Commonwealth of Virginia

Information Technology Resource Management

INFORMATION TECHNOLOGY SYSTEMS SECURITY GUIDELINE

Virginia Information Technologies Agency (VITA)

ITRM Publication Version Control

<u>ITRM Publication Version Control:</u> It is the user's responsibility to ensure that he or she has the latest version of the ITRM publication. Questions should be directed to the Director for Policy, Practice and Architecture (PPA) at VITA's IT Investment and Enterprise Solutions (ITIES) Directorate. ITIES will issue a Change Notice Alert when the publication is revised. The Alert will be posted on the VITA Web site. An email announcement of the Alert will be sent to the Agency Information Technology Resources (AITRs) at all state agencies and institutions, as well as other parties PPA considers interested in the publication's revision.

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

Version	Date	Purpose of Revision
Original	07/17/2008	Original

Preface

Publication Designation
ITRM IT Systems Security Guideline

Subject
Information Technology Systems Security

Effective Date
07/17/2008

Scheduled Review
One (1) year from effective date

Authority
Code of Virginia § 2.2-603(F)
(Authority of Agency Directors)

Code of Virginia, §§ 2.2-2005 – 2.2-2032.
(Creation of the Virginia Information Technologies Agency;
"VITA;" Appointment of Chief Information Officer (CIO)

Scope
This *Guideline* is offered as guidance to all executive, legislative, and judicial branch, and independent State agencies and institutions of higher education (collectively referred to as "Agency") that manage, develop, purchase, and use information technology (IT) resources in the Commonwealth.

Purpose
To guide Agencies in the implementation of the information technology systems security requirements defined by ITRM Standard SEC501-01, Section 4.

General Responsibilities
(Italics indicate quote from the Code of Virginia)
Chief Information Officer
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*

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 of Virginia's IT systems and data.

IT Investment and Enterprise Solutions Directorate

In accordance with the *Code of Virginia* § 2.2-2010, the CIO has assigned the IT Investment and Enterprise Solutions Directorate the following duties: *Develop and*

adopt policies, standards, and guidelines for managing information technology by state agencies and institutions."

All Executive, Legislative, and Judicial Branch and Independent State Agencies
In accordance with §2.2-2009 of the *Code of Virginia,*, all executive, legislative, and judicial branch and independent State agencies and institutions of higher education are responsible for complying with all Commonwealth ITRM policies and standards, and considering Commonwealth ITRM guidelines that address security of state government electronic information from unauthorized uses, intrusions or other security threats issued by the Chief Information Officer of the Commonwealth.

Definitions
Agency - All executive, legislative, and judicial branch and independent State agencies and institutions of higher education that manage, develop, purchase, and use IT resources in the Commonwealth of Virginia (COV).
CISO - Chief Information Security Officer – The CISO is the senior management official designated by the CIO of the Commonwealth to develop Information Security policies, procedures, and standards to protect the confidentiality, integrity, and availability of COV IT systems and data.
Data An arrangement of numbers, characters, and/or images that represent concepts symbolically.
Data Owner - An agency Manager, designated by the Agency Head or Information Security Officer, who is responsible for the policy and practice decisions regarding data. For business data, the individual may be called a business owner of the data.
Electronic Information - Any information stored in a format that enables it to be read, processed, manipulated, or transmitted by and IT system.
Government Electronic Information - Electronic information owned or held by COV.
ISO – Information Security Officer - The individual designated by the Agency Head to be responsible for the development, implementation, oversight, and maintenance of the agency's IT security program.
IT System - An interconnected set of IT resources and data under the same direct management control.
Information Technology (IT) - Telecommunications, automated data processing, databases, the Internet, management information systems, and related information, equipment, goods, and services.
Information Technology (IT) Security - The protection afforded to IT systems and data in order to preserve their availability, integrity, and confidentiality.
Information Technology (IT) Security Audit - An independent review and examination of an IT system's

policy, records, and activities. The purpose of the IT security audit is to assess the adequacy of IT system controls and compliance with established IT security policy and procedures.

Least Privilege - The minimum level of data, functions, and capabilities necessary to perform a user's duties.

Risk - The possibility of loss or injury based on the likelihood that an event will occur and the amount of harm that could result.

Risk Assessment (RA) - The process of identifying and evaluating risks so as to assess their potential impact.

Risk Mitigation - The continuous process of minimizing risk by applying security measures commensurate with sensitivity and risk.

Sensitivity - A measurement of adverse affect on COV interests, the conduct of agency programs, or the privacy to which individuals are entitled that compromise of IT systems and data with respect to confidentiality, integrity, and/or availability could cause IT systems and data are sensitive in direct proportion to the materiality of the adverse effect caused by their compromise.

Sensitivity Classification - The process of determining whether and to what degree IT systems and data are sensitive.

Separation of Duties - Assignment of responsibilities such that no one individual or function has control of an entire process. It is a technique for maintaining and monitoring accountability and responsibility for IT systems and data.

Threat - Any circumstance or event (human, physical, or environmental) with the potential to cause harm to an IT system in the form of destruction, disclosure, adverse modification of data and/or denial of service by exploiting vulnerability.

Vulnerability*:* A condition or weakness in security procedures, technical controls, or operational processes that exposes the system to loss or harm.

Related ITRM Policy and Standards

ITRM Policy, SEC500-02: Information Technology Security Policy (Revised 07/01/2007)

ITRM Standard SEC501-01: Information Technology Security Standard (Revised 07/01/2007)

ITRM Standard SEC502-00: Information Technology Security Audit Standard (Revised 09/01/2007)

TABLE OF CONTENTS

List of Figures

List of Tables

1   Information Technology Systems Security

This Guideline presents a methodology for Information Technology (IT) systems security suitable for supporting the IT Security Framework of the Commonwealth of Virginia (COV) Information Technology Security Policy (ITRM Policy SEC500-02) and the Information Technology Security Standard (ITRM Standard SEC501-01.) These documents are hereinafter referred to as the "Policy," and "Standard," respectively.

The function of the Policy is to define the overall COV IT security program, while the Standard defines high-level COV IT security requirements. This Guideline describes methodologies for agencies to use when implementing the systems security program outlined in the policy and detailed in the Standard. Agencies are not required to use these methodologies and may use methodologies from other sources or develop their own methodologies, if these methodologies reflect the intent of the policy and implement the requirements of the Standard.

1.1   Roles and Responsibilities

There is a variety of IT Security roles in an effective IT Security program. Roles range from the Information Security Officer (ISO) with overall responsibility for the agency's IT Security program, to system-specific roles such as System Owner, Data Owner, System Administrator, and others as appropriate.

The Standard requires Agency Heads to designate an ISO, and strongly encourages the Agency Head to designate at least a backup ISO. To the extent practical, Agency Heads and ISOs are encouraged to assign a different person to each IT Security role. All security roles must be documented in the position description of the individual assigned to the role.

In smaller agencies, assigning a different person to each IT Security role may not be practical. In such cases, agencies should consider sharing resources between multiple agencies. Assigning an ISO to provide security expertise for multiple agencies should occur where practical. In the case of sharing an ISO between agencies, the agency still retains the responsibility of security over their data and infrastructure.

Agencies are encouraged to go beyond the requirements of the Standard in assigning IT Security roles, where appropriate. For example, in cases where responsibilities for applications and infrastructure are divided, agencies are encouraged to designate two System Administrators, one with responsibility for applications security and one with responsibility for infrastructure security of the IT system. Refer to Table1 below for delineation of each IT security role.

