COMMONWEALTH OF VIRGINIA

Information Technology Resource Management

Information Security Policy

Virginia Information Technologies Agency (VITA)

ITRM Publication Version Control

ITRM Publication Version Control: It is the User's responsibility to ensure they have the latest version of this ITRM publication. Questions should be directed to VITA's Director for Enterprise Architecture (EA) Division within the Commonwealth Security and Risk Management Directorate. EA will issue a Change Notice Alert and post on the VITA Web site, provide an email announcement to the Agency Information Technology Resources (AITRs) and Information Security Officers (ISOs) at all state agencies and institutions of higher education as well as other parties EA considers to be interested in the change.

This chart contains a history of this ITRM publication's revisions.

Version	Date	Purpose of Revision
Original	1990	Base Document: COV ITRM Policy 90.1 Information Technology Security Policy
Revision 1	12/07/2001	Revision to align with current information security best practices.
Revision 2	07/01/2006	Re-designation of COV ITRM 90.1 to COV ITRM SEC500-02 and complete revision of the policy.
Revision 3	07/01/2007	Revision to align with changes to the *Code of Virginia.* A "legal black line" highlights all changes in this document.
Revision 4	10/30/2007	Revision to incorporate ITIB's directive (dated October 18, 2007) to change compliance date from July, 2008 to November 1, 2007 for section 3.1.8.
Revision 5	07/17/2008	Revision to remove language in the scope section that excluded "Academic Instruction and Research" systems and added language to recognize several legislative mandates relating to data security and privacy in the "Statement of Policy" section. The document was also revised to clarify the Commonwealth's IT Security Program and reference that the components of that program are implemented by requirements contained in related IT security standards. All changes are identified in "Blue" along with a "legal black line" to the right of these changes.
SEC519-00	07/24/09	Re-designation of COV ITRM SEC500-02 to COV ITRM SEC519-00 due to substantial rewrite of the Commonwealth's IT Security Policy. Revision to streamline this policy to provide direction regarding the intent and structure of the COV Security Program. This *Policy* has been broadened to include security best practices holistically. Requirement statements have been moved to security standards.
Reviewed	06/17/2014	No changes
SEC519-01	09/15/2021	This document was rewritten. Change markings are not included.

Identifying Changes in This Document

See the latest entry in the table above.

Vertical lines in the left margin indicate that the paragraph has changes or additions.
Specific changes in wording are noted using italics and underlines; with italics only indicating new/added language and italics that is underlined indicating language that has changed.

The following examples demonstrate how the reader may identify updates and changes:

Example with no change to text – The text is the same.

Example with revised text – This text is the same. *A wording change, update or clarification has been made in this text*.

Example of new section – *This section of text is new.*

Review Process

Enterprise Architecture (EA) Division provided the initial review of this publication.

Online Review

All Commonwealth agencies, stakeholders, and the public were encouraged to provide their comments through the Online Review and Comment Application (ORCA). All comments were carefully evaluated and individuals that provided comments were notified of the action taken.

Agency Online Review

The report was posted on VITA's Online Review and Comment Application (ORCA) for 30 days. All agencies, stakeholders, and the public were encouraged to provide their comments through ORCA. All comments were carefully evaluated and individuals that provided comments were notified of the action taken.

PREFACE

Publication Designation
ITRM Policy SEC519-01

Subject
Information Security Policy

Effective Date
September 15, 2021

Compliance Date
September 15, 2021

Supersedes
COV ITRM Policy SEC500-02
SEC519-00

Scheduled Review
Two (2) years from effective date

Most Recent Review
June 17, 2014

Authority
Code of Virginia, §2.2-2009 (Additional Powers of the CIO relating to security)
Code of Virginia, §2.2-603
(Authority of Agency Directors)
Code of Virginia (§ 2.2-5514) (Prohibition on the Use of Certain Products and Services)

Scope
This policy is applicable to the Commonwealth's executive, legislative, and judicial branches, as well as independent and institutions of higher education (collectively referred to as "Agency"). This policy is offered only as guidance to local government entities.

Purpose
To protect the Commonwealth information assets by defining the minimum information security program for agencies of the Commonwealth of Virginia (COV). This policy establishes the Commonwealth Information Security program as a comprehensive framework for agencies to follow in developing agency security programs to reduce the risk to COV information irrespective of the medium containing the information.

