

# COMMONWEALTH OF VIRGINIA



**Information Technology Resource Management Standard**

## **INFORMATION TECHNOLOGY SECURITY STANDARD**

**Department of Technology Planning**

## Preface

### Publication Designation

COV ITRM Standard SEC2001-01.1

### Subject

Information Technology Security

### Effective Date

December 7, 2001

### Supersedes

COV ITRM Standard SEC2000-01.1, Information Technology Security, dated October 13, 2000

### Scheduled Review

One (1) year from effective date

### 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)

Code of Virginia § 2.2-3803  
(Administration of systems including personal information; Internet privacy policy)

Executive Order 51 (99)  
(Implementing Certain Recommendations by the Governor's Commission on Information Technology)

### Scope

This standard is applicable to all State agencies and institutions of higher education (collectively referred to as "Agency") that manage, develop, purchase, and use information technology resources in the Commonwealth. However, Academic "instruction or research" systems/infrastructures that are completely isolated from "administrative and business" systems/infrastructures are exempt from this standard. This standard is offered as guidance only to local government entities.

### Purpose

- 1) To define the minimum requirements for the administration of an agency's information technology security program.
- 2) To promote secure communications and the appropriate protection of information resources within the Commonwealth.
- 3) To facilitate the alignment and adaptation of security technology to the business needs of the Commonwealth.

### Objectives

- Define and promulgate the minimum security standards for the protection of the Commonwealth's information technology resources and sensitive information;
- Provide for the compilation of planning material and documentation to support the development of information technology security programs.
- Clarify the security components to be addressed as part of an Agency's security program.

### 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 promulgate policies, standards, and guidelines for managing information technology in the Commonwealth".

#### Department of Information Technology (DIT)

*EO-51 (99)*. D – Directs that "DIT shall develop policies and procedures regarding access to state databases and data communications in order to ensure the security of such databases from unauthorized use, intrusion, or other security threats. DIT shall coordinate the implementation of such policies and procedures with agencies maintaining databases hosted outside of the State Data Center.

**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 Policy 90-1: Information Technology Security (Revised 05/19/95)

COV ITRM Guideline SEC2001-01.1: Information Technology Security Guideline

## Table Of Contents

Executive Summary .....	1
Background .....	2
Approach.....	2
Reviews .....	3
Statement of ITRM Requirements for Information Technology Security.....	4
A. Business Analysis and Risk Assessment.....	4
B. Security Awareness .....	5
C. Technical Training.....	7
D. Technical Communications .....	7
E. Authentication, Authorization and Encryption.....	8
F. Data Security.....	9
G. Systems Interoperability Security .....	10
H. Physical Security.....	10
I. Personnel Security .....	11
J. Threat Detection .....	12
K. Security Tool Kit .....	13
L. Incident Handling .....	13
M. Monitoring and Controlling System Activities.....	14
Business Continuity Planning.....	16
Glossary .....	17
Appendix A: High Level Flowchart “Information Technology Security Program Development Cycle”.....	19
Appendix B: Assignment of Uniform Alphanumeric Publication Designations for all Policies, Standards, and Guidelines.....	21

## Executive Summary

The continuing support and involvement of top State agency management is a prerequisite for an effective information technology security program. Management's responsibilities shall include the following:

- Designating an Information Systems Security Officer for the Agency who administers the information technology security function.
- Determining the optimal place of the security function within the agency hierarchy with the shortest practicable reporting lines to the agency head.
- Approving a business impact analysis, a risk assessment, and a continuity plan.
- Facilitating the communication process between data processing managers and those in other areas of the organization.
- Establishing a program of security safeguards.
- Establishing and providing for a security awareness and training program.

The Information Systems Security Officer for the Agency shall maintain documentation of the Agency's information technology security program. It is the vehicle that will be used to communicate the specific procedures needed to implement the security program. It shall contain information on all aspects of the program, inclusive of the following *thirteen security components*:

business impact and risk assessment; security awareness; technical training; technical communications; authentication, authorization and encryption; data security; systems interoperability security; physical security; personnel security; threat detection; security tool kit; incident handling; monitoring and controlling systems activities.

This standard supports the Security Architecture endorsed by the Council on Technology Services. Additionally, those security best practices that are recommended as associative guidelines, but which are not mandatory, are stated in COV ITRM Guideline SEC2001-01.1, Information Technology Security Guideline.

## Background

This standard is applicable to all State agencies and institutions of higher education (collectively referred to as “Agency”) that manage, develop, purchase, and use information technology resources in the Commonwealth. It is consistent with the provisions of COV ITRM Policy 90-1: Information Technology Security (Revised 05/19/95). However, Academic “instruction or research” systems/infrastructures that are completely isolated from “administrative and business” systems/infrastructures are exempted from this standard.

Responsibility for the development of the Agency’s Information Technology Security Program begins at the management level and flows down through the agency or institution to the individual user.

- Each Agency head is responsible for the security of the Agency’s information technology resources.
- The Information Systems Security Officer, appointed by the head of each Agency, is responsible for implementing and maintaining adequate information technology security programs.
- Owners are responsible for determining adequate and appropriate levels of protection for the information technology resources under their control to prevent unauthorized access or disclosure and to ensure effective and accurate processing and continuity of operations for accomplishment of the organization’s mission.
- Custodians are responsible for ensuring the adequate and appropriate levels of protection for the information technology resources under their supervision to prevent unauthorized access or disclosure, and to ensure effective and accurate processing and continuity of operations for accomplishment of the organization’s mission.
- Each employee, including owners, custodians, and users, is responsible for the adequate protection of information technology resources within their control or possession.