Table 1 IT security Roles and Responsibilities

Role	Designated By	Role Requirements	Recommended Qualifications	Responsibilities
Agency Head	Governor or Board, as defined by statute	Defined by Governor or Board, as defined by statute	Defined by Governor or Board, as defined by statute	Oversee Agency IT security program. • Designate ISO • Designate or delegate other Agency IT security roles • Review BIA, RA, COOP • Review IT Security Audit Plan & results of IT security audits • Monitor Corrective Action Plans (CAPs) • Report incidents that threaten the security of databases & data communications
ISO	Agency Head	• Must be a COV employee • Must not be a system or data owner • Should not exercise (or report to an individual who exercises) operational IT or IT security application or infrastructure responsibilities	• In-depth knowledge of systems owned & of Agency's overall business • In-depth knowledge of Agency's IT and operating environment & requirements • Security Certifications[1]	Overall security of Agency IT systems & liaison to the CISO of the Commonwealth • Develop/maintain IT security program as defined by Policy, Standard, and Audit Standard. • Assign (unless Agency Head assigns) other Agency IT security roles

Privacy Officer	Agency Head /ISO	At Agency Head's/ ISO's discretion	• In-depth knowledge of system owned & of Agency's overall business
			• In-depth knowledge of Agency's IT and operating environment & requirements
			• Security Certifications
				• Only mandatory if required by law or regulation
				• Responsibilities otherwise exercised by ISO
				• Provide guidance on privacy laws:
				  • Disclosure of & access to sensitive data
				  • Security & protection requirements in conjunction with IT systems when there is overlap among sensitivity, disclosure, privacy, & security issues

System Owner	Agency Head / ISO	• Required for all sensitive IT systems • Must be a COV employee • Must not be ISO or system administrator for system owned	In-depth knowledge of system owned & of Agency's overall business	• Responsible for the overall security of the IT system • Accountable to the Agency Head • Manage IT system risk • Designate system administrator

---

[1] IT Security certifications include Certified Information Systems Security Professional (CISSP), Certified Information Security Manager (CISM), and Certified Information Security Auditor (CISA), among others.

Role	Designated By	Role Requirements	Recommended Qualifications	Responsibilities
Data Owner	Agency Head / ISO	• Required for all sensitive IT systems • Must be a COV employee • Must not be system administrator for system processing data owned • Must not be ISO	In-depth knowledge of system owned & of Agency's overall business	• Promotes IT security awareness to data users • Develops additional requirements, guidelines & procedures needed to protect the data owned • Classify data sensitivity • Define data protection requirements for data owned & communicate requirements to System Owner • Define data access requirements • Designate Data Custodian
System Administrator	System Owner	• Required for all sensitive IT systems • Must not be ISO	Required technical skills	• Day-to-day administration of the IT system • Implement requirements of the IT security program Note: *Where responsibilities for applications & infrastructure are divided, two System Administrators may be designated, one with responsibility for applications security & one with responsibility for infrastructure security.*
Data Custodian (3rd party in logical or physical possession of data)	Data Owner	• May be an individual or an organization (COV or partner) • Must not be ISO	Required technical skills	• Protect data from unauthorized access, alteration, destruction, or usage • Operate IT systems in a manner consistent with COV IT security policies and standards
IT System Users	NA	NA	NA	• Read and comply with Agency IT security requirements • Immediately report potential and actual breaches of IT security • Protect security of IT systems and data

1.2   IT Systems Security

IT Systems Security comprises technical, operational, and administrative activities which help to make IT security an integral part of COV IT systems. The activities occur in five areas:

- IT Systems Security Planning;
- IT System Hardening;
- IT Systems Interoperability Security;
- Malicious Code Protection; and
- IT Systems Development Life Cycle.

2   IT Systems Security Plans

The objective of system security plan is to ensure appropriate protections for information system resources are identified and implemented. Completion of a system security plan for each sensitive system is a requirement of the Standard section 4.2. The following guidance provides information on how to prepare a system security plan and is designed to be adaptable in a variety of organizational structures and used as reference by those having assigned responsibility for activity related to security planning.

The system security plan should be viewed as documentation of the structured process of planning adequate, cost-effective security protection for a system. It should reflect input from various managers with responsibilities concerning the system, including the data owner, the system owner, and the Information Security Officer (ISO). Additional information may be included in the plan with the structure and format organized according to agency needs.

2.1   Overview

The Standard requires each agency to develop, document, and implement an agency-wide information security program to provide protection for the data and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or service provider. System security planning is an important activity that supports the system development life cycle (SDLC) by providing existing and planned security controls. Documentation should be updated as system events dictate the need for revision in order to accurately reflect the current state of the system.

The system security plan provides a summary of the security requirements for the information system. The plan also describes the controls in place or planned for meeting those security requirements in the information system. The planning effort uses other key security-related documents for the system as shown in Figure 1 below. These include the Business Impact Analysis, IT DR section of the Continuity of Operations Plan, Risk Assessment Report, and IT Security Audit Corrective Action Plan, among others.
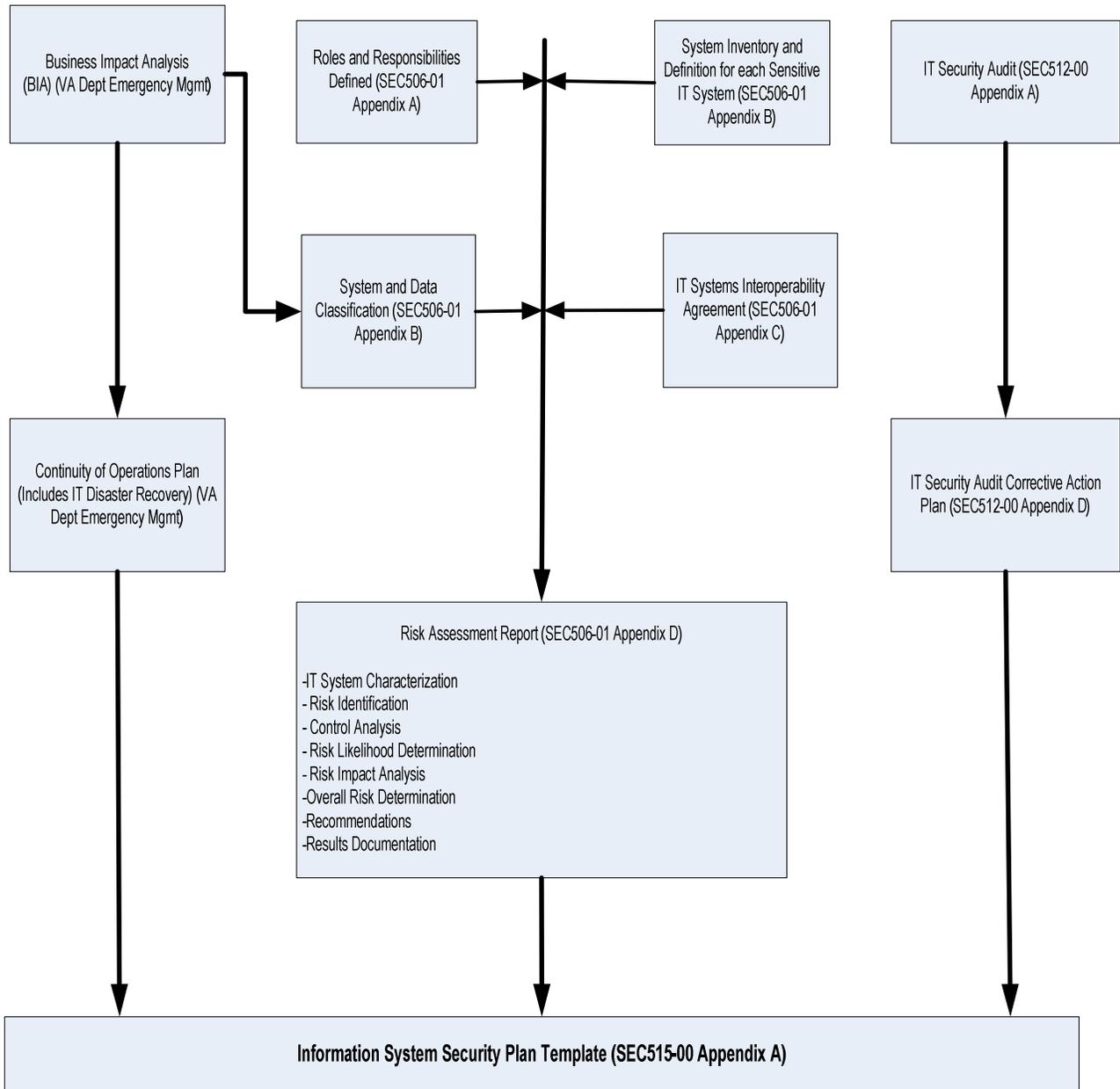
Figure 1 Security Planning Process Inputs

