ITRM Standard SEC501-06
Date: April 4, 2011
Compliance Date for Revisions: July 1, 2011

COMMONWEALTH OF VIRGINIA

Information Technology Resource Management

Information Security Standard

Virginia Information Technologies Agency (VITA)

ITRM Publication Version Control

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

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

Version	Date	Purpose of Revision
Original	12/07/2001	Base Document
Revision 1	07/01/2006	To update all sections of the Standard in accordance with changes to the Code of Virginia as well as incorporate emerging best practices.
	10/10/2006	To remove from section 2.1 (page 3) "Risk Response" that was erroneously left in the final version of this standard. Also, there are no requirements impacted by this correction.
Revision 2	07/1/2007	Revision to align with changes (blue highlights) to the Code of Virginia and to document additional and substantively revised standards. The compliance date for these new and substantively revised standards is July 1, 2008.
Revision 3	10/30/2007	Revision to incorporate ITIB's directive (dated October 18, 2007) to change compliance date from July 2008 to November 1, 2007 for section 9.5.2 items 3 through 6.
Revision 4	07/24/2008	Revision to align with changes (blue highlights) to the Code of Virginia, removed language in the scope section that excluded "Academic Instruction and Research" systems, and to document additional and revised standards. There is a new section for Application Security. The compliance date for these new and substantively revised standards is January 1, 2009 except for academic and research systems previously exempted, the compliance date shall be July 1, 2009.
Revision 5	08/11/2009	Revision to establish a new Wireless Security section and enhance the Application Security section. Broaden scope to include recommendations for security best practices relative to non-electronic data. Refine intent and incorporate changes based on contributions and suggestions of the COV Information Security community. On October 19, 2009, Section 2.2.4 #1 was revised for clarity. Effective February 2, 2010, Section 5.3.2, # 8, page 29 - the requirement related to the frequency of changing user passwords for sensitive systems was changed from 42 days to 90 days to be consistent with current COV network password change frequency requirements. Agencies may require users of sensitive systems to change their passwords on a more frequent basis.

Revision 6	*04/4/2011*	*Revisions effective April 4, 2011* *Revision to indicate how to identify changes in the document by a vertical line in the left margin and underlined italics indicating added language.* *Revised to address the new IT governance structure in the Commonwealth.* *See section 1.2.1, section 2.7.2 #3, section 4.3.2 #s 9, 10, & 11, section 4.7.2 #8, section 9.2.2 # 6, and section 9.5.2 for new guidance and requirements.*

Review Process

Information Technology Enterprise Governance and Solutions (ESG) Directorate Review

Policy, Practices, and Architecture (PPA) Division provided the initial review of this publication.

Online Review

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

PREFACE

Publication Designation
COV ITRM Standard SEC501-06

Subject
Information Security

Date
April 4, 2011

Compliance Date
July 1, 2011 for revisions to the standard

Supersedes
COV ITRM Standard SEC501-01 dated *August 11, 2009 (revision: 5).*

Scheduled Review
One (1) year from effective date

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

Scope
In general, this *Standard* is applicable to the Commonwealth's executive, legislative, and judicial branches, and independent agencies and institutions of higher education (collectively referred to as "Agency"). This *Standard* is offered only as guidance to local government entities. Exemptions from the applicability of this *Standard* are defined in detail in Section 1.6.

In addition, the Code of Virginia § 2.2-2009, specifies that policies, procedures, and standards that address security audits (Section 2.7 of this *Standard*) apply only to *"all executive branch and independent agencies and institutions of higher education."* Similarly, *the* Code of Virginia § 2.2-603, specifies that requirements for reporting of information security incidents (Section 9.4 of the *Standard)* apply only to *"every department in the executive branch of state government."*

Purpose
To define the minimum requirements for each Agency's information security management program.

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

Secretary of Technology
Reviews and approves statewide technical and data policies, standards and guidelines for information technology and related systems recommended by the CIO.

Chief Information Officer of the Commonwealth (CIO)
Develops and recommends to the Secretary of Technology statewide technical and data policies, standards and guidelines for information technology and related systems.

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 information technology systems and data.

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

Information Technology Advisory Council (ITAC)
Advises the CIO and Secretary of Technology on the development, adoption and update of statewide technical and data policies, standards and guidelines for information technology and related systems.

Executive Branch Agencies
Provide input and review during the development, adoption and update of

statewide technical and data policies, standards and guidelines for information technology and related systems. Comply with the requirements established by COV policies and standards. Apply for exceptions to requirements when necessary.

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

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

International Standards
International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) ISO/IEC 27000 series.

Definitions
Definitions are found in the single comprehensive glossary that supports Commonwealth Information Technology Resource Management (ITRM) documents (COV ITRM Glossary).