General Responsibilities
(Italics indicate quote from the Code of Virginia requirements)

Chief Information Officer of the Commonwealth
In accordance with Code of Virginia, § 2.2-2009, the Chief Information Officer (CIO) is assigned the following duties: "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. Such policies, procedures, and standards will apply to the Commonwealth's executive, legislative, and judicial branches, and independent agencies and institutions of higher education. The CIO shall work with representatives of the Chief Justice of the Supreme Court and Joint Rules Committee of the General Assembly to identify their needs."

Chief Information Security Officer
The Chief Information Officer (CIO) has designated the Chief Information Security Officer (CISO) to develop Information Security policies, procedures and standards to protect the confidentiality, integrity, and availability of the Commonwealth's information assets.

Virginia Information Technologies Agency (VITA) At the direction of the CIO, VITA leads efforts that draft, review and update technical and data policies, standards, and guidelines for information technology and related systems. VITA uses requirements in IT technical and data related policies and standards when establishing contracts, reviewing procurement requests, agency IT projects, budget requests and strategic plans, and when developing and managing IT related services.

Executive Branch Agencies Provide input and review during the development, adoption and update of statewide technical and data policies, standards and guidelines for information technology and related systems.

Judicial and Legislative Branches In accordance with the Code of Virginia §2.2-2009: the: "CIO shall work with representatives of the Chief Justice of the Supreme Court and Joint Rules Committee of the General Assembly to identify their needs."

Glossary of Security Definitions
As appropriate, terms and definitions used in this document can be found in the COV ITRM IT Glossary. The COV ITRM IT Glossary may be referenced on the ITRM Policies, Standards and Guidelines web page at http://www.vita.virginia.gov/library/default.aspx?id=537.

Related Policies, Standards, and Guidelines Current version of all COV ITRM Security Standards (SEC), NIST 800-53

TABLE OF CONTENTS

1. INFORMATION SECURITY POLICY STATEMENT

1.1 Background

The Commonwealth of Virginia (COV) utilizes Commonwealth information to provide state government services. Such information is contained in a myriad of mediums including paper, electronic records, voice mail, the spoken word, etc.

Agency information security programs are built on the concept of public trust. An agency information security program provides a sustainable consistent approach to information safeguards that can be replicated across paper and electronic files, systems and transactions. The COV Information Security Program provides the framework and practices for Agencies to use in securing their information. The COV Information Security Program is designed to provide direction and assistance to agencies in developing and implementing agency information security programs that reduce the risk to COV information irrespective of the medium containing the information.

The Commonwealth relies increasingly on electronic records utilizing information technology (IT) for the effective delivery of government services. Rapid and continuing technical advances have increased the dependence of COV agencies on IT and their reliance on various security measures to protect agency electronic information. This policy establishes the Commonwealth Information Security Program as a comprehensive framework for agencies to follow in developing agency security programs that protect their information.

1.2 Guiding Principles

The following principles guide the development and implementation of the COV Information Security Program.

a. COV sensitive information is any data of which the compromise with respect to confidentiality, integrity, and/or availability could adversely affect COV interests, the conduct of Agency programs, or the privacy to which individuals are entitled.

b. Information security is:
    1. A cornerstone of maintaining public trust;
    2. Managed to address both business and technology requirements;
    3. Risk-based and cost-effective;
    4. Aligned with agency and COV priorities, industry best practices, and government requirements;
    5. Directed by policy but implemented by business owners; and
    6. Applied holistically irrespective of medium.

1.3 Statement of Policy

It is the policy of the COV (§2.2-603.F) that each Agency Head is responsible for securing the electronic data that is held by the agency and shall comply with the requirements of §2.2-2009. In addition, the Director of every department is responsible for the security of the agency's electronic information, and for establishing and maintaining an agency information security program compliant with this policy and meets all of the requirements established by COV ITRM Security Standards.

This policy and related standards provide the security framework that each agency will use to establish and maintain their information security program. Agency Heads may establish additional, more restrictive, information security programs, but must establish a documented

program that meets the requirements of this *Policy* and related *Standards,* at a minimum. If, in the judgment of the Agency Head, the agency cannot meet one or more of the requirements established by COV ITRM Security Standards, the Agency Head can submit an exception to request acceptance of risk.

In addition, agencies that have access to, or handle information that is subject to laws or regulations should ensure compliance with those respective requirements. For example, agencies could be subject to laws and regulations including, but not limited to the following:

- Health Insurance Portability and Accountability Act of 1996 (HIPAA);
- Internal Revenue Service (IRS) 1075;
- Privacy Act of 1974;
- Payment Card Industry (PCI) Standard;
- Rehabilitation Act of 1973;
- §508 General Services Administration (GSA) Government-wide IT Accessibility Program;
- Criminal Justice Information Services (CJIS);
- Social Security Administration (SSA);
- Federal Education Rights and Privacy Act of 1974 (FERPA); and
- National Institute of Standards and Technology (NIST).