2.2   System Name and Identifier

The first item listed in the system security plan is the system name and identifier2. Assignment of a unique identifier supports the agency's ability to easily collect agency information and security metrics specific to the system as well as facilitate complete traceability to all

---

[2] We suggest the following format for unique identifier: Agency code followed by two letter identifier for component type followed by a four digit sequential number as in this example for VITA (136AP0001). The 136 is VITA's agency code, AP in this case is for Application Program, and number assigned. Letter codes are AP (Application Program); DA (Data Asset [database, files etc]; ST (software tools).

requirements related to system implementation and performance. This identifier should remain the same throughout the life of the system and be retained in audit logs related to system use.

2.3   *System Owner and Designated Contacts*

A designated system owner must be identified in the system security plan for each system as stated in section 2.2 of the Standard. This person is the key point of contact (POC) for the system and is responsible for coordinating system development life cycle (SDLC) activities specific to the system as well as for providing ongoing operational business decisions related to use of and changes to the system. This section should also include names of other key contact personnel who can address inquiries regarding system characteristics and operation including but not limited to business owner, data owner, system administrator, ISO, etc. The plan should include the following contact information:

- Name
- Title
- Agency
- Address
- Phone Number
- Email Address

2.4   *System Security Plan Approval*

Organizational policy and procedures should be developed for plan submission, or other documentation required by the agency.

The agency head or designated ISO is responsible for system security plan approval and the following related responsibilities:

- Authorizes operation of an information system,

- Issues an interim authorization to operate the information system under specific terms and conditions, or

- Denies authorization to operate the information system (or if the system is already operational, halts operations) if unacceptable security risks exist.

2.5   *System Operational Status*

Indicate one or more of the following for the system's operational status. If more than one status is selected, list which part of the system is covered under each status.

- Operational – the system is in production
- Under Development – the system is being designed, developed, or implemented
- Undergoing a major modification – the system is undergoing a major conversion or transition.

If the system is under development or undergoing a major modification, provide information about the methods used to assure that up-front security requirements are included. Include specific controls in the appropriate sections of the plan depending on where the operational status of the system.

2.6   General Description/Purpose

Prepare a brief description (one to three paragraphs) of the function and purpose of the system (e.g., economic indicator, network support for an agency, business census data analysis, crop reporting support).

2.7   System Environment

Provide a brief (one to three paragraphs) general description of the technical system.
Include any environmental or technical factors that raise special security concerns, such as use of Personal Digital Assistants, wireless technology, etc. Typically, operational environments are as follows:

- **Standalone or Small Office/Home Office (SOHO)** describes small, informal computer installations that are used for home or business purposes. Standalone encompasses a variety of small-scale environments and devices, ranging from laptops, mobile devices, or home computers, to telecommuting systems, to small businesses and small branch offices.

- **Managed or Enterprise** are typically large agency systems with defined, organized suites of hardware and software configurations, usually consisting of centrally managed workstations and servers protected from the Internet by firewalls and other network security devices.

- **Custom environments** contain systems in which the functionality and degree of security do not fit the other environments. Two typical Custom environments are Specialized Security-Limited Functionality and Legacy:

  - **Specialized Security-Limited Functionality**. A Specialized Security-Limited Functionality environment contains systems and networks at high risk of attack or data exposure, with security taking precedence over functionality. It assumes systems have limited or specialized (not general purpose workstations or systems) functionality in a highly threatened environment such as an outward facing firewall or public web server or whose data content or mission purpose is of such value that aggressive trade-offs in favor of security outweigh the potential negative consequences to other useful system attributes such as legacy applications or interoperability with other systems. A Specialized Security-Limited Functionality environment could be a subset of another environment.

  - **Legacy**. A Legacy environment contains older systems or applications that may use older, less-secure communication mechanisms. Other machines operating in a

Legacy environment may need less restrictive security settings so that they can communicate with legacy systems and applications. A Legacy environment could be a subset of a standalone or managed environment.

2.8 Laws, Regulations, and Policies Affecting the System

List any laws, regulations, or policies that establish specific requirements for confidentiality, integrity, or availability of the system and information retained by, transmitted by, or processed by the system. Each agency should decide on the level of laws, regulations, and policies to include in the system security plan. Examples might include the Privacy Act of 1974 or a specific statute or regulation concerning the information processed (such as Health Insurance Portability and Accountability Act of 1996, the Rehabilitation Act of 1973, Payment Card Industry Data Security Standards, Internal Revenue Service standards, etc.).

2.9 Security Controls

The ITRM Information Technology Security Standard SEC501-01 provides minimum security requirements for COV information and information systems. The requirements represent a broad-based, balanced information security program that addresses the management, operational, and technical aspects of protecting the confidentiality, integrity, and availability of COV information and information systems. An agency must meet the minimum security requirements in this standard by applying security controls selected in accordance with Information Technology Security Policy SEC500-02 and the designated impact levels of the information systems. An agency has the flexibility to tailor the security control baseline in accordance with the terms and conditions set forth in the standard. Tailoring activities include: (i) the application of scoping guidance; (ii) the specification of compensating controls; and (iii) the specification of agency-defined parameters in the security controls, where allowed. The system security plan should document all tailoring activities.

2.9.1 Mitigating Controls

Mitigating security controls are the management, operational, or technical controls employed by an agency in lieu of prescribed controls in the low, moderate, or high security control baselines, which provide equivalent or comparable protection for an information system. Mitigating security controls for an information system will be employed by an agency only under the following conditions: (i) the agency selects the compensating controls ; (ii) the agency provides a complete and convincing rationale and justification for how the mitigating controls provide an equivalent security capability or level of protection for the information system; and (iii) the agency assesses and formally accepts the risks associated with employing the mitigating controls in the information system. The use of mitigating security controls must be reviewed, documented in the system security plan, and approved by the authorizing official for the information system.

2.9.2 Minimum Security Controls

Now that the security controls have been selected, tailored, and the common controls identified, describe each control. The description should contain 1) the security control title; 2) how the security control is being implemented or planned to be implemented; 3) any scoping guidance that has been applied and what type of consideration; and 4) indicate if the security control is a common control and who is responsible for its implementation.

Security controls have a well-defined organization and structure. The security controls are organized into classes and families for ease of use in the control selection and specification process. There are three general classes of security controls (i.e., management, operational, and technical). Each family contains security controls related to the security function of the family. Security control class designations (i.e., management, operational, and technical) are defined below for clarification in preparation of system security plans:

> *Management controls* focus on the management of the information system and the management of risk for a system. They are techniques and concerns that are normally addressed by management.

> *Operational controls* address security methods focusing on mechanisms primarily implemented and executed by people (as opposed to systems). These controls are put in place to improve the security of a particular system (or group of systems). They often require technical or specialized expertise and often rely upon management activities as well as technical controls.

