME” develops, disseminates, and updates the Information Security Roles and Responsibilities Policy. This policy and procedure establishes the minimum requirements for the Information Security Roles and Responsibilities Policy.

This policy is intended to meet the control requirements outlined in SEC519 and SEC501, Section 1.3 Roles and Responsibilities.

# SCOPE

All “YOUR AGENCY NAME” employees (classified, hourly, or business partners).

# ACRONYMS

CIO: Chief Information Officer

COV: Commonwealth of Virginia

CSRM: Commonwealth Security and Risk Management

EBARS: Enterprise Backup and Restore System

ISO: Information Security Officer

IT: Information Technology

ITRM: Information Technology Resource Management

LAN: Local Area Network

PC: Personal Computer

RAS: Remote Access Server

SEC501: Information Security Standard 501

SEC519: Information Security Policy 519

SLA: Service Level Agreement

SOP: Standard Operating Procedure

VCCC: VITA Customer Care Center

“YOUR AGENCY NAME”: “YOUR AGENCY NAME”

VPN: Virtual Private Network

# DEFINITIONS

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

# BACKGROUND

The Information Security Roles and Responsibility Policy at “YOUR AGENCY NAME” is intended to facilitate the effective implementation of the processes necessary meet the roles and responsibility requirements as stipulated by the COV ITRM Security Standard SEC501, COV ITRM Information Security Policy SEC519, and security best practices. This policy directs that “YOUR AGENCY NAME” meet these requirements for all IT systems.

# STATEMENT OF POLICY

In accordance with SEC519 and SEC501, “YOUR AGENCY NAME” shall utilize an organization chart that depicts the reporting structure of employees when assigning specific responsibilities for the security of IT systems and data. “YOUR AGENCY NAME” shall maintain documentation regarding specific roles and responsibilities relating to information security.

1. **KEY SECURITY ROLES**
   1. Key security roles included in the COV Information Security Program 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.
      1. Chief Information Officer of the Commonwealth (CIO)
         1. 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.”
         2. The CIO of the Commonwealth is “YOUR AGENCY NAME”’s Agency Head.
      2. Chief Information Security Officer (CISO)
         1. 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.
            2. Reviews requested exceptions to COV Information Security Policies, Standards and Procedures.
            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:

Preparing, disseminating, and maintaining information security, policies, standards, guidelines and procedures as appropriate;

Collecting data relative to the state of IT security in the COV and communicating as needed; and

Providing consultation on balancing an effective information security program with business needs.

* + - * 1. Provides networking and liaison opportunities to Information Security Officers (ISOs).
      1. The CISO is “YOUR AGENCY NAME”’s ISO and shall report directly to the Agency Head, the CIO.
    1. Agency Head
       1. Each 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.

Acceptable methods of communicating the designation to the CISO, include:

An email directly from the agency head, or

An email from an agency head designee which copies the agency head, or

A hard-copy letter or facsimile transmission signed by the agency head.

This designation must include the following information:

ISO’s name,

ISO’s title and

ISO’s contact information.

* + - * 1. Designate at least one backup for the ISO.

“YOUR AGENCY NAME” should also consider designating deputy ISOs for different geographic locations or specialized business units.

* + - * 1. 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.
        2. Review and approve the agency’s Business Impact Analyses (BIAs), Risk Assessments (RAs), and Continuity Plan (previously referred to as Continuity of Operations Plan or COOP), to include an IT Disaster Recovery Plan, if applicable.
        3. 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.

* + - * 1. 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:

Requiring development and implementation of an agency plan for IT security audits, and submitting this plan to the CISO;

Requiring that the planned IT security audits are conducted;

Receiving reports of the results of IT security audits;

Requiring development of Corrective Action Plans to address findings of IT security audits; and

Reporting to the CISO all IT security audit findings and progress in implementing corrective actions in response to IT security audit findings.

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

* + - * 1. Ensure a program of information security safeguards is established.
        2. Ensure that an information security awareness and training program is established.
        3. Provide the resources to enable employees to carry out their responsibilities for securing IT systems and data.
        4. 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.
        5. Prevent or have designee prevent conflict of interests and adhere to the security concept of separation of duties by assigning roles so that:

The ISO is not a System Owner or a Data Owner except in the case of compliance systems for information security;

The System Owner and the Data Owner are not System Administrators for IT systems or data they own; and

A System Owner can own multiple IT systems.

A Data Owner can own data on multiple IT systems.

System Administrators can assume responsibility for multiple IT systems.

The ISO, System Owners, and Data Owners are COV employees.