Appendix A provides a high-level flow chart for developing and implementing an Agency Information Technology Security Program.

## Approach

The Commonwealth’s Security Architecture consists of the following set of thirteen components:

- Business Analysis and Risk Assessment
- Security Awareness
- Technical Training
- Technical Communications
- Authentication, Authorization and Encryption
- Data Security
- Systems Interoperability Security
- Physical Security
- Personnel Security

- Threat Detection
- Security Tool Kit
- Incident Handling
- Monitoring and Controlling System Activities

These components provide a framework to enable secure communications and the appropriate protection of information resources within the Commonwealth. In addition, they provide the basis for designing the Agency's security program and safeguards. Thus, for each component listed above a subset of standards has been identified that, together, comprise this ITRM Information Technology Security Standard.

In addition, as part of information technology security planning, agencies need to ensure that sensitive information is not compromised as a result of a disruption of business. Thus, a section that states the requirements for business continuity planning follows the above information technology security components.

## **Reviews**

A full review of the COV ITRM Standard SEC2001-01.1 is anticipated annually.

---

## Statement of ITRM Requirements for Information Technology Security

This section groups the specifications of the Information Technology Security Standard by the thirteen security components that comprise the Commonwealth's Security Architecture.

### A. Business Analysis and Risk Assessment

Business Analysis and Risk Assessment refer to those practices, technologies and/or services used to identify information resources that are confidential and/or critical to the Agency; and to identify and evaluate the potential security threats, and associated risks, to those resources.

The starting point of establishing effective information technology security is to identify the information resources that are owned and/or utilized by the Agency. "Information resources" include government information, information technology, and associated personnel. Once identified, the Agency needs to determine which of these resources require protection against unavailability, unauthorized access, or disclosure, i.e., their level of sensitivity. For example, various information may require protection under the "Government Data Collection and Dissemination Practices Act" (*Code of Virginia* § 2.2-3800) or the federal Health Insurance Portability and Accountability Act (HIPAA); or, the unavailability of a database may adversely affect the ability of an Agency to accomplish its mission. This process is referred to as business analysis (or business impact analysis).

Once the level of sensitivity of the information resources has been identified through the business impact analysis, the threats to which they are subject need to be identified and evaluated. This process is referred to as a risk assessment. As an example, the probability of each "threat event" occurring and the resultant impact of that event on the information resources could be assessed during this process. Examples of potential impacts that would adversely affect the Agency and/or State include financial loss, public embarrassment, loss of public confidence, noncompliance to State or Federal statutes, and degraded customer (public) service. The Agency needs to decide if and when a residual level of risk may be acceptable.

Based on the business impact analysis and the risk assessment, the Agency determines what types of safeguards are appropriate to address their defined risks. In this manner, the safeguards deployed reflect the true importance of the State's investment in the information resources used to accomplish the Agency's mission. (Subsections B through M address different types of security safeguards.) All implemented safeguards shall be referable back to the business impact analysis and risk assessment.

Business impact analysis and risk assessment is not viewed as just a one-time task or project, but rather as a tactical operational process. Both internal changes (e.g., changes to technical infrastructure or to applications) as well as external changes (e.g., technology advances, new Federal statutes, etc.) could directly impact the level of sensitivity and the threats applicable to information resources. Agencies, therefore, shall periodically deploy business impact analysis and risk assessment techniques to determine if their security safeguards are relevant and adequate, and then update their safeguards accordingly.

## A.1 Standards

A.1.a) The head of each Agency shall be responsible for the security of the Agency's information resources; and formally appoints an Information Systems Security Officer (ISSO) who is responsible for the development, implementation, oversight, and maintenance of the Agency's information security program.

A.1.b) Each Agency must establish, document, implement and maintain an information security policy and program appropriate to its business and technology environment. The policy and program must be consistent with Federal regulations (e.g., H.I.P.A.A; Rehabilitation Act Sec. 508) and State laws (e.g., "Government Data Collection and Dissemination Practices Act").

A.1.c) Security program documentation must specify how exceptions to security standards are to be handled. All such exceptions must be completely reviewed by a level of management above that approving the exception.

A.1.d) Each Agency must conduct a business impact analysis and risk assessment throughout the Agency (to include relevant business partners) to identify various levels of sensitivity associated with the information resources as defined; to identify the potential security threats to those resources; and to determine the appropriate level of security to be implemented to safeguard those resources. The business impact analysis and risk assessment can be reviewed and updated as needed, but at minimum must be reviewed and updated every three years.

A.1.e) Security programs must include protective measures and procedures to ensure that the appropriate levels of confidentiality, integrity and availability of data, information, and systems are sustainable.

A.1.f) Development, installation and/or changes to the Agency environment, technical infrastructure, and information systems must be reviewed for security implications and approved by the Agency's ISSO, or by person(s) delegated said approval authority by the Agency's ISSO, as part of the planning and design process; and then coordinated thoroughly during development and implementation. Acknowledgement of this review and approval by the Agency's ISSO, or delegated authority, must be documented and auditable.

