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 Policy Practice and Architecture (PPA) within the Information Technology Investment and Enterprise Solutions (ITIES) Directorate. PPA 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 PPA 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.

Review Process

Technology Strategy and Solutions Directorate Review

N. Jerry Simonoff, VITA Director of Information Technology Investment and Enterprise Solutions (ITIES), and Chuck Tyger, Director for Policy, Practices, and Architecture Division, provided the initial review of the report.

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 SEC519-00

Subject
Information Security Policy

Effective Date
July 24, 2009

Compliance Date

Supersedes
COV ITRM Policy SEC500-02
Date: July 17, 2008 (Revision 5)

Scheduled Review
Two (2) years from effective date

Authority
Code of Virginia, §2.2-2009
(Additional Powers of the CIO relating to security)

Scope
This policy is applicable to the Commonwealth's executive, legislative, and judicial branches and 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.

Information Technology Investment and Enterprise Solutions Directorate
In accordance with the *Code of Virginia* § 2.2-2010, the CIO has assigned the Information Technology Investment and Enterprise Solutions Directorate the following duties: *Develop and adopt policies, standards, and guidelines for managing information technology by state agencies and institutions*."

International Standards
International Standard, Information Technology – code of practice for information security management, ISO/IEC 27002.

Related ITRM Standard
Current version of COV ITRM Standard SEC501: Information Security Standard

TABLE OF CONTENTS

1. INFORMATION SECURITY (IS) 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:

   1. A critical asset that shall be protected; and

   2. Restricted to authorized personnel for official use.

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;

6. Applied holistically irrespective of medium.

1.3 Statement of Policy

It is the policy of the COV that each Agency Head is responsible for the security of the agency's electronic information, and for establishing and maintaining an agency information security program that is 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, at a minimum, establish a documented program that meets the requirements of this *Policy* and related *Standards*. 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 accept residual risks and approve the exception for submission to the Chief Information Security Officer (CISO) utilizing the form and defined processes in the Appendix of this document.

In addition, agencies that have access to, or handle information that is subject to laws or regulations (e.g., Health Insurance Portability and Accountability Act of 1996 (HIPAA), Internal Revenue Service (IRS) 1075, the Privacy Act of 1974, the Payment Card Industry (PCI) Standard, the Rehabilitation Act of 1973, §508, or the Federal National Security Standards) should ensure that those respective requirements are addressed within the agency's information security program.

2. COV INFORMATION SECURITY PROGRAM

The COV Information Security Program establishes the requirements for creating and implementing agency information security programs 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;
- Comply with the appropriate federal or state legislated and regulatory requirements.

2.1 Key Security Roles

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 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 COV ITRM Security Standard (SEC501).

Chief Information Officer of the Commonwealth (CIO)
Chief Information Security Officer (CISO)
Agency Head
Information Security Officer (ISO) [Note: Should report to the Agency Head where practical]
Privacy Officer [Note: When required by law, otherwise optional]
IT System Users

2.2 Information Security Program Component Areas

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, including appropriate standards, guidelines, procedures, templates, and other tools that agencies can use to develop and administer their agency information security programs, is comprised of nine component areas. These components provide the basis for designing the agency's information security program and safeguards. They do not represent organizational functions within the information security program, but rather the functional areas of the information security program.

2.2.1 Risk Management

Risk Management addresses protecting COV information and IT systems commensurate with sensitivity and risk, including system availability needs. Accordingly, Risk Management is a central component of an agency information security program and allows each agency to determine how these factors apply to its IT systems and data.

2.2.2 IT Contingency Planning

IT Contingency Planning defines processes and procedures that plan for and execute recovery and restoration of IT systems and information that support essential business functions if an event occurs that renders the IT systems and information unavailable. Contingency Planning includes Continuity of Operations Planning, Disaster Recovery Planning, and IT System Backup and Restoration.

2.2.3 IT Systems Security

IT Systems Security defines the steps necessary to provide adequate and effective protection for agency IT systems and information in the areas of IT systems security plans, information system hardening, information systems

interoperability security, malicious code protection, and systems development life cycle security.