Related ITRM Policy
Current version of the COV ITRM Policy (SEC519-): Information Security Policy.

Table of Contents

1. INTRODUCTION

1.1. Intent

The intent of this *Information Security Standard* is to establish a baseline for information security and risk management activities for agencies across the Commonwealth of Virginia (COV). These baseline activities include, but are not limited to, any regulatory requirements that an agency is subject to, information security best practices, and the requirements defined in this *Standard*. These information security and risk management activities will provide protection of, and mitigate risks to agency information systems and data.

This *Standard* defines the minimum acceptable level of information security and risk management activities for the COV agencies that must implement an information security program that complies with requirements identified in this *Standard*. Agencies may develop their own information security standards, based on needs specific to their environments. Agency standards must provide for protection of the agency's information systems and data, at a level greater than or equal to the baseline requirements set forth in this *Standard*. As used in this *Standard*, sensitivity encompasses the elements of confidentiality, integrity, and availability. See *IT System and Data Sensitivity Classification* for additional detail on sensitivity.

The COV Information Security Program consists of the following component areas:

- Risk Management
- IT Contingency Planning
- Information Systems Security
- Logical Access Control
- Data Protection
- Facilities Security
- Personnel Security
- Threat Management
- IT Asset Management

These component areas provide a framework of minimal requirements that agencies shall use to develop their agency information security programs with a goal of allowing agencies to accomplish their missions in a safe and secure environment. Each component listed above contains requirements that, together, comprise this *Information Security Standard*.

This *Standard* recognizes that agencies may procure IT equipment, systems, and services covered by this *Standard* from third parties. In such instances, Agency Heads remain accountable for maintaining compliance with this *Standard* and agencies must enforce these compliance requirements through documented agreements with third-party providers and oversight of the services provided.

1.2. ŦOrganization of this Standard

The component areas of the COV Information Security Program provide the organizational framework for this *Standard*. Each component area consists of one or more sections containing:

- A **Purpose** statement that provides a high-level description of the component area or subcomponent area and its importance in the COV Information Security Program;
- **Requirements** that are mandatory technical and/or programmatic activities for a specific component area;
- ***Recommended Best Practices*** *are advisory in nature and provide guidance to agencies in the development of their information security programs;*
- **Notes**, which provide rationale and explanation regarding the requirements; and
- **Examples** that describe the ways in which agencies might meet the requirements, but are not intended to replace agency judgment.

1.2.1. *Identifying Changes in this Document*

Please see the latest entry in the revision table above. Vertical lines in the left margin indicate the paragraph has changes or additions. Specific changes in wording are noted using italics indicating added language.

1.3. Roles and Responsibilities

Each agency should utilize an organization chart that depicts the reporting structure of employees when assigning specific responsibilities for the security of IT systems and data. Each agency shall maintain documentation regarding specific roles and responsibilities relating to information security.

1.4. Information Security Program

Each agency shall establish, document, implement, and maintain its information security program appropriate to its business and technology environment in compliance with this *Standard*. In addition, because resources that can reasonably be committed to protecting IT systems are limited, each agency must implement its information security program in a manner commensurate with sensitivity and risk.

1.5. Exceptions to Security Requirements

If an Agency Head determines that compliance with the provisions of this *Standard* or any related information security standards would adversely impact a business process of the agency, the Agency Head may request approval to deviate from a specific requirement by submitting an exception request to the CISO. For each exception, the requesting agency shall fully document:

1. The business need,
2. The scope and extent,
3. Mitigating safeguards,
4. Residual risks,
5. The specific duration, and
6. Agency Head approval.

Each request shall be in writing to the CISO and approved by the Agency Head indicating acceptance of the defined residual risks. Included in each request shall be a statement detailing the reasons for the exception as well as mitigating controls and all residual risks. Requests for exception shall be evaluated and decided upon by the CISO, and the requesting party informed of the action taken. An exception *will not be*

accepted for processing unless all residual risks have been *documented* and the Agency Head has approved, indicating acceptance of these risks. *The exception request must be submitted by the Agency Head or Agency ISO.* Denied exception requests may be appealed to the CIO of the Commonwealth. The form that agencies must use to document exception requests is included in the Appendix to this document.

1.6. Exemptions from Applicability

The following are explicitly exempt from complying with the requirements defined in this document:

1. Systems under development and/or experimental systems that do not create additional risk to production systems
2. Surplus and retired systems

2. RISK MANAGEMENT

2.1. Purpose

Risk Management delineates the steps necessary to identify, analyze, prioritize, and mitigate risks that could compromise IT systems and data. This section defines requirements for the following areas:

- Key Information Security Roles and Responsibilities
- Business Impact Analysis
- IT System and Data Sensitivity Classification
- Sensitive IT System Inventory and Definition
- Risk Assessment
- IT Security Audits

2.2. Key Information Security Roles and Responsibilities

2.2.1. Purpose

This Section defines the key IT security roles and responsibilities included in the Commonwealth's Information Security Program. These roles and responsibilities are assigned to individuals, and may differ from the COV role title or working title of the individual's position. Individuals may be assigned multiple roles, as long as the multiple role assignments provide adequate separation of duties, provide adequate protection against the possibility of fraud, and do not lead to a conflict of interests.