> *Technical controls* focus on security controls that the computer system executes. The controls can provide automated protection for unauthorized access or misuse, facilitate detection of security violations, and support security requirements for applications and data.

2.10 Completion and Approval Dates

The completion date of the system security plan should be provided. The completion date should be updated whenever the plan is periodically reviewed and updated. The system security plan should also contain the date the authorizing official or the designated approving authority approved the plan. Approval documentation, i.e., approval memorandum, should be on file or attached as part of the plan.

2.11 Ongoing System Security Plan Maintenance

Once the information system security plan is developed, it is important to periodically assess the plan, review any change in system status, functionality, design, etc., and ensure that the plan continues to reflect the correct information about the system. This documentation and its correctness are critical for system compliance activity. All plans should be reviewed and updated, if appropriate, at least every three years or more often if necessary. Some items to include in the review are:

- Change in information system owner;
- Change in information security representative;
- Change in system architecture;
- Change in system status;
- Additions/deletions of system interconnections;
- Change in system scope;
- Change in authorizing official

3   IT System Hardening

IT System Hardening comprises technical security controls designed to protect COV IT systems against IT security vulnerabilities. These controls include, among others, removing unneeded services, blocking unused networking ports, updating patch levels, and eliminating default accounts and passwords. The primary means of implementing these controls is through the development and enforcement of baseline IT security configuration standards.

3.1 Baseline IT Security Configuration Standards

A baseline IT security configuration standard is a comprehensive set of configuration settings for a particular type of IT system platform. As a set, these configuration settings provide an adequate level of technical security control for the type of IT system platform.

3.1.1   Establishing Baseline IT Security Configuration Standards

Agencies should establish baseline IT security configuration standards for each group of IT systems with similar characteristics. These groups of IT system classes may be defined by (but are not limited to) specific:

1. Hardware platforms (e.g., desktop models, routers, wireless access points);
2. Operating systems (e.g., Windows XP, Windows 2000, Unix);
3. Functions (e.g., back-office administration workstations, publicly accessible web servers, engineering workstations); and
4. Combinations of the above.

Agencies should establish baseline IT security configuration standards both for sensitive and non-sensitive IT systems. Sensitive IT systems will likely require more stringent controls than less sensitive systems. In addition, agencies may need to establish multiple baseline IT security configuration standards for each group of sensitive and non-sensitive IT systems. For example, a customer-facing IT system will likely require more stringent controls than an IT system for internal agency use.

In general, more stringent baseline security configuration standards are more difficult and costly to implement and manage. The baseline security configuration standard of each IT

system should be based on the system's sensitivity, its criticality to agency operations, and its potential exposure to risk.

Many standard baselines have been developed by IT system vendors. An easy and effective way to baseline IT systems is to use baselines developed and recommended by the vendors of the hardware, operating systems, and database management systems used by the agency. After examining vendor offerings, other useful sources of potential baselines should be considered, such as the websites provided by the National Institute of Standards and Technology (http://csrc.nist.gov/checklists/), and the Center for Internet Security (http://www.cisecurity.org/sitemap.html)[3]. COV agencies may access the proprietary material on the Center for Internet Security (CIS) free of charge.

To download CIS benchmarks:
1. Browse to the CIS website;
2. Click on a bench mark;
3. Select "Public User";
4. Fill out the on-line form;
5. Select the benchmarks to download;
6. Read and accept the user agreement; and
7. Download the desired benchmarks.

3.1.2   Baseline IT Security Configuration Standards Records

Each agency should maintain records outlining the baseline IT security configuration standard for each group of IT systems that it operates. This documentation can be as simple as a checklist describing the individual controls comprising the standard, and whether or not the control has been applied to the respective IT system. For circumstances in which the agency's security configuration for an individual IT system deviates from the baseline security configuration standard for the group, the agency should maintain records documenting the business necessity for the deviation, as well as System Owner approval of the deviation. Because requirements for baseline IT security configuration standards records vary widely based on the needs of the agency, this Guideline does not recommend a specific format for these records.

3.1.3   Vulnerability Scanning

Vulnerability scanning uses automated tools to probe IT systems and applications for weaknesses that could be exploited. Some examples of common weaknesses probed include:

1. Open Ports
   A port is like a door between a network and an IT system. Open ports enable an outside user or computer system to invoke and execute an application on the local

---

[3] Hyperlinks are current as of July 2008.

IT system. While this can be very useful, and is often necessary to the work of the agency, uncontrolled open ports almost always pose risks. When hardening an IT system, all open ports should be evaluated, and if no business requirement exists, they should be closed.

2. Active Services
   Services (also known as daemons or background processes) are computer programs that run in the background (transparently to human users) waiting to be useful to the operating system or other programs. Many active services are vital to the normal function and operation of a given IT system, but, depending on the operating system and configuration, active services may require high privileges. These services can pose serious vulnerabilities to all aspects of the security of the IT systems and the data it processes. When hardening an IT system, all active services should be evaluated, and if no business requirement exists, they should be disabled.

3. Patch Level
   Most IT systems vendors (hardware, operating systems, and applications) continuously examine their products for security vulnerabilities and develop patches (fixes) for them. Patches are often automatically distributed, but because of the increasing number of patches, many organizations lag in applying the most current patches across the enterprise. An un-patched IT system remains vulnerable to the issue the patch was designed to correct. Some vulnerability scanners probe the IT system to determine if known patches have been applied.

Many commercial and open source products for vulnerability scanning are available. Some effective, no-cost tools include[4]:

- Microsoft Baseline Security Analyzer (http://www.microsoft.com/technet/security/tools/mbsa2/default.mspx) provides basic remote scanning limited to Microsoft operating systems. This product is quick and easy to administer, but provides only very basic functionality.

- Nessus (http://www.nessus.org) provides a modular network scanner with available plug-ins covering almost every common IT system.

- Nmap (http://insecure.org) is a free security scanner that can evaluate the ports being used by and open on IT systems, and discover servers and services on a computer network. Nmap is used by Nessus.

3.1.4   Baseline Review and Modification

---

[4] Hyperlinks are current as of July 2008.

Agencies should periodically review individual IT system security configurations and baseline IT security configuration standards for currency and validity. Individual IT system security reviews should occur whenever an IT system has undergone significant changes or the threat environment has changed. Because of the dynamic nature of the IT security threat environment, best practice suggests agencies should review both individual IT systems security configurations and baseline IT security configuration standards annually, at a minimum. Changes to individual IT systems security configurations and baseline IT security configuration standards should be approved in advance by the System Owner.

4   Malicious Code Protection

Malicious Code Protection controls protect IT systems from damage caused by software designed to infiltrate or damage a computer system without the owner's informed consent. Types of this malicious software, often known as "malware", include computer viruses, worms, Trojan horses, spyware, and adware.

4.1   Types of Malicious Code

4.1.1   Infectious Malware: Viruses and Worms

Infectious malware are distinguished by their ability to replicate themselves. Today, the distinction between viruses and worms is hazy, but many authorities believe a virus requires human action to reproduce, while a worm propagates autonomously.

4.1.2   Concealment Malware: Trojan Horses

Concealment malware masquerades as a desirable program, but has a hidden agenda. Trojan horses have been used for simple vandalism (destroying files and IT systems), but more recent Trojan horses often have more sinister purposes. These modern Trojans can be used to enable unauthorized IT system access (rootkits), monitor system and user actions (spyware/adware, loggers), and remotely control IT systems to cause them to attack other targets (bots).

4.1.3   Rootkits

A rootkit is installed in order to give an unauthorized user complete access and control of a target IT system. Rootkits conceal the tracks of privileged activity by hiding files, network connections, memory addresses, or registry entries from other programs which detect privileged accesses to computer resources. Rootkits, in themselves, do not harm the systems on which they are installed, but their ability to conceal illegal activities and damage creates a considerable vulnerability.

