**Information Security Program Policy Template**

### Information Security Program Policy TEMPLATE

###

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

# PURPOSE

The purpose of this policy is to establish and maintain an effective security program which promotes information security and ensures the security of the Commonwealth’s databases and data communications from unauthorized uses, intrusions or other security threats and 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 Program Policy. This policy and procedure establishes the minimum requirements for the Information Security Program Policy.

This policy is intended to meet the control requirements outlined in SEC519 and SEC501, Section 1.4 Information Security Program.

# 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

ISO: Information Security Officer

IT: Information Technology

ITRM: Information Technology Resource Management

SEC501: Information Security Standard 501

SEC519: Information Security Policy 519

“YOUR AGENCY NAME”: “YOUR AGENCY NAME”

# DEFINITIONS

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

# BACKGROUND

The Information Security Program Policy at “YOUR AGENCY NAME” is intended to facilitate the effective implementation of the processes necessary meet the information security program requirements as stipulated by the COV ITRM Security Standard SEC501, COV ITRM Information Security Policy 519, and security best practices. This policy directs that “YOUR AGENCY NAME” meet these requirements for all IT systems.

# 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** | CIO | Directors and Managers | System Owner | Users | Information Security Officer |
| **Tasks** |  |   |   |   |   |
| Development of policies, procedures, and standards for assessing risks | A | R | C |  | R |
| Development, implementation, oversight, and maintenance of security program |  |  |  |  | A |
| Acknowledge and sign access agreement |  |  | R | A | R |
| Developing and implementing procedures |  | A |  |  |  |
| Oversee security program |  |  |  |  | A |
| Final interpretation of policy | A |  |  |  |  |
| Review all policies and procedures |  |  |  |  | A |

# STATEMENT OF POLICY

In accordance with SEC519 and SEC501, “YOUR AGENCY NAME” shall establish, document, implement, and maintain its information security program appropriate to its business and technology environment. In addition, because resources that can reasonably be committed to protecting IT systems are limited, “YOUR AGENCY NAME” must implement its information security program in a manner commensurate with sensitivity and risk.

1. INFORMATION SECURITY PROGRAM
	1. Pursuant to §2.2-2009 of the Code of Virginia, the Chief Information Officer of the Commonwealth is responsible for the development of policies, procedures, and standards for assessing security risks to the Commonwealth’s databases and data communications. The Chief Information Security Officer is appointed as the Information Security Officer (ISO). The ISO is responsible for the development, implementation, oversight, and maintenance of “YOUR AGENCY NAME”’s security program. This program and its associated policies are consistent with various state and federal information security regulations, for example, various information may require protection under the “Government Data Collection and Dissemination Practices Act” (Code of Virginia § 2.2-3800 et seq.) or the Federal Health Insurance Portability and Accountability Act (HIPAA).
	2. In addition, this policy establishes a program to ensure the confidentiality, availability, and integrity of data “YOUR AGENCY NAME” owns or serves as a custodian of, thereby reducing the risks of data loss, unauthorized modification and improper disclosure.
	3. This Program is modeled after: Information Security Policy (SEC519), Information Security Standard (SEC501), and the requirements necessary to maintain adequate security for the “YOUR AGENCY NAME” technology environment. This Program encompasses all security related COV policies, procedures, standards, and guidelines, as well as “YOUR AGENCY NAME” policies, procedures, directives, and branch specific operational procedures.
	4. Each “YOUR AGENCY NAME” employee/contractor will comply by acknowledging and signing the “YOUR AGENCY NAME” Information Security Access Agreement (ISAA). These employee/contractor agreements will be maintained by CSRM and retained for each employee/contractor as long as they are employed at “YOUR AGENCY NAME”.
	5. “YOUR AGENCY NAME” Directors and Managers are responsible for developing and implementing procedures that ensure compliance with the “YOUR AGENCY NAME” Information Security Program.
	6. The ISO is responsible for overseeing the “YOUR AGENCY NAME” Information Security Program by: promoting information security awareness; providing security-related technical assistance to directorates/branches; implementing and administering security programs and procedures; performing risk analyses; investigating alleged security breaches; developing, maintaining and disseminating a contingency management plan; and training users on proper methods of securing technology resources.
	7. The Chief Information Officer is responsible for final interpretation of this policy. Any exceptions to this policy must be documented and reviewed and approved by a level of management above that approving the exception. All documented exceptions to this policy will be kept on file by the ISO.
	8. The policy titles below are considered an integral part of the Information Security Policy and are referenced due to their relation to IT security. These policies are maintained by various divisions throughout “YOUR AGENCY NAME” and should be reviewed for update on a periodic basis by the issuing division or upon request by the ISO. All new policies/procedures developed within “YOUR AGENCY NAME” should be reviewed by the ISO for security implications.