2.2.4 Logical Access Control

Logical Access Control defines the steps necessary to protect the confidentiality, integrity, and availability of IT systems and information against compromise. Logical Access Control requirements identify the measures needed to verify that all system users are who they say they are and that they are permitted to use the systems and information they are attempting to access. Logical Access Control defines requirements in the areas of account management, password management, and remote access.

2.2.5 Data Protection

Data Protection provides security safeguards for the processing and storing of data. This component outlines the methods that agencies can use to safeguard the electronic information, irrespective of medium, in a manner commensurate with the sensitivity and risk of the information stored. Data Protection includes requirements in the areas of media protection and encryption.

2.2.6 Facilities Security

Facilities Security safeguards require planning and application of facilities security practices to provide a first line of defense for COV electronic information against damage, theft, unauthorized disclosure of information, loss of control over system integrity, and interruption to computer services.

2.2.7 Personnel Security

Personnel Security controls reduce risk to COV information by specifying access determination and control requirements that restrict access to information to only individuals who require such access as part of their job duties. Personnel Security also includes security awareness and training requirements to provide all IT system users with appropriate understanding regarding COV Information Security Policies and acceptable use requirements for IT systems and data.

2.2.8 Threat Management

Threat Management addresses protection of IT systems and information by preparing for and responding to information security incidents. This includes threat detection, incident handling, and security monitoring and logging.

2.2.9 IT Asset Management

IT Asset Management concerns protection of the components that comprise IT systems by managing them in a planned, organized, and secure fashion. Asset Management includes IT asset control, software license management, and configuration management and change control.

Figure 1 illustrates the interaction of the component areas of the COV Information Security Program that will enable COV agencies to accomplish their missions in a safe and secure environment when creating, maintaining, using, or disposing electronic records and processing such records with automated information systems.