4.1.4   4.1.4 Monitoring Malware: Spyware / Adware and Loggers

Trojans are often used to install programs which monitor user activities and send the
information to the attacker. Spyware is a ubiquitous type of monitor primarily used to
track Web activity. Spyware has been used to monitor purchasing habits, and to collect
usernames and passwords. Loggers monitor keystrokes and can send very sensitive
information to the attacker.

4.1.5   4.1.5 Bots

Bots are programs, usually spread by Trojans, which can seize control of an Internet-
connected system and cause it to participate in a network-based attack on another IT
system. Attackers have assembled networks of bots, or "zombies", and used them to send
so much network traffic to a victim's IT system that the victim was unable to conduct
business over the Internet.

4.1.6   4.1.6 Malicious Program Prohibitions and Requirements

Due to the prevalence of malware and its potentially adverse impact on IT systems,
agencies must make malware detection, protection, and eradication key features of their
security programs. Malware takes many forms, and can impact IT systems in varying
ways. Therefore, the Standard requires agencies to:

- Prohibit all users of their IT systems from developing, experimenting, or intentionally
  propagating malware, or even opening email attachments from unknown sources.
  Malware can be launched simply by opening an email attachment, and experimenting
  with such programs can unintentionally spread them throughout an organization.

- Provide malware detection, protection, eradication, logging, and reporting capabilities
  on all IT systems. This includes malware carried by email. The definition files that
  keep the malware-protection programs current must be automatically downloaded as
  new files become available. Malware protection must automatically start whenever
  the IT system is booted. Meeting these requirements is essential in preventing the
  introduction and spread of malware within an organization.

- Train users in protecting the agency's IT systems against malware as part of the IT
  security training program. Awareness of the danger posed by malware, and the
  proactive steps required to prevent its introduction into an organization are also
  essential in preventing the introduction and spread of malware within an organization.

- Design agency networks to enable malware to be removed or quarantined before it
  can infect a production IT system. One common design is to conduct scanning for
  malware on an IT system platform in the organization's screened subnet (also known
  as a DMZ), where it can be quarantined before entering the organization's internal
  network.

▪ Implement IT system user and administrator procedures to respond to attacks by malware. Because malware can spread so quickly, organizations should have response procedures that can be implemented as soon as a malware outbreak is detected.

▪ Use only new media (e.g., CD-ROM, DVD, and Flash Drives) or sanitized media for making copies of software for distribution. Distribution media may only be created on workstations or desktops that are inaccessible to casual users. Practices such as these prevent the spread of malware from contaminated systems and media, either by accident or design.

▪ Prohibit, by written policy, the installation of software on Agency IT systems until the software is approved by the Information Security Officer (ISO) or designee. All software should be evaluated by competent personnel to determine that it does not have unintended effects before it is introduced into the organization. Agencies should be particularly vigilant to prevent the unintended introduction of keystroke logging programs into their IT environments.

4.2 Malicious Code Protection Best Practices

1. **Educate the users.** User awareness is heightened by including information about malware and malware protection in regular bulletins to agency IT systems users.

2. **Train your users.** Make sure every user receives training about their role in responding to a malware infection.

3. **Use multiple vendors, but not on the same IT system.** Using multiple vendors reduces the risk of vulnerability in one vendor's protection code putting the entire agency at risk.

4. **Centrally manage the updating of protection software.** Do not leave the decision of when, what, and how to update to the users.

5. **Put most of the load outside of the agency network.** Use hardware-based malware protection solutions and place the devices on the edge of the agency network. This provides defense-in-depth and reduces the amount of anti-malware work agency desktops and workstations have to perform. However, it does not obviate the requirement for malware protection on each system.

4.3 4.3 Response to Malicious Code Incidents

Once a malware incident is detected, it is very important to follow the general recommendations described in the IT Threat Management Guideline (ITRM Guideline SEC506-01). Some specific response measures include:

1. If the affected IT system can be isolated from the network without increasing the impact, do so.
2. If the affected IT system can be taken out of production use without increasing the impact, do so.
3. If there is an indication of root kit installation, isolate the system, keep it powered on, and contact the VITA Customer Care Center for forensic support. Shutting down the IT system could erase valuable evidence.
4. Follow the incident reporting guidelines detailed at
    http://www.vita.virginia.gov/security/incident/guidance.cfm .
5. For a server, desktop, or workstation, once any evidence has been collected and the system has been released for use, it's best to wipe all storage and completely rebuild the IT system from scratch. Even after using root kit detection software, it is almost impossible to completely guarantee all root kits or backdoors have been removed, unless the IT system is rebuilt.

5   IT Systems Development Life Cycle (SDLC) Security

IT SDLC security analysis and design defines security-related tasks that must occur in each phase of the SDLC (Figure 2) starting with project initiation through disposal. IT security controls are most effective if designed into the IT system and maintained as an integral part of the system. To provide effective security, for example, agencies should conduct IT risk assessments of systems at various points throughout the SDLC, including an initial risk assessment in the early stages of system development, as well as follow-up risk assessments in later stages of the SDLC. Templates and examples for conducting security tasks during the
SDLC may be found in the Commonwealth Project Management Guideline
http://www.vita.virginia.gov/oversight/projects/default.aspx?id=555 .[5]

---

[5] Hyperlinks are current as of July 2008
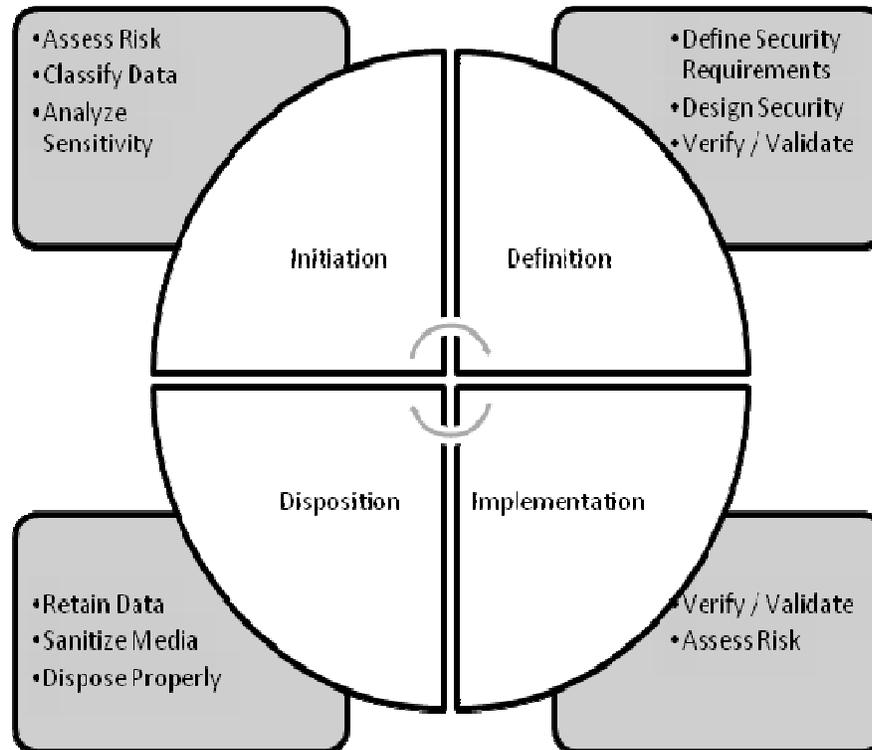
Figure 2 IT SDLC security Activities

5.1   *Project Initiation Security Tasks*

Conduct an initial high-level risk assessment of the IT system. Since the system has not yet been designed, use the initial requirements. Instructions can be found in the IT Risk Assessment Guideline (ITRM SEC506-01). Classify the data the IT system will process, and determine the sensitivity of the proposed IT system. Instructions can be found in ITRM SEC506-01, Section 4. Make sure the collection and maintenance of sensitive data is truly needed by the agency.