A.1.g) Security programs must be coordinated and integrated with contingency planning and business resumption activities.

## B. Security Awareness

Security Awareness refers to those practices, technologies and/or services used to promote User awareness, User training and User responsibility with regards to security risks, vulnerabilities, methods, and procedures related to information technology resources. A "User" is an individual or group who has access to an information system and/or its data.

Users within an Agency need to understand the sensitivity of the Agency's information resources (discussed in Subsection A) and their responsibility in protecting those resources. For example, Users need to be aware of the threats and the associated impacts of a compromised password; of potential viruses transmitted over the Internet; of corrupted databases; and of the accessibility of printed information generated from the system.

Although, responsibility to adhere to State statutes and Agency policy and procedures are accepted by personnel upon engagement, Security Awareness programs provide a proactive mechanism to foster further comprehension of an individual's security responsibilities; to contextualize security responsibilities to specific job duties and case examples; to motivate personnel towards a security-conscious behavior while performing their duties; and to reinforce the consequences of security failures on the State, the Agency, its mission, its customers, and the User.

The appropriate amount, depth, and timing of Security Awareness is a risk-based decision. Best practices suggest that a Security Awareness program that utilizes a combination of periodic training sessions (introductory/refreshers) and on-going security awareness promotion (marketing) are most effective. In addition, where appropriate, an Agency may decide not to grant certain access rights to personnel until the desired level of Security Awareness Training has been successfully completed. Lastly, as the business and technical environment changes, security awareness material will need to be updated accordingly.

## **B.1 Standards**

B.1.a) Each Agency must establish and maintain information technology security awareness programs to ensure that all individuals are aware of their security responsibilities and know how to fulfill them.

B.1.b) A security awareness training program must:

- be approved by the Agency's Information Systems Security Officer (ISSO);
- specify timeframes for receiving training (initial, ongoing and/or refresher);
- provide both general and position appropriate security awareness content; and,
- be documented on an auditable medium.

B.1.c) All new hires who use information resources or who have access to areas where information resources reside, must receive formal security awareness training as designed by their Agency within 30 calendar days of their start date.

B.1.d) Receipt of Security Awareness Training must be documented in the employee's personnel file with employee's acknowledgement of receipt and understanding.

B.1.e) Security Awareness Refresher Training must be provided to personnel annually at a minimum.

## C. Technical Training

Technical Training refers to those practices, technologies and/or services used in training Security officers, system administrators and/or other personnel involved in the administration or development of information systems.

Individuals who are assigned responsibilities for information technology security safeguards need in-depth training regarding the security methodologies and techniques required to configure, implement, administer, and maintain those safeguards. For example, a security administrator may need to know the method and techniques for granting various types of access rights to the database, how to set up and maintain an effective firewall to filter external access, and how to detect intrusions to the system. Typical sources for technical training include instructor-led programs (3<sup>rd</sup> party or internal), commercial off-the-shelf training modules, technical publications, and operations manuals provided by the vendor.

### C.1 Standards

C.1.a) Each Agency must establish and maintain information technology security training programs to ensure that all individuals involved in managing, administering, designing, developing, implementing, and/or maintaining information resources are aware of their security responsibilities and know how to fulfill them.

C.1.b) Information technology security training programs must be commensurate to the level of expertise required for the system components and information resources for which they are responsible. The program must include content that enables the individual to identify and evaluate threats, vulnerabilities, and risks specific to those components and resources. The program must further include content regarding technical alternatives, methods, and standards which represent best practices appropriate to those components and resources, and which can be utilized to effectively implement safeguards as appropriate.

## D. Technical Communications

Technical communications refer to those practices, technologies and/or services used to communicate technical information and notifications regarding the status of security related events and safeguards.

In addition to the communications inherent in Security Awareness and Technical Training, the security architecture requires a means to support the timely and meaningful exchange of information regarding: 1) new security technology products and/or features, best practices, emerging industry standards, and security safeguards success stories; 2) proposed changes to the security infrastructure and associated implementation plans; and 3) alerts, status, and recommended actions in response to security attacks. Examples of technical communication medium include internal enterprise list servers, government sponsored security conferences, subscriptions to security research consortiums, etc.

Technical communications are instrumental in the security architecture as they foster both a proactive stance and a systemic view in addressing security issues within a dynamic business and technology environment.

### **D.1 Standards**

D.1.a) If any data or documentation contains sensitive information, then the Agency must ensure that such information is given accountable and authorized dissemination only.

## **E. Authentication, Authorization and Encryption**

Authentication refers to the process of verifying the identity of a user. Authorization refers to the process of establishing and enforcing a user's rights and privileges to access specified resources. Encryption refers to the process of converting computer data and messages to something incomprehensible by means of a key, so that it can be reconverted only by an authorized recipient holding the matching key.

Authentication answers the question, "Are you who you say you are?" It is a means of establishing the validity of a claimed identity to the system, which becomes the basis for individual accountability. There are three means of authenticating a user's identity, which can be used alone or in combination: 1) validating something the individual knows (e.g., a password, a Personal Identification Number (PIN), or a cryptographic key); 2) validating something the individual possesses, referred to as a "token" (e.g., an ATM card or a smart card); or 3) validating something the individual "is", referred to as a "biometric" (e.g., fingerprints or voice patterns).