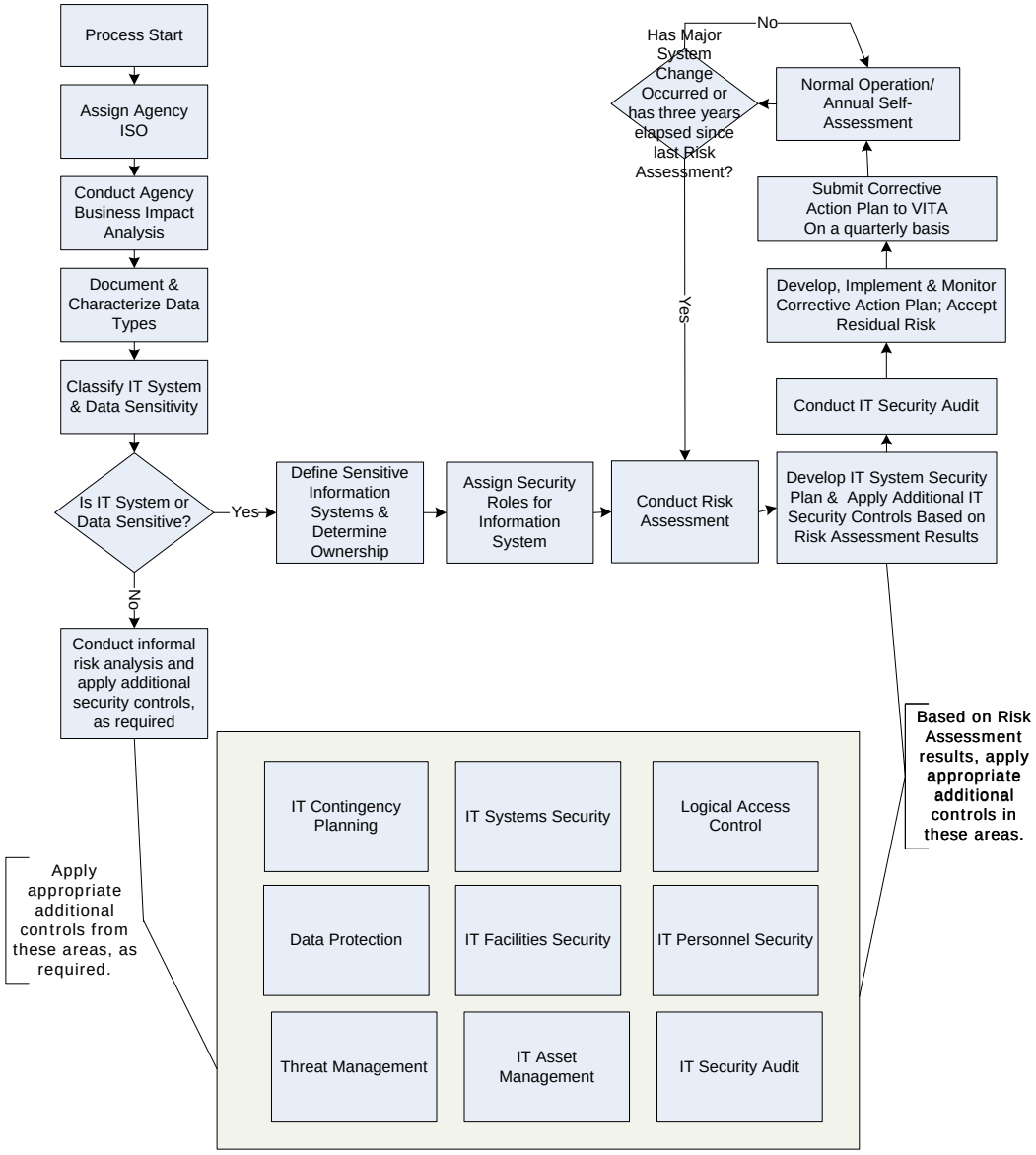

Figure 1 - Commonwealth of Virginia Information Security Program Framework

2.3 Compliance

The COV measures compliance with information security policies and standards through processes that include, but are not limited to monitoring and audits.

2.3.1 Monitoring

2.3.1.1 General Monitoring Activities

Monitoring is used to improve information security, to assess appropriate use of COV information technology resources, and to protect those resources from attack. Use of COV information technology resources constitutes permission to monitor that use. There is no expectation of privacy when utilizing COV information technology resources. The COV reserves the right to:

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

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.

2.3.1.2 User Agreement to Monitoring

Any use of COV information technology resources constitutes consent to monitoring activities that may be conducted whether or not a warning banner is displayed.

2.3.2 IT Security Audits

The Code of Virginia § 2.2-2009 gives the CIO the responsibility to *"direct the development of policies, procedures and standards for performing security audits of state electronic information."* Specific requirements related to performing IT security audits are contained in the current version of the *IT Security Audit Standard* (COV ITRM SEC502).

3. 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 impact 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 in writing to the CISO and approved by the Agency Head indicating acceptance of the defined residual risks. Included in each request shall be a statement detailing the reasons for the exception as well as mitigating controls and all residual risks. 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. The form that agencies must use to document exception requests is included in the Appendix to this document.

4. GLOSSARY AND LIST OF ACRONYMS

Please refer to the current version of the Commonwealth of Virginia Information Technology Resource Management Information Security Standard (COV ITRM Standard SEC 501) for the Glossary of Security Definitions and list of Acronyms.

APPENDIX – INFORMATION SECURITY POLICY AND STANDARD EXCEPTION REQUEST FORM

Any agency requesting an exception to any requirement of this policy and the related Standards must submit the form on the following page.

COV Information Security Exception Request Form

Agency Name: _____Contact for Additional Information: _____

Standard Name: _____

Standard requirement to which an exception is requested:_____

Note: This request is for an exception(s) to a requirement(s) of a component standard of the Commonwealth's Information Security Program and approval of this request does not in any way address the feasibility of operational implementation. You are encouraged to check with your technical support staff prior to submitting this request.

1. Provide the **Business or Technical Justification:**

2. Describe the scope including quantification and requested duration (not to exceed one (1) year):

3. Describe all associated risks:

4. Identify the controls to mitigate the risks:

5. Identify all unmitigated risks:

I have evaluated the business issues associated with this request and I accept any and all associated risks as being reasonable under the circumstances.

_____	_____	_____
Printed name Agency Head	**Signature**	**Date**

Chief Information Security Officer of the Commonwealth (CISO) Use Only

Approved_____ Denied_____ Comments:

_____ _____
CISO Date

Agency Request for Appeal Use Only

Approved_____ Comments:

_____ _____
Agency Head Date

Chief Information Officer of the Commonwealth (CIO) Office Use Only (Appeal)

Appeal Approved_____ Appeal Denied_____ Comments:

_____ _____
CIO Date