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

* + 1. Information Security Officer (ISO)
       1. 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 “YOUR AGENCY NAME” 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:

Attending Information Security Orientation training,

Successfully completing at least 3 course hours per year of security courses authorized by the CISO. A recognized professional IT Security Certification, i.e., CISSP, CISM, CISA, SANS, may be substituted for two (2) courses,

Attending one mandatory ISOAG meeting per year, and

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 may be applied to this requirement.

* + - * 1. Work with other “YOUR AGENCY NAME” Directorates to document the responsibilities of the designee for each role identified in their job descriptions, and to develop and maintain a “YOUR AGENCY NAME” organization chart that that depicts the reporting structure of all “YOUR AGENCY NAME” employees who use IT systems and data and their IT security roles and responsibilities.
        2. Review the assignment of individuals to the roles described in this policy, including System Owner, Data Owner(s), and System Administrator(s).
    1. Privacy Officer
       1. 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.
    2. System Owner
       1. 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.
       2. 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.
    3. Data Owner
       1. 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.
    4. System Administrator
       1. 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.
    5. Data Custodian
       1. 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.
    6. IT System Users
       1. All users of COV IT systems including, but not limited to, employees and contractors are responsible for the following:
          1. Reading and complying with “YOUR AGENCY NAME” 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.
       2. Refer to the Information Resource Acceptable Use Policy for further information.

1. **ADDITIONAL ROLES AND RESPONSIBILITIES**
   1. IT Director
      1. Directors are considered to be accountable for their directorate’s IT data, systems, hardware, and software resources. Directors may further delegate these responsibilities to their assistant directors and branch managers. However, the director is ultimately responsible. The IT director’s responsibilities include:
         1. Monitor and enforce all security and usage policies.
         2. Authorize access to information systems, data, and equipment for which their directorate is the owner/trustee or designate an alternate in writing.
         3. Prevent the installation and use of computer games and other non-business software on directorate IT resources. This applies to employees whom have been granted local administrator rights to their PCs by their director.
         4. Monitor for and responding promptly to IT resource security deficiencies, misuse, theft, destruction or intrusion attempts by notifying the CSRM directorate immediately using the Information Security Incident Reporting Procedure.
         5. Inform VCCC whenever a user resigns, transfers, or is terminated from “YOUR AGENCY NAME” employment. This notification should be in writing and no less than two working days prior to the resignation or transfer, or at the time of termination. If immediate denial of LAN services is necessary, contact the VCCC immediately and follow up in a written message.
         6. Submit requests to VCCC for new PC hardware, returned unused PC hardware, and approved home use of “YOUR AGENCY NAME” PC hardware.
         7. Contact VCCC to install any business related software required for directorate staff to perform their job duties.
   2. Virginia Information Technologies Agency
      1. “YOUR AGENCY NAME” is responsible for designing and implementing controls and procedures that specifically intend to minimize the risk of loss or misuse of networked IT resources used, processed or stored within the “YOUR AGENCY NAME” organization. “YOUR AGENCY NAME” will:
         1. Locate file servers, related IT equipment such as switches and wiring components, and original copies of LAN software in an environmentally safe and physically secure area.
         2. Monitor the LAN activity and security structure, and respond promptly to any indication of misuse or destruction of LAN equipment and software.
         3. Take measures to prevent the installation or proliferation of computer viruses on LAN equipment.
         4. Monitor LAN software usage to ensure compliance with copyright laws and regulations.
         5. Use the Enterprise Backup and Restore System (EBARS) to backup agency network servers. Additionally, other backup methods will be used to supplement EBARS as well.
         6. Maintain and periodically test the LAN disaster recovery plan.
         7. Provide remote access services via RAS and VPN to IT users who have contacted VCCC for a new service request.
         8. Provide user assistance as needed.
         9. Perform LAN maintenance on a regular basis.
         10. Provide on call assistance, if needed, after business hours.
         11. Research and evaluate new technologies, which may include testing and implementing new software or new software upgrades.
         12. Comply with the “YOUR AGENCY NAME” Standard Operating Procedures (SOPs) and customer Service Level Agreements (SLAs).
         13. Report all security issues even hacking attempts promptly to the CSRM Directorate.
         14. Manage antivirus software and updates on the enterprise by subscribing to an automatic updating service. (i.e., Symantec provides this service and issues updated virus signatures on a daily basis for “YOUR AGENCY NAME”).
         15. Enable enterprise based antivirus-related logging on all managed PCs, and advise users with local administrator rights not to disable or change this capability.

# ASSOCIATED

**PROCEDURE** “YOUR AGENCY NAME” 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 NAME””)

**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 | 07/01/2014 | Supersedes “YOUR AGENCY NAME” CSRM IT Security Roles Resp Pol Pro and “YOUR AGENCY NAME” CSRM PC LAN Policy |
| 2 | 11/12/2021 | Formatting changes |