Once authenticated, logical access controls are utilized to authorize and enforce a user's access to and actions towards specified resources. This authorization may be based on identity, roles (e.g., data entry clerk, administrator, supervisor) location, time, types of transactions, service constraints (e.g., number of concurrent users), access mode (e.g., read, write, delete), or a combination of these criteria. Both internal authorization safeguards (such as Access Control Lists) and external controls (such as secure gateways/firewalls) can be deployed. Another mechanism that can be used for strong access control is encryption, whereby encrypted information can only be decrypted by those possessing the appropriate cryptographic key.

### **E.1 Standards**

E.1.a) Each Agency must ensure that Users are authenticated prior to accessing the systems which are "owned" by that Agency.

E.1.b) Each Agency must establish a formal authentication control policy that establishes the criteria for administering authentication safeguards.(e.g., a formal password policy that includes the criteria for password aging, history, length and composition).

E.1.c) Each Agency must store all sensitive data used in authenticating the user, including passwords, in protected files.

E.1.d) Public key certificates must be based on the most current IETF X509 standards.

E.1.e) Each Agency must authorize and enforce a user's access to and actions towards specified resources based on least privilege. Least privilege states that a user is given only that set of privileges necessary to perform his/her job.

E.1.f) The use of cryptology technologies for data storage and data communications (transmission of data) must be based on open standards.

E.1.g) All Virginia On-Line Transaction (VOLT) Certificates utilized by an Agency must be issued by service providers who are currently granted "Authorized Certificate Authority" status via a Virginia VOLT contract.

E.1.h) Each Agency that stores encrypted data must establish an Encryption Key Management policy and procedure to address the integrity and recovery of the "keys".

## **F. Data Security**

Data Security refers to those practices, technologies and/or services used to ensure that security safeguards are applied appropriately to data which is provided, processed, exchanged and/or stored by the State.

The term "data" includes, but is not limited to, data in a database, information about an Operating System (OS), operational policies and procedures, system design, organization policies and procedures, system status, and personnel schedules. Data Security safeguards strive to sustain the level of integrity, availability and confidentiality of this data as stated by the Agency's policy. Data security is the responsibility of the data owner. The appropriate types/pieces of data (procedures, databases, operating documents, etc), and their level of sensitivity, need to be identified as part of the business impact analysis and risk assessment (see Subsection A).

Examples of data security safeguards include Agency developed procedures (e.g., information distribution and change management procedures), vendor delivered configurable controls (e.g., automatic screen savers), and add-on technologies (e.g., hashing algorithms). Data security safeguards are clearly interdependent with other safeguards described in this architecture (e.g., physical security, authentication, authorization, and encryption).

### **F.1 Standards**

F.1.a) Ownership of data must be specifically identified by each Agency. [Note, based on the Agency's business impact analysis and risk assessment referred to in Subsection A, files and data elements to be protected will be identified.]

F.1.b) Owners are responsible for determining the appropriate levels of data security required.

F.1.c) All sensitive data must be removed from system hardware, software or media by the owner prior to its “reuse” by another Agency, or for “reuse” by another system within the Agency. Similarly, all sensitive data must be removed from system hardware, software or media by the owner prior to its disposal.

## **G. Systems Interoperability Security**

Systems interoperability refers to those practices, technologies and/or services used to ensure that security safeguards are applied consistently and appropriately to mechanisms that allow diverse systems and networks to interoperate.

Agencies often depend on interoperability for the timely exchange and sharing of information and data to effectively perform their business services. An Agency’s systems may interoperate with those of other Agencies, other governmental bodies (local, state, or federal), with businesses or with public users; and those systems may operate on different platforms or with different technologies. Synergies, cost savings, and economies of scale can result by ensuring that security safeguards between “interoperating entities” are compatible and sustain the desired security protection levels of those entities. Industry best practices suggest that deploying vendor-neutral, open standards provides a common denominator in support of interoperability.

### **G.1 Standards**

G.1.a) Each Agency must ensure that authentication, authorization and data security, as established by the data owner, are not compromised during data sharing and systems interoperability.

G.1.b) Auditable user agreements must be established between the Agencies sharing data, which clearly state the degree of authentication and levels of protection required.

G.1.c) Web-enabled transactions that require user authentication, or transfer of sensitive data, or that involve the transfer of funds, must use encryption (e.g. SSLv3).

## **H. Physical Security**

Physical Security refers to those practices, technologies and/or services used to ensure that physical security safeguards are applied. Physical security safeguards take into account 1) the physical facility housing the information resources; 2) the general operating location; and 3) the support facilities that underpin the operation of the information systems.

Accordingly, physical security safeguards need to be considered for information resources residing in static facilities (such as buildings), mobile facilities (such as computers mounted in vehicles), and portable facilities (in-transit facility housing). Appropriate physical safeguards need to be established based on the risks related to geographic location, including natural threats (such as flooding), man-made threats (such as burglary or civil disorders), and threats from nearby activities (such as toxic chemical processing or electromagnetic interference). Lastly, physical safeguards need to assure that the appropriate levels of support facilities such as electric power, heating, and air-conditioning are sustainable as required by the information resources.

For example, physical access controls may be used to restrict and monitor the entry and exit of personnel to/from a room, a data center, or a building. Physical access controls may range from badges and locks to retina scanning personal identification devices and vibration detectors. Physical access controls need to be considered for those areas containing system hardware, as well as for those areas which house network wiring, electric power, backup media, source documents, etc.