5.2   *Project Definition Security Tasks*

The results of the initial risk assessment can be used to define the IT security requirements for the system. The system should be designed so as to support essential IT security requirements. Develop procedures to verify and validate that the implemented system has incorporated the required security controls. Executing the procedures should result in a report identifying controls that did not meet security specifications.

5.3   *Project Implementation Security Tasks*

Using the developed test procedures, validate and verify the IT system has incorporated the required security controls. Conduct a risk assessment of the implemented system. Use the results to drive any required operational controls.

5.4   Disposition Security Tasks

At the end of the IT system's life cycle, and prior to disposal:

- Retain data in accordance with the agency's record retention policy.

- Sanitize all data storage media. Guidance may be found in the IT Data Protection Guideline (SEC507-00).

Dispose of IT system components in accordance with the Removal of Commonwealth Data from Surplus Computer Hard Drives and Electronic Media Standard (ITRM Standard SEC514-03).

- *Appendix A* provides a system security plan template.
- *Appendix B* provides a glossary for this guideline and for the template.

Appendices

These Appendices provide a template and glossary that agencies may use to document their use of many of the methodologies described in this Guideline. Each template consists of:

1) An example of the document, completed with functional information; and

2) A blank version of the template for use by COV agencies.

The examples use different fonts for instructions and example information, as follows:
- Times New Roman text is used for the template itself.
- **Shaded Arial Bold text** is example text.
- *Times New Roman Italic text* is provided as instructions for completing the template.

Appendix A - Information System Security Plan

Sample Template

The following sample has been provided ONLY as one example. Agencies may be using other formats and choose to update those to reflect any existing omissions based on this guidance. This is not a mandatory format; it is recognized that numerous agencies and information security service providers may have developed and implemented various approaches for information system security plan development and presentation to suit their own needs for flexibility.

Information System Security Plan Template

1. Information System Name/Title: Unique identifier and name given to the system.

2. Information System Owner and other Designated Contacts: Name, title, agency, address, email address, and phone number of person who owns the system.

3. Authorizing Official: Name, title, agency, address, email address, and phone number of the official designated as the authorizing official, such as Agency Head or designated ISO.

4. Information System Operational Status: Indicate the operational status of the system. If more than one status is selected, list which part of the system is covered under each status.

Operational	Under Development	Major Modification

5. General System Description/Purpose: Describe the function or purpose of the system and the information processes.

6. System Environment: Provide a general description of the technical system. Include the primary hardware, software, and communications equipment.

7. **Related Laws/Regulations/Policies:** List any laws or regulations that establish specific requirements for the confidentiality, integrity, or availability of the data in the system.

8. Plan to Implement Recommended Controls (reference Risk Assessment): Provide a description of how security controls recommended from the risk assessment are being implemented or planned to be implemented, and who is responsible for the implementation.

9. Information System Security Plan Completion Date: _____ Enter the completion date of the plan.

10. Information System Security Plan Approval Date: _____ Enter the
date the system security plan was approved and indicate if the approval documentation is
attached or on file.

Appendix B - Glossary

COMMON TERMS AND DEFINITIONS

Academic Instruction and Research Systems: Those systems used by institutions of higher education for the purpose of providing instruction to students and/or by students and/or faculty for the purpose of conducting research.

Access: Access: The ability to use, modify or affect an IT system or to gain entry to a physical area or location.

Access Controls: Access controls: A set of security procedures that monitor access and either allow or prohibit users from accessing IT systems and data. The purpose of access controls is to prevent unauthorized access to IT systems.

Accountability: The association of each log-on ID with one and only one user, so that the user can always be tracked while using an IT system, providing the ability to know which user performed what system activities.

Agency Head: The chief executive officer of a department established in the government of the Commonwealth of Virginia.

Alert: Notification that an event has occurred or may occur.

Alternate Site: A location used to conduct essential business functions in the event that access to the primary facility is denied or the primary facility has been so damaged as to be unusable.

Application: A computer program or set of programs that meet a defined set of business needs. See also *Application System.*

Application System: An interconnected set of IT resources under the same direct management control that meets a defined set of business needs. See also *Application, Support System,* and *Information Technology (IT) System.*

Asset: Any software, data, hardware, administrative, physical, communications, or personnel resource.

Assurance: Measurement of confidence in a control or activity.

Attack: An attempt to bypass security controls on an IT system in order to compromise the data.

Audit: An independent review and examination of records and activities to test for adequacy of controls, measure compliance with established policies and operational procedures, and recommend changes to controls, policies, or procedures.

Authentication: The process of verifying an identity of a user to determine the right to access specific types of data or IT system.

Authorization: The process of granting access to data or IT system by designated authority after proper identification and authentication.

Availability: Protection of IT systems and data so that they are accessible to authorized users when needed without interference or obstruction.

Backup: The process of producing a reserve copy of software or electronic files as a precaution in case the primary copy is damaged or lost.

Business Continuity Plan: A set of processes and procedures to recover an organization's essential business functions in a manner and on a schedule to provide for the ongoing viability of the organization if a disruption to normal operations occurs.

Baseline Security Configuration: The minimum set of security controls that must be implemented on all IT systems of a particular type.

Business Function: A collection of related structural activities that produce something of value to the organization, its stakeholders or its customers. See also *Essential Business Function.*

Business Impact Analysis (BIA): The process of determining the potential consequences of a disruption or degradation of business functions.

Change Control: A management process to provide control and traceability for all changes made to an application system or IT system.

Chief Information Officer of the Commonwealth (CIO): The CIO oversees the operation of the Virginia Information Technologies Agency (VITA) and, under the direction and control of the Virginia Information Technology Investment Board (the Board), exercises the powers and performs the duties conferred or imposed upon him by law and performs such other duties as may be required by the Board.

Chief Information Security Officer of the Commonwealth (CISO): The CISO is the senior management official designated by the CIO of the Commonwealth to develop Information Security policies, procedures, and standards to protect the confidentiality, integrity, and availability of IT systems and data.

Commonwealth of Virginia (COV): The government of the Commonwealth of Virginia, and its agencies and departments.

Commonwealth of Virginia Computer Incident Response Team (COV CIRT): A function of the Incident Management division of the COV Security and Risk Management directorate. The COV CIRT operates under the direction of the Incident Management Director, and is primarily comprised of the Incident Management engineers, with additional resources available as needed on a per incident basis from IT Partnership technical, legal and human resources staff.

Computer Emergency Response Team Coordination Center (CERT/CC): a center of Internet security expertise, located at the Software Engineering Institute at Carnegie Mellon University that studies Internet security vulnerabilities, researches long-term changes in networked systems, and develops information and training to assist the CERTs of other organizations. See also *Incident Response Team* and *United States Computer Emergency Response Team (US-CERT).*

Confidentiality: The protection of data from unauthorized disclosure to individuals or IT systems..

Configuration Management: A formal process for authorizing and tracking all changes to an IT system during its life cycle.

Continuity of Operations Planning: The process of developing plans and procedures to continue the performance of essential business functions in the event of a business interruption or threat of interruption.

Continuity of Operations Plan (COOP): A set of documented procedures developed to provide for the continuance of essential business functions during an emergency.

Control Objectives for Information and related Technology (COBIT): A framework of best practices (framework) for IT management that provides managers, auditors, and IT users with a set of generally accepted measures, indicators, processes and best practices to assist them in maximizing the benefits derived through the use of information technology and developing appropriate IT governance and control.

Countermeasure: An action, device, procedure, technique, or other measure that reduces vulnerability or the impact of a threat to an IT system.