2. COV Information Security Program

The COV Information Security Program establishes the requirements for creating and implementing agency information security policies and procedures to protect COV information from threats, whether internal or external, deliberate or accidental. The COV Information Security Program includes the use of all reasonable information security control measures to:

- Protect COV information against unauthorized access and use;
- Maintain the integrity of COV information;
- Ensure COV information is available when needed; and
- Comply with the appropriate federal or state legislated and regulatory requirements.

2.1 Key Security Roles

Key security roles in the COV Information Security Program are assigned to individuals. The roles 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 segregation of duties, provide adequate protection against the possibility of fraud, and do not lead to a conflict of interests. While this section lists the roles, specific requirements related to these roles are defined in the current version of the *ITRM Standard (SEC501)*.

Chief Information Officer of the Commonwealth (CIO)
Chief Information Security Officer (CISO) of the Commonwealth
Agency Head
Information Security Officer (ISO)
Privacy Officer [Note: When required by law, otherwise optional]
System Owner
System Administrator
Data Owner
Data Custodian

IT System Users

2.2 Information Security Program The policy of the COV is to secure its electronic information using methods based on the sensitivity of the information and the risks to which the information are subject, including the dependence of critical agency business processes on the information and related systems.

The COV Information Security Program framework addresses the requirements set forth in § 2.2-2009 *Additional duties of the CIO relating to security of government information*. The COV Information Security Program includes:

- Development of policies, standards, and guidelines that provide for the security of state government electronic information;
- Addressing the scope and frequency of security audits;
- Preventing unauthorized use, intrusions, or other security threats;
- Provide for the protection of confidential data;
- Developing and maintaining a risk management program designed to identify information technology security gaps and develop plans to mitigate the gaps;
- Requiring that any contract for information technology entered into by the Commonwealth address compliance with applicable federal laws and regulations pertaining to information security and privacy;
- Preparation of annual reports to the Governor, the Secretary, and General Assembly on the status of IT security governance;
- Promptly receive reports of incidents that threaten Commonwealth data from directors of departments in the executive branch of state government and take such actions as are necessary, convenient, and desirable to ensure the security of the Commonwealth's electronic information (§ 2.2-603);
- Providing technical guidance to Department of General Services (DGS) in the development of policies, standards, and guidelines for the recycling and disposal of computers and other technology assets;
- Providing all agencies information, guidance, and assistance related to IT security policies, standards, and guidelines;
- Identification and notification of all hardware and software that has been prohibited pursuant to Chapter 55.3 (§ 2.2-5514); and
- Developing a curriculum and materials for training all state employees in information security awareness.

2.2.1 Standards

IT Security Standards are included below.

- SEC501 IT Security Standard defines the IT security control activities to protect confidential records, maintain information integrity, and preserve information availability. (See § 2.2-2009 A.2., A.3., A.5.)

- SEC525 Hosted Environment IT Security Standard establishes a baseline for information security and risk management activities associated with Commonwealth data stored in a data center not owned or leased by the Commonwealth of Virginia. (See § 2.2-2009 A.2.,

A.3., A.5.)

Other Standards

- SEC502 IT Security Audit Standard defines the scope and frequency of IT security audits for COV agencies and the requirements to complete a successful audit. (See § 2.2-2009.A.1.)

- SEC511 IT Standard Use of Non-Commonwealth Computing Devices to Telework is intended to protect COV information technology assets and the data they process and store while supporting agency teleworking activities.

- SEC514 Removal of Commonwealth Data from Electronic Media Standard defines the requirements for removing Commonwealth data when electronic media is disposed or replaced. (See § 2.2-2009.F.)

- SEC520 Risk Management Standard defines the risk management activities for COV agencies, including the requirements for a business impact analysis (BIA) and risk assessments. (See § 2.2-2009.A.4.)

- SEC527 Cybersecurity Awareness Training Standard defines the curriculum and materials for training all state employees in information security awareness and in proper procedures for detecting, assessing, reporting, and addressing information security threats. (See § 2.2-2009.I.)