Physical security safeguards provide a first line of defense for information resources against physical damage, physical theft, unauthorized disclosure of information, loss of control over system integrity, and interruption to computer services.

### **H.1 Standards**

H.1.a) Mission critical system facilities must be located in a secure location that is locked and restricted to authorized personnel only.

H.1.b) Access to “critical” computer hardware, wiring, displays and networks must be controlled by rules of least privilege.

H.1.c) System configurations (i.e., hardware, wiring, displays, networks) of “critical” systems must be documented. Installations and changes to those physical configurations must be governed by a formal change management process.

H.1.d) A system of monitoring and auditing physical access to “critical” computer hardware, wiring, displays and networks must be implemented (e.g. badges, cameras, access logs).

H.1.e) Back-ups of mission critical data must be stored off-site in a secured location.

## **I. Personnel Security**

Personnel Security refers to those practices, technologies and/or services used to ensure that personnel security safeguards are applied appropriately to those personnel working for, or on behalf, of the State.

Personnel Security begins during the staffing process. Early in the process of defining a position, the responsible supervisor determines the type of computer access that is needed for the position and the sensitivity of that position. Best practices suggest that two general principles should be followed in defining a position: *separation of duties* and *least privilege*. Separation of duties refers to dividing roles and responsibilities so that a single individual cannot subvert a critical process. For example, separate responsibility should be given for requesting a personal identification number and for authorizing a personal identification number. Least privilege refers to granting a user only those accesses that they need to perform their official duties. For example, a data entry clerk may not need to run analysis reports against the entire Agency database. As part of the process to fill a position, best practices also suggest that testing and

background screening should be used as appropriate to help validate and/or access a candidate's qualifications, past performance and appropriateness for a particular position.

Once personnel have been staffed, personnel security safeguards are administered according to the Agency's security policy via User account management. User account management involves 1) establishing the procedures for requesting, issuing, and closing user accounts over the life cycle events of personnel (e.g., initial hire, transfers, position promotion, retirement, resignation, etc.); 2) tracking users and their respective access authorizations; and 3) managing these functions on an on-going basis.

### **I.1 Standards**

I.1.a) Access must be explicitly granted to personnel by the Owner (i.e., not allowed by default).

I.1.b) Access granted to personnel must be based on least privilege (i.e., only up to the level needed to perform one's duties).

I.1.c) Access must be terminated concurrent with when the requirement for access no longer exists (e.g., as result of transfer, termination , and change of duties).

### **J. Threat Detection**

Threat detection refers to those practices, technologies and/or services used 1) to detect that a suspicious activity may be occurring on systems/networks; and 2) to alert security administrators and security staff accordingly.

An attack on a system or network can come from either inside or outside of an Agency, and could be intentional (e.g., transmittal of viruses, "worms", or "Trojan horses") or unintentional (e.g., accidental deletion of a control file).

Threat detection may include the real-time monitoring of activities such as logons, connectivity, operating system calls, command parameters, or system performance logs. Threat detection safeguards support the analysis of performance thresholds, behavioral anomalies, use patterns and trends (such as degradation in system performance over time), or the existence of known threats (such as known viruses). For example, automated tools could monitor the levels and rate of change in disk space on an E-mail server to determine if potential "spamming" (i.e., sending continuous bulk e-mail) is occurring with the potential to consume all available space on that server.

Threat detection may also include a review of activities "after the fact", and over a specific time frame (e.g., reviewing the number and types of rejected passwords overtime may indicate that a "password cracking" activity is under attempt.)

Alerts from automated threat detection tools may be active (immediate paging of appropriate security personnel) or passive (logging specific types of activities to a daily system security log for later review).

## **J.1 Standards**

J.1.a) Each Agency must establish and implement a process to identify and evaluate threats and assign appropriate action based on risks.

J.1.b) Firewall technology must have security logging turned on.

## **K. Security Tool Kit**

This subsection refers to those practices, technologies and/or services used to manage, analyze, filter, test and/or control security safeguards. For example, firewall technology provides a mechanism through which authentication, authorization, filtering and directing of remote users to an internal system can be accommodated. Typically an Agency's security tool kit will be comprised of a combination of commercial off-the shelf products, industry proven free shareware, and Agency developed software tools. The tools may be positioned on the perimeter of systems or integrated into the systems; and may be deployed on either an operational or as needed basis. Examples of common technologies within an organization's security tool kit include firewall technology, vulnerability scanners, and sniffers.

### **K.1 Standards**

K.1.a) Agencies with external connections using TCP/IP must utilize firewall technology.

K.1.b) Each Agency must test its firewall technology on a periodic basis to ensure compliance with security policies.

K.1.c) Each Agency must deploy multi-layered protection at the Internet gateway, the network server and the desktop levels to prevent the introduction of malicious code into the system.

## **L. Incident Handling**

Incident Handling refers to those practices, technologies and/or services used to respond to suspected or known breaches to security safeguards.

Once a suspected intrusion activity has been qualified as a security breach (i.e., incident), it is imperative that the incident be contained as soon as possible, and then eradicated so that any damage and risk exposure to the Agency and the Commonwealth are avoided or minimized. Information technology security incidents refer to deliberate, malicious acts which may be technical (e.g., creation of viruses, system hacking) or non-technical (e.g., theft, property abuse, service disruption). In several cases, if the incident is left "unchecked" (i.e., not contained), then the damage resulting from these incidents continues to spread within, and across, Agencies.