# ASSOCIATED

**POLICIES &**

**PROCEDURES** “YOUR AGENCY NAME” Information Security Roles and Responsibilities

 “YOUR AGENCY NAME” IT Security Exceptions and Exemptions Policy

 “YOUR AGENCY NAME” BIA Policy

 “YOUR AGENCY NAME” IT System and Data Classification Policy

 “YOUR AGENCY NAME” Logical Access Controls Policy

 “YOUR AGENCY NAME” Remote and Wireless Access Control Policy

 “YOUR AGENCY NAME” Mobile Device Access Controls Policy

 “YOUR AGENCY NAME” Security Awareness and Training Policy

 “YOUR AGENCY NAME” IT Security Audit, Monitoring and Logging Policy

 “YOUR AGENCY NAME” IT Security Assessment and Authorization Policy

 “YOUR AGENCY NAME” IT Configuration Management Policy

 “YOUR AGENCY NAME” Contingency Planning Policy

 “YOUR AGENCY NAME” IT Identification and Authentication Policy

 “YOUR AGENCY NAME” IT Incident Response Policy

 “YOUR AGENCY NAME” IT System Maintenance Policy

 “YOUR AGENCY NAME” IT Media Protection Policy

 “YOUR AGENCY NAME” Physical and Environmental Policy

 “YOUR AGENCY NAME” IT System Security Planning Policy

 “YOUR AGENCY NAME” IT Personnel Security Policy

 “YOUR AGENCY NAME” IT Risk Assessment Policy

 “YOUR AGENCY NAME” IT System and Services Acquisition Policy

 “YOUR AGENCY NAME” IT System and Communications Protection Policy

 “YOUR AGENCY NAME” IT System and Communications Encryption Policy

 “YOUR AGENCY NAME” IT System and Information Integrity Policy

 “YOUR AGENCY NAME” Emergency Response Employee Communications Procedure

 “YOUR AGENCY NAME” Emergency Response Damage Assessment Procedure

 “YOUR AGENCY NAME” Disaster Recovery Staffing Policy

 “YOUR AGENCY NAME” Information Resource Acceptable Use Policy

 “YOUR AGENCY NAME” Information Security Incident Reporting Procedure

 “YOUR AGENCY NAME” Information Security Incident Response Procedure

**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” Virginia Information Technologies Agency; ““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 Information Security Policy |
| 2 | 11/21/2021 | Formatting changes |

**Attachment 1**

**Information Security Access Agreement**

**Commonwealth of Virginia**

**Virginia Information Technologies Agency**

As a user of the Commonwealth of Virginia's information technology services, I understand and agree to abide by the following terms which govern my access to and use of these information technology services:

Access has been granted to me as a necessary privilege in order to perform authorized job functions for the Commonwealth. I understand and agree that I am prohibited from using or knowingly permitting use of any assigned or entrusted access control mechanisms (such as log-in IDs, passwords, terminal IDs, user IDs, file protection keys or production read/write keys) for any purpose other than those required to perform my authorized job functions;

I understand and agree that I will not disclose information concerning any access control mechanism of which I have knowledge unless properly authorized to do so, and I will not use any access mechanism which has not been expressly assigned to me;

I agree to abide by all applicable Commonwealth of Virginia policies, standards and guidelines and “YOUR AGENCY NAME” policies and procedures, which relate to the security of Commonwealth information technology services and the information contained therein;

If I observe any incidents of non-compliance with the terms of this agreement, I am responsible for reporting them to the Commonwealth’s Chief Information Security Officer;

**By signing this agreement**, I hereby certify that I understand the preceding terms and provisions and that I accept the responsibility of adhering to the same. I further acknowledge that any infractions of this agreement will result in disciplinary action, including but not limited to the termination of my access privileges.

**Employee/Business Partner (Print)** **Date:\_\_\_\_\_\_\_\_**

**Employee/Business Partner (Signature):\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Virginia Information Technologies Agency:**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

 **Division Name**