Credential: Information, such as a user ID and password passed from and IT system or IT system user to an IT system to establish access rights.

Cryptography: The process of transforming plain text into cipher text, and cipher text into plain text.

Customer-Facing IT System: An IT system designed and intended for by external agency customers and or by the public. COV employees, contractors, and business partners may also use such systems. See also IT System and Internal IT System.

Data: An arrangement of numbers, characters, and/or images that represent concepts symbolically...

Database: A collection of logically related data (and a description of this data), designed to meet the information needs of an organization.

Data Classification: A process of categorizing data according to its sensitivity.

Data Custodian: An individual or organization in physical or logical possession of data for Data Owners. Data Custodians are responsible for protecting the data in their possession from unauthorized access, alteration, destruction, or usage and for providing and administering general controls, such as back-up and recovery systems.

Data Owner: An agency Manager, designated by the Agency Head or Information Security Officer, who is responsible for the policy and practice decisions regarding data. For business data, the individual may be called a business owner of the data.

Data Security: Data Security refers to those practices, technologies, and/or services used to apply security appropriately to data.

Data Sensitivity: See Sensitivity.

Demilitarized Zone(DMZ): A network segment made up of a firewall(s) that is located between the protected and the unprotected networks

Digital Certificate: An electronic document attached to a file that certifies the file is from the organization it claims to be from and has not been modified from the original format.

Digital Signature: A number that uniquely identifies the sender of a message and proves the message is unchanged since transmission.

Disaster Recovery Plan (DRP): A set of documented procedures that identify the steps to restore essential business functions on a schedule that supports agency mission requirements.

Data Storage Media: A device used to store IT data. Examples of data storage media include floppy disks, fixed disks, CD-ROMs, and USB flash drives.

Electronic Information: Any information stored in a format that enables it to be read, processed, manipulated, or transmitted by an IT system.

Encryption: The process or the means of converting original data to an unintelligible form so it cannot be read by unauthorized users..

Essential Business Function: A business function is essential if disruption or degradation of the function prevents the agency from performing its mission as described in the agency mission statement.

Evaluation: Procedures used in the analysis of security mechanisms to determine their effectiveness and to support or refute specific system weaknesses.

Extranet: A trusted network; used by COV to connect to a third-party provider.

Federal Information Security Management Act (FISMA): Federal legislation whose primary purpose is to provide a comprehensive framework for IT security controls in Federal agencies.

Firewall: Traffic-controlling gateway that controls access, traffic, and services between two networks or network segments, one trusted and the other untrusted.

Function: A purpose, process, or role.

Group: A named collection of IT system users; created for convenience when stating authorization policy.

Group-based Access: Authorization to use an IT system and/or data based on membership in a group.

Harden: The process of implementing software, hardware, or physical security controls to mitigate risk associated with COV infrastructure and/or sensitive IT systems and data.

High Availability: A requirement that the IT system is continuously available, has a low threshold for down time, or both.

Identification: The process of associating a user with a unique user ID or login ID.

Incident Response Capability (IRC): The follow-up to an incident including reporting, responding and recovery procedures.

Information: Data organized in a manner to enable their interpretation.

Information Security Officer (ISO): The individual designated by the Agency Head to be responsible for the development, implementation, oversight, and maintenance of the agency's IT security program.

Information Technology (IT): Telecommunications, automated data processing, databases, the Internet, management information systems, and related information, equipment, goods, and services.

Information Technology (IT) Assurance: Measures that protect and defend information and IT systems by providing for their availability, integrity, authentication, confidentiality, and non-repudiation.

Information Technology (IT) Contingency Planning: The component of Continuity of Operations Planning that prepares for continuity and/or recovery of an organization's IT systems and data that support its essential business functions in the event of a business interruption or threat of interruption.

Information Technology (IT) Infrastructure Library (ITIL): A framework of best practice processes designed to facilitate the delivery of high quality information technology (IT) services.

Information Technology (IT) Security: The protection afforded to IT systems and data in order to preserve their availability, integrity, and confidentiality.

Information Technology (IT) Security Architecture: The logical and physical security infrastructure made up of products, functions, locations, resources, protocols, formats, operational sequences, administrative and technical security controls, etc., designed to provide the appropriate level of protection for IT systems and data.

Information Technology (IT) Security Audit: The examination and assessment of the adequacy of IT system controls and compliance with established IT security policy and procedures.

Information Technology (IT) Security Auditor: CISO personnel, agency Internal Auditors, the Auditor of Public Accounts, or a private firm that, in the judgment of the agency, has the experience and expertise required to perform IT security audits.

Information Technology (IT) Security Breach: The violation of an explicit or implied security policy that compromises the integrity, availability, or confidentiality of an IT system.

Information Technology (IT) Security Controls: The protection mechanisms prescribed to meet the security requirements specified for an IT system.

Information Technology (IT) Security Event: An occurrence that has yet to be assessed but may affect the performance of an IT system.

Information Technology (IT) Security Incident: An adverse event or situation, whether intentional or accidental, that poses a threat to the integrity, availability, or confidentiality of an IT system.

Information Technology (IT) Security Incident Response Team: An organization within an agency constituted to monitor IT security threats and prepare for and respond to

cyber attacks. See also *Computer Emergency Response Team Coordination Center (CERT/CC)* and *United States Computer Emergency Response Team (US-CERT).*

Information Technology (IT) Security Logging: Chronological recording of system activities sufficient to enable the reconstruction, review, and examination of the sequence of environments and activities surrounding or leading to an operation, a procedure, or an event in a transaction from its inception to its final results.

Information Technology (IT) Security Policy: A statement of the IT Security objectives of an organization, and what employees, contractors, vendors, business partners, and third parties of the organization must do to achieve these objectives.

Information Technology (IT) Security Program: A collection of security processes, standards, rules, and procedures that represents the implementation of an organization's security policy

Information Technology (IT) Security Requirements: The types and levels of protection necessary to adequately secure an IT system.

Information Technology (IT) Security Safeguards: See *Information Technology (IT) Security Controls.*

Information Technology (IT) Security Standards: Detailed statements of how employees, contractors, vendors, business partners, and third parties of an organization must comply with its IT Security policy.

Information Technology (IT) System: An interconnected set of IT resources under the same direct management control. See also *Application System* and *Support System.*

Information Technology (IT) System Sensitivity: See Sensitivity.

Information Technology (IT) System Users: As used in this document, a term that includes COV employees, contractors, vendors, third-party providers, and any other authorized users of IT systems, applications, telecommunication networks, data, and related resources.

Integrity: The protection of data or IT system from intentional or accidental unauthorized modification.

Internal IT System: An IT system designed and intended for use only by COV employees, contractors, and business partners. See also IT System and Customer-Facing IT System.

Internet: An external worldwide public data network using Internet protocols to which COV can establish connections.

Intranet: A trusted multi-function (data, voice, video, image, facsimile, etc.) private digital network using Internet

protocols, which can be developed, operated and maintained for the conduct of COV business.

Intrusion Detection: A method of monitoring traffic on the network to detect break-ins or break-in attempts, either manually or via software expert systems.

Intrusion Detection Systems (IDS): Software that detects an attack on a network or computer system. A Network IDS (NIDS) is designed to support multiple hosts, whereas a Host IDS (HIDS) is set up to detect illegal actions within the host. Most IDS programs typically use signatures of known cracker attempts to signal an alert. Others look for deviations of the normal routine as indications of an attack.

Intrusion Prevention Systems (IPS): Software that prevents an attack on a network or computer system. An IPS is a significant step beyond an IDS (intrusion detection system), because it stops the attack from damaging or retrieving data. Whereas an IDS passively monitors traffic by sniffing packets off of a switch port, an IPS resides inline like a firewall, intercepting and forwarding packets. It can thus block attacks in real time.