Handling incidents can be logistically complex, and may require information and assistance from sources outside the Agency (e.g., technical specialists, law enforcement entities such as state

police or FBI, and the public affairs office). Industry best practices suggest that organizations who adopt both proactive and reactive means to address incident handling are better able to limit the negative implications of incidents. Examples of proactive activities include establishing communication mechanisms to report incidents and to disseminate incident alerts; and identifying technical experts who can provide emergency assistance if needed. Examples of reactive activity include blocking or aborting computer processes; temporarily denying user access; and deploying inoculation software.

### **L.1 Standards**

L.1.a) Each Agency must develop an Incident Response Plan (IRP), which identifies the responsibilities and actions to be taken in response to incidents.

L.1.b) Each Agency must ensure that out-of-band communication alternatives are established as part of their Incident Response Plan (i.e., that the “compromised” device, platform, or media is not used to notify users or to report the incident).

### **M. Monitoring and Controlling System Activities**

Monitoring and Controlling System Activities refers to those practices, technologies and/or services used to ensure that the implementation and maintenance of security safeguards and system changes are adequately documented and managed, such that accountability can be established.

Monitoring and Controlling System Activities is part of an Agency’s comprehensive auditing program that facilitates the following security controls. It provides a means to assess policy compliance (e.g., security check list), verify operational assurance (e.g., penetration testing), maintain individual accountability (e.g., user audit trails, change management approvals), and to support intrusion problem analysis (e.g., user behavior anomalies; repeated failed log-in attempts; reconstruction of events).

Monitoring and Controlling System Activities can be self-administered (by the Agency) or independently administered (by parties external to the Agency). Personnel involved in these activities must have a high-level of expertise in the information technology security field and of auditing practices; and must administer said activities objectively.

Industry practices suggest that security safeguards tend to degrade over the operational lifecycle of systems as users and operators discover new ways to intentionally or unintentionally bypass or subvert security. Agencies must therefore make a risk-based decision regarding the timing (e.g., annual independent audit; daily audit log analysis) and scope (e.g., system, application or user level) of Monitoring and Controlling System Activities.

### **M.1 Standards**

M.1.a) Each Agency must monitor and track systems, activities and operations, with resulting data made accessible, to ensure compliance and accountability with security policies.

M.1.b) Each Agency must include a configuration management process in their security program that establishes accountability for changes to information system components.

## Business Continuity Planning

The purpose of business continuity planning is to provide for the continuation of critical business functions in the event of disruptions. The preparation for handling disaster contingencies is generally called business continuity planning or contingency management. A secondary purpose of business continuity planning is to minimize the effect of disruptions. Many potential contingencies and disasters can be averted, or the damage they cause reduced, if appropriate steps are taken early to control the event.

Accordingly, Agency management shall ensure the necessary allocation of resources for the development and maintenance of a business continuity plan for critical information technology systems for the support of critical business functions. As part of this planning, the Agency shall establish plans to ensure that sensitive information is not compromised as a result of said disruptions.

Agencies shall develop, document, maintain and periodically test a business continuity plan that will provide a reasonable assurance that critical data processing support can be continued, or resumed within an acceptable time frame, if normal operations of the system are interrupted. These plans will include adequate coverage of:

- Emergency response procedures appropriate to any incident or activity that may endanger lives, property, or the capability to perform essential functions.
- Arrangements, procedures, and responsibilities, including data backup, offsite storage and contingency safeguards, that ensure critical operations can be continued and that sensitive information can be protected if normal processing or data communications are interrupted for any reason for an unacceptable period of time.
- Recovery procedures and responsibilities to facilitate the rapid restoration of normal operations at the primary site, or if necessary, at a new facility, following the destruction, major damage or other interruptions at the primary site.
- Minimally acceptable prioritized level of degraded operation of critical systems or functions to guide implementation at the backup operational site. The business continuity plan must accommodate the established priorities.
- Interim manual processes to enable the continuance of critical operations in the absence of data processing support.

The business continuity plan for large systems supporting critical agency or institutional functions shall be fully documented. Small systems, such as those located in the office environments, may develop a more abbreviated and less formal plan. All plans must be operationally tested at a frequency commensurate with the risk and magnitude of loss or harm that could result from the disruption of information processing support.

## Glossary

**Agency** – The term “Agency” means executive branch Agencies and institutions of higher education.

**Authentication** – The term “authentication” refers to the process of verifying the identity of a user.

**Authorization** – The term “authorization” refers to the process of establishing and enforcing a user’s rights and privileges to access specified resources.

**Best Practice** - The term “best practice” means a guideline or specification that is advisory in nature and whose compliance is strongly recommended; however, it is not binding on Agencies.

**CISA** – Certified Information Systems Auditor

**CISSP** – Certified Information Systems Security Professionals

**Commonwealth of Virginia Network (COVANET)** – COVANET is the Commonwealth’s statewide telecommunications network administered by the Department of Information Technology which includes wide-area network, long distance services, and other related services.

**COVITS** – Commonwealth of Virginia Information Technology Symposium

**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.

**Data** – The term “data” includes but is not limited to data in a database, information about an OS, operational policies and procedures, system design, organization policies and procedures, system status, and personnel schedules.

