

COMMONWEALTH OF VIRGINIA



Information Technology Resource Management Policy

INFORMATION TECHNOLOGY SECURITY POLICY

Department of Technology Planning

Preface

Publication Designation

COV ITRM Policy 90-1

Subject

Information Technology Security

Effective Date

May 19, 1995

Supersedes

COV ITRM Policy 90-1, dated December 9, 1991

Scheduled DTP Review

One (1) year from the effective date, and annually thereafter.

Authority

Code of Virginia, § 2.2-226
(Powers and Duties of the Secretary of Technology)

Code of Virginia, § 2.2-2651
(Powers and Duties of the Council on Technology Services)

Code of Virginia, § 2.2-1701
(Powers and Duties of the Department of Technology Planning)

Scope

This policy is applicable to all state agencies and institutions of higher education (hereinafter collectively referred to as "agencies") that are engaged in such functions as planning, managing, developing, purchasing, and using information technology resources in the Commonwealth. Local government entities are encouraged to consider the implications of this policy for their work.

Purpose

To define the Commonwealth's information technology security program and the minimum security requirements for a State agency's security program. This policy recognizes that overall information technology security for the Commonwealth is achieved through the

collective operation of the State agency programs.

Objectives

The objective of this policy is to establish and promulgate guidance for the protection of Commonwealth information technology resources and sensitive information.

General Responsibilities

Secretary of Technology

In accordance with the *Code of Virginia*, the Secretary of Technology, as Chief Information Officer for the Commonwealth, is assigned the following duties: "Direct the formulation and promulgation of policies, standards, specifications and guidelines for information technology in the Commonwealth..."

Council on Technology Services (COTS)

In accordance with the *Code of Virginia*, the Council on Technology Services is assigned the following duties: "establishes COTS to advise and assist the Secretary of Technology in exercising the powers and performing the duties conferred..."

Department of Technology Planning (DTP)

In accordance with the *Code of Virginia*, the Department of Technology Planning is assigned the following duties: "develop and adopt policies, standards, and guidelines for managing information technology in the Commonwealth".

All State Agencies

Responsible for complying with COV ITRM policies and standards and considering COV ITRM guidelines issued by the Secretary of Technology.

Definitions

See Glossary

Related COV ITRM Policies, Standards, and Guidelines

COV ITRM Standard SEC2001-01.1, Information Technology Security Standard

COV ITRM Guideline SEC001-01.1, Information Technology Security Guideline

Table of Contents

Statement of ITRM Policy for Information Technology Security.....	1
Glossary	2

Statement of ITRM Policy for Information Technology Security

The Commonwealth relies heavily on the application of information technology for the effective management of governmental programs. Rapid and continuing technical advances have increased the dependence of State agencies on information systems. The value of State information, software, hardware, telecommunications, and facilities must be recognized by agencies as an important State resource, and be protected through agency security programs.

It is the policy of the Commonwealth that each agency head is responsible for the security of the agency's information technology resources and that all State agencies shall take appropriate steps to secure their information technology resources and sensitive information through the development of an agency information technology security program. As security encompasses a broad spectrum of safeguards, each agency should determine which information resources must be protected. All systems must include security safeguards that reflect the true importance of the information processed on the system and/or the State's investment embodied in the components of the information technology system.

The specific structure of an agency's information technology security program will vary depending on the scope and nature of the information technology resources and sensitive information for which the agency is responsible. Moreover, each agency's information environment will determine in large measure the manner in which agencies establish and maintain an effective information technology security program.

All agencies must maintain documentation of their information technology security program consistent with the requirements of the *Information Technology Security Standard*, COV ITRM Standard SEC2001-01.1

Glossary

Critical (or Mission Critical) – The term “critical” refers to those information resources whose unavailability or improper use has the potential to adversely affect the ability of an Agency to accomplish its mission.

Confidential Information – The term “confidential information” refers to information prohibited from public disclosure that may cause harm to the state, its citizens or other individuals or organizations.

Information – The term “information” means any communication or representation of knowledge such as facts, data or opinions in any medium or form, including textual, numerical, graphic, cartographic, narrative or audiovisual forms.

Information Resources – The term “information resources” includes government information, information technology and associated personnel.

Information Systems - The term “information systems” means a discrete set of information resources

organized for the collection, processing, maintenance, transmission and dissemination of information, in accordance with defined procedures.

Information Technology – The term “information technology” means any equipment or interconnected system or subsystem of equipment, that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission or reception of data or information by an Agency. The term information technology includes computers, ancillary equipment, software, firmware and similar procedures, services and related resources.

Sensitive Information – Sensitive information refers to any confidential or critical information for which the loss, misuse, or unauthorized access to or modification or improper disclosure could adversely affect the Commonwealth’s interest, the conduct of Agency programs, or the privacy to which individuals are entitled.