2.2.2. IT Security Governance Reporting

The CIO creates an annual report to the Governor, the Secretary, and General Assembly. This report includes: the results of security audits, the extent to which security policy, standards, and guidelines have been adopted by executive branch and independent agencies, and a list of those executive branch agencies and independent agencies that have not implemented acceptable security and risk management regulations, policies, standards, and guidelines to control unauthorized uses, intrusions, or other security threats. (See § 2.2-2009 B.)

The CIO also conducts an annual comprehensive review of cybersecurity policies of every executive branch agency, with a particular focus on any breaches in information technology that occurred in the reviewable year and any steps taken by agencies to strengthen cybersecurity measures. The CIO shall issue a report of his findings to the Chairmen of the House Committee on Appropriations and the Senate Committee on Finance. Such report shall not contain technical information deemed by the CIO to be security sensitive or information that would expose security vulnerabilities. (See § 2.2-2009 C.)

Note: VITA requirements will not infringe upon the responsibilities assigned to the Comptroller, the Auditor of Public Accounts, or the Joint Legislative Audit and Review Commission by other provisions of the Code of Virginia. (See § 2.2-2009 D.)

2.2.3. Incidents

CIO receives reports of incidents from Agency Heads in the executive branch of state government. Agency heads shall report to the Chief Information Officer all known incidents that threaten the security of the Commonwealth's data within 24 hours from when the department discovered or should have discovered their occurrence. (See § 2.2-2009 E and §2.2-603)

2.2.4. Removal of Commonwealth Data from Electronic Media

The CIO provides technical guidance to the Department of General Services in the development of policies, standards, and guidelines for the recycling and disposal of computers and other technology assets. Such policies, standards, and guidelines include the expunging of all confidential data and personal identifying information of citizens of the Commonwealth prior to such sale, disposal, or other transfer of computers or other technology assets. These requirements are outlined in *ITRM Standard SEC514 Removal of Commonwealth Data from Electronic Media Standard* (See § 2.2-2009.F.)

2.2.5. Provide IT Security Resources

The IT security program includes training and agency outreach to help agencies understand and adhere to security policies and standards (See § 2.2-2009.G.)

2.2.6. Prohibited Hardware, Software, Services Notification

The CIO will identify any hardware, software, or services that are prohibited for use by Commonwealth entities. Prohibited items will be included in *ITRM Standard SEC528 Prohibited Hardware, Software and Services Policy* (See § 2.2-2009.H.)

2.2.7. Cybersecurity Awareness Training

The CIO established *ITRM Standard SEC527 Cybersecurity Awareness Training Standard* for the Executive, Judicial, Legislative, and Independent agencies. The Cybersecurity Awareness Training Standard defines the curriculum and materials for training all state employees in information security awareness and in proper procedures for detecting, assessing, reporting, and addressing information security threats (See § 2.2-2009.I.)

3. User Agreement to Monitoring

Users must comply with all requirements of *DHRM 1.75 Use of Electronic Communications and Social Media*, which defines the appropriate use of COV information technology by COV employees, and any applicable agency policies. Any use of COV information technology resources constitutes consent to monitoring of that use and any activities that may be conducted through COV IT resources, whether or not a warning banner is displayed. There is no expectation of privacy when utilizing COV information technology resources.

The COV and agencies reserve the right to:

a. Review the data contained in or traversing COV information resources including social media

b. Review the activities on COV information IT resources.

c. Act on information discovered as a result of monitoring and disclose such information to law enforcement and other organizations as deemed appropriate by the Agency Head.

d. Monitor at any time, without notice and without the user's permission.

4. Process for Requesting Exceptions

If an Agency Head determines that compliance with the provisions of this *policy* or any related information security standards would adversely affect a business process of the agency, the Agency Head may request

approval to deviate from a specific requirement by submitting an exception request to the CISO. For each exception, the requesting agency shall fully document:

- The business need;
- The scope and extent;
- Mitigating safeguards;
- Residual risks;
- The specific duration; and
- Agency Head approval.

Each request shall be approved by the Agency Head indicating acceptance of the defined residual risks prior to submission to the CISO. Requests for exception shall be evaluated and decided upon by the CISO, and the requesting party informed of the action taken. An exception cannot be processed unless all residual risks have been identified and the Agency Head has approved, indicating acceptance of these risks. Denied exception requests may be appealed to the CIO of the Commonwealth.

Any agency requesting an exception to any requirement of this policy and the related Standards must document their request. The Exception Request Form must be submitted in the Commonwealth's Enterprise Governance Risk and Compliance (eGRC) system. The form is also included in the appendix of *ITRM SEC501* and on the website at: https://www.vita.virginia.gov/it-governance/itrm-policies-standards/#securityPSGs