**Encryption** – The term encryption refers to the process of converting computer data and messages to something incomprehensible by means of a key, so that it can be reconverted only by an authorized recipient holding the matching key.

**Firewall Technology** – The term “firewall technology” refers any combination of network hardware, network software, and host-based software used within an organization to prevent unauthorized access to system software or data in accordance with its security policy (e.g. includes routers with access list proxy gateways, host-based firewall software, and specialized password devices).

**FTP** – File Transfer Protocol

**HIPAA** – Health Insurance Portability and Accountability Act

**HVAC** – Heating, Ventilation and Air Conditioning

**IETF** – Internet Engineering Task Force

**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.

**IPSec** – Internet Protocol Security

**IRP** – Incident Response Plan

**ISSO** – Information Systems Security Officer (agency-level)

**NIST** – National Institute of Standards and Technology

**Open Standard** – infers that the standard is not proprietary to a specific manufacturer, vendor, product or owner, but may be used among various components and products such that it facilitates interoperability; and it has been approved by an appropriate national or international standards body.

**OS** – Operating System

**Out-of-band Communication** – The term refers to a communication device, platform or media other than that communication media or platform on which a suspected or actual security threat is occurring. Thus, it becomes the alternative communication device, platform or media used to report an incident.

**Owner** - The term “owner” refers to that group (i.e., Agency or Agency unit) which controls a set of information resources and determines its level of criticality and sensitivity.

**PGP** – Pretty Good Privacy (a security product name)

**PKI** – Public Key Infrastructure

**Public network** – refers to that network infrastructure not controlled by the Agency (e.g., Internet, COVANET).

**Policy** – The term policy means any general statement of direction and purpose designed to promote the coordinated planning, practical acquisition, effective development, and efficient use of information technology resources.

**SANS** – Systems Administration, Networking and Security (a cooperative research organization)

**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.

**SHTTP** – Secure Hypertext Transfer Protocol.

**SSH** – Secure Shell Protocol

**SSL** – Secure Socket Layer

**Standard** - The term “standard” means a directive or specification whose compliance is mandatory, and whose implementation is deemed achievable, measurable, and auditable for compliance.

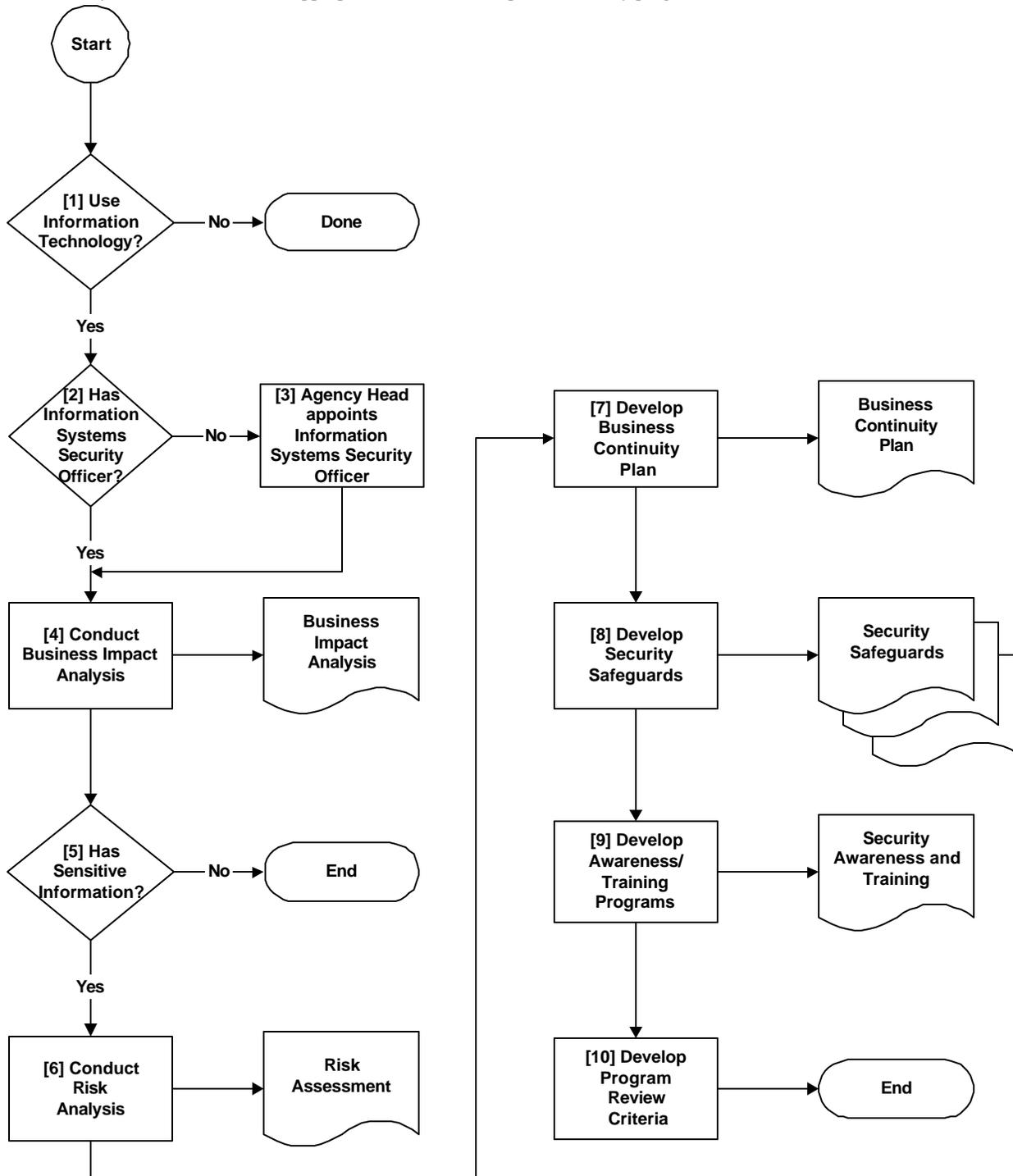
**TCP/IP** – Transmission Control Protocol/Internet Protocol