ISO/IEC 17799: An IT security standard published in 2005 by the International Organization for Standardization (ISO) and the International Electro-technical Commission (IEC). It provides best practice recommendations on IT security management for use by those who are responsible for initiating, implementing or maintaining information security management systems.

Key: A sequence of data used in cryptography to encrypt or decrypt information

Key Escrow: The process of storing the encryption key with a third-party trustee to allow the recovery of encrypted text.

Least Privilege: The minimum level of data, functions, and capabilities necessary to perform a user's duties.

Logon ID: An identification code (normally a group of numbers, letters, and special characters) assigned to a particular user that identifies the user to the IT system.

Malicious Code: Harmful code (such as viruses and worms) introduced into a program or file for the purpose of contaminating, damaging, or destroying IT systems and/or data. Malicious code includes viruses, Trojan horses, trap doors, worms, spy-ware, and counterfeit computer instructions (executables).

Malicious Software: See Malicious Code.

Management Control: A set of mechanisms designed to manage organizations to achieve desired objectives.

Mission Critical Facilities: The data center's physical surroundings as well as data processing equipment inside

and the systems supporting them that need to be secured to achieve the availability goals of the system function.

Monitoring: Listening, viewing, or recording digital transmissions, electromagnetic radiation, sound, and visual signals.

Non-repudiation: A characteristic of a message that validates that the message was sent by a particular organization or individual, and cannot be refuted.

Off-site Storage: The process of storing vital records in a facility that is physically remote from the primary site. To qualify as off-site, the facility should be at least 500 yards from the primary site and offer environmental and physical access protection.

Operational Controls: IT security measures implemented through processes and procedures.

Operational Risk: The possibility of loss from events related to technology and infrastructure failure, from business interruptions, from staff related problems and from external events such as regulatory changes.

Out-of-Band Communications: A secondary communications channel for emergencies and/or redundancy.

Password: A unique string of characters that, in conjunction with a logon ID, authenticates a user's identity.

Personal Digital Assistant (PDA): A digital device, which can include the functionality of a computer, a cellular telephone, a music player and a camera

Personal Identification Number (PIN): A short sequence of digits used as a password.

Personally Identifiable Information (PII): Any piece of information that can potentially be used to uniquely identify, contact, or locate a single person.

Personnel: All COV employees, contractors, and subcontractors, both permanent and temporary.

Phishing: A form of criminal activity characterized by attempts to acquire sensitive information fraudulently, such as passwords and credit card details, by masquerading as a trustworthy person or business in an apparently official electronic communication.

Privacy: The rights and desires of an individual to limit the disclosure of individual information to others.

Privacy Officer: The privacy officer, if required by statute (such as HIPPA) provides guidance on the requirements of state and federal Privacy laws; disclosure of and access to sensitive data; and security and protection requirements in conjunction with the IT system when there is some overlap among sensitivity, disclosure, privacy, and security issues.

Risk: The potential that an event may cause a material negative impact to an asset.

Risk Management: Identification and implementation of IT security controls in order to reduce risks to an acceptable level.

Recovery: Activities beyond the initial crisis period of an emergency or disaster that are designed to return IT systems and/or data to normal operating status.

Residual Risk: The portion of risk that remains after security measures have been applied.

Restoration: Activities designed to return damaged facilities and equipment to an operational status.

Risk: The possibility of loss or injury based on the likelihood that an event will occur and the amount of harm that could result.

Risk Assessment (RA): The process of identifying and evaluating risks so as to assess their potential impact.

Risk Mitigation: The continuous process of minimizing risk by applying security measures commensurate with sensitivity and risk.

Role-based Access Control: A type of access control in which IT system users receive access to the IT systems and data based on their positions or roles in an organization.

Roles and Responsibility: Roles represent a distinct set of operations and responsibilities required to perform some particular function that an individual may be assigned. Roles may differ from the individual's business title. This document contains the roles and responsibilities associated with implementing IT security.

Recovery Time Objective (RTO): The amount of time targeted for the recovery of a business function or resource after a disaster occurs.

Secure: A state that provides adequate protection of IT systems and data against compromise, commensurate with sensitivity and risk.

Sensitive: See Sensitivity.

Sensitivity: A measurement of adverse affect on COV interests, the conduct of agency programs, or the privacy to which individuals are entitled that compromise of IT systems and data with respect to confidentiality, integrity, and/or availability could cause.. IT systems and data are sensitive in direct proportion to the materiality of the adverse effect caused by their compromise.

Sensitivity Classification: The process of determining whether and to what degree IT systems and data are sensitive.

Separation of Duties: Assignment of responsibilities such that no one individual or function has control of an entire process. It is a technique for maintaining and monitoring accountability and responsibility for IT systems and data.

Shared Accounts: A logon ID or account utilized by more than one entity.

Spy-ware: A category of malicious software designed to intercept or take partial control of a computer's operation without the informed consent of that machine's owner or legitimate user. While the term taken literally suggests software that surreptitiously monitors the user, it has come to refer more broadly to software that subverts the computer's operation for the benefit of a third party.

State: See *Commonwealth of Virginia (COV).*

Support System: An interconnected set of IT resources under the same direct management control that shares common functionality and provides services to other systems. See also *Application System* and *Information Technology (IT) System.*

Subnet: A portion of a network that shares a common address component. On TCP/IP networks, subnets are defined as all devices whose IP addresses have the same prefix.

System. See *Information Technology (IT) System*

System Administrator: An analyst, engineer, or consultant who implements, manages, and/or operates a system at the direction of the System Owner, Data Owner, and/or Data Custodian.

System Owner: An agency Manager, designated by the Agency Head or Information Security Officer, who is responsible for the operation and maintenance of an agency IT system.

Technical Controls: IT security measures implemented through technical software or hardware.

Third-Party Provider: A company or individual that supplies IT equipment, systems, or services to COV Agencies.
Threat: Any circumstance or event (human, physical, or environmental) with the potential to cause harm to an IT system in the form of destruction, disclosure, adverse modification of data, and/or denial of service by exploiting vulnerability.

Token: A small tangible object that contains a built-in microprocessor utilized to store and process information for authentication.

Trojan horse: A malicious program that is disguised as or embedded within legitimate software.

Trusted System or Network: An IT system or network that is recognized automatically as reliable, truthful, and accurate, without continual validation or testing.

United States Computer Emergency Response Team (US-CERT): A partnership between the Department of Homeland security and the public and private sectors, intended to coordinate the response to IT security threats from the Internet. As such, it releases information about current IT security issues, vulnerabilities and exploits as Cyber Security Alerts, and works with software vendors to create patches for IT security vulnerabilities. See also *Computer Emergency Response Team Coordination Center (CERT/CC)* and *Incident Response Team.*

Universal Serial Bus (USB): A standard for connecting devices.

Untrusted: Characterized by absence of trusted status. Assumed to be unreliable, untruthful, and inaccurate unless proven otherwise.

USB Flash Drive: A small, lightweight, removable and rewritable data storage device.

User ID: A unique symbol or character string that is used by an IT system to identify a specific user. See Logon ID.

Virginia Department of Emergency Management (VDEM): A COV department that protects the lives and property of Virginia's citizens from emergencies and disasters by coordinating the state's emergency preparedness, mitigation, response, and recovery efforts.

Version Control: A management process that provides traceability of updates to operating systems and supporting software.
Virus: See Malicious Code.

Virginia Information Technologies Agency (VITA): VITA is the consolidated, centralized IT organization for COV.

Vital Record: A document, regardless of media, which, if damaged or destroyed, would disrupt business operations.

Vulnerability: A condition or weakness in security procedures, technical controls, or operational processes that exposes the system to loss or harm.

Workstation: A terminal, computer, or other discrete resource that allows personnel to access and use IT resources.