**User** – An individual or group who has access to an information system or its data.

**VPN** – Virtual Private Network

## Appendix A: High Level Flowchart “Information Technology Security Program Development Cycle”

(Note, this cycle can be reiterated as appropriate to review and update a security program.)



**Flowchart Process Description:**

The following process description provides a brief explanation of the steps outlined in the flowchart above.

Step 1: The Agency Head shall review the asset portfolio of that Agency to determine if the Agency currently owns and deploys information technology in fulfilling the Agency's mission. As defined in the glossary, 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. If the Agency does not own and deploy information technology, then there is no need to develop an information technology security program at this time. If the Agency does own and deploy information technology, then proceed to Step 2.

Step 2: The Agency Head shall review the personnel portfolio of the Agency to determine if the Agency has a designated Information Systems Security Officer (ISSO). The role of the ISSO is take responsibility for the development, implementation, maintenance and oversight of the Agency's information technology security program. If the Agency does not have an ISSO, then go to Step 3. If the Agency Head has already appointed an ISSO, then proceed directly to Step 4.

Step 3: The Agency head formally appoints an Information Systems Security Officer (ISSO) for that Agency.

Step 4: The ISSO will direct the Agency through a Business Impact Analysis. (See Subsection A of this document.) The objective of the Business Impact Analysis is to identify the information resources owned and/or utilized by the Agency, and then to determine which of those resources require protection against unavailability, unauthorized access or disclosure. The result of this process is a documented Agency Business Impact Analysis.

Step 5: The ISSO will review the Business Impact Analysis to determine if the Agency has any "sensitive information". As defined in the glossary, 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. If the Agency does not own and/or utilize any sensitive information, then there is no need to develop an information technology security program at this time. If the Agency does own and/or utilize sensitive information, then proceed to Step 6.

Step 6: The ISSO will direct the Agency through a Risk Assessment. (See Subsection A of this document.) The objective of the Risk Assessment is to identify the threats to sensitive information resources, the probability of each threat event occurring, and their resultant impact. The result of this process is a documented Agency Risk Assessment.

Step 7: The ISSO will coordinate the development of a Business Continuity Plan. The objective of the Business Continuity Plan is to provide for the continuation of critical business functions in the event of disruptions. The result of this process is a documented Agency Business Continuity Plan.

Step 8: The ISSO will direct the Agency in developing and/or deploying, and maintaining, adequate and appropriate security safeguards to protect sensitive information resources for both normal operating environments and planned contingency operating environments. (Subsections D through M of this document.) The result of this process is a set of deployed and documented security safeguards.

Step 9: The ISSO will direct the Agency in developing and/or deploying, and maintaining, adequate and appropriate security awareness and security training programs. (Subsections B and C of this document). The result of this process is documented Security Awareness and Security Training programs.

Step 10: The ISSO shall identify the type(s) of events, both internal and external, that will trigger the reiteration of this security program development cycle by the Agency, so that the Agency's security program is updated as appropriate.

## Appendix B: Assignment of Uniform Alphanumeric Publication Designations for all Policies, Standards, and Guidelines

The Department of Technology Planning is responsible for assigning a uniform alphanumeric Publication Designation (PD) to all Commonwealth of Virginia (COV) Information Technology Resource Management (ITRM) Policies, Standards, and Guidelines (PSG). The PD is derived, in part, from components of the Commonwealth Enterprise Architecture (EA) known as “Infrastructure Domains.” The “Infrastructure Domains” and Governance are defined in the [Commonwealth EA Glossary](#). The Governance code is used to identify those PSG that are not uniquely related to a specific infrastructure domain, e.g. “IT Project Management” or “IT Project Oversight.”

The following alpha codes will be used to identify each PSG:

Infrastructure Domains + Governance	Code
Governance and Transitional Processes	GOV
Platform Architecture	PLA
Database Architecture	DAT
Network Architecture	NET
Security Architecture	SEC
Cost Allocation Architecture	COS
Systems Management Architecture	SYS
Information Architecture	INF
Application Architecture	APP
Middleware Architecture	MID

Publication Designations are constructed as follows:

COV ITRM (“Policy,” “Standard,” or “Guideline”) XXXYYYY-ZZZ

Where:           XXX is the assigned Infrastructure Domain + Governance code;  
                   YYYY is the year of initial issue; and  
                   ZZZ is the sequential number assigned to link related PSG.

Example:        COV ITRM Standard GOV2000-01.1 is a standard that implements  
                   COV ITRM Policy GOV2000-01.1.