2.2.2. Chief Information Officer of the Commonwealth (CIO)

The Code of Virginia §2-2.2009 states that *"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."*

2.2.3. Chief Information Security Officer (CISO)

The CISO is responsible for development and coordination of the COV Information Security Program and, as such, performs the following duties:

1. Administers the COV Information Security Program and periodically assesses whether the program is implemented in accordance with COV Information Security Policies and Standards.

2. Reviews requested exceptions to COV Information Security Policies, Standards and Procedures.

3. Provides solutions, guidance, and expertise in IT security.

4. Maintains awareness of the security status of sensitive IT systems.

5. Facilitates effective implementation of the COV Information Security Program, by:

a. Preparing, disseminating, and maintaining information security, policies, standards, guidelines and procedures as appropriate;
b. Collecting data relative to the state of IT security in the COV and communicating as needed;
c. Providing consultation on balancing an effective information security program with business needs.

6. Provides networking and liaison opportunities to Information Security Officers (ISOs).

2.2.4. Agency Head

Each Agency Head is responsible for the security of the agency's IT systems and data. The Agency Head's IT security responsibilities include the following:

1. Designate an Information Security Officer (ISO) for the agency, no less than biennially. :

   Note: Acceptable methods of communicating the designation to the CISO, include:
   - An email directly from the agency head, or
   - An email from *an* agency *head designee* which copies the agency head, or
   - A hard-copy letter or facsimile transmission signed by the agency head.
   - This designation must include the following information:
     a. ISO's name
     b. ISO's title
     c. ISO's contact information

   Note: The ISO should report directly to the Agency Head where practical and should not report to the CIO. The ISO is responsible for developing and managing the agency's information security program. The Agency Head is strongly encouraged to designate at least one backup for the ISO. Agencies with multiple geographic locations or specialized business units should also consider designating deputy ISOs as needed.

2. Ensure that an agency information security program is maintained, that is sufficient to protect the agency's IT systems, and that is documented and effectively communicated. Managers in all agencies and at all levels shall provide for the IT security needs under their jurisdiction. They shall take all reasonable actions to provide adequate IT security and to escalate problems, requirements, and matters related to IT security to the highest level necessary for resolution.

3. Review and approve the agency's Business Impact Analyses (BIAs), Risk Assessments (RAs), and Continuity of Operations Plan (COOP), to include an IT Disaster Recovery Plan, if applicable.

4. Review or have the designated ISO review the System Security Plans for all agency IT systems classified as sensitive, and:
   - Approve System Security Plans that provide adequate protections against security risks; or

- Disapprove System Security Plans that do not provide adequate protections against security risks, and require that the System Owner implement additional security controls on the IT system to provide adequate protections against security risks.

5. Ensure compliance is maintained with the current version of the *IT Security Audit Standard* (COV ITRM Standard SEC502). This compliance must include, but is not limited to:
   a. Requiring development and implementation of an agency plan for IT security audits, and submitting this plan to the CISO;
   b. Requiring that the planned IT security audits are conducted;
   c. Receiving reports of the results of IT security audits;
   d. Requiring development of Corrective Action Plans to address findings of IT security audits; and
   e. Reporting to the CISO all IT security audit findings and progress in implementing corrective actions in response to IT security audit findings.

   Note: If the IT security audit shows no findings, this is to be reported to the CISO as well.

6. Ensure a program of information security safeguards is established.

7. Ensure an information security awareness and training program is established.

8. Provide the resources to enable employees to carry out their responsibilities for securing IT systems and data.

9. Identify a System Owner who is generally the Business Owner for each agency sensitive system. Each System Owner shall assign a Data Owner(s), Data Custodian(s) and System Administrator(s) for each agency sensitive IT system.

10. Prevent or have designee prevent conflict of interests and adhere to the security concept of separation of duties by assigning roles so that:
    a. The ISO is not a System Owner or a Data Owner except in the case of compliance systems for information security;
    b. The System Owner and the Data Owner are not System Administrators for IT systems or data they own; and
    c. The ISO, System Owners, and Data Owners are COV employees.

Notes:
- Other roles may be assigned to contractors. For roles assigned to contractors, the contract language must include specific responsibility and background check requirements.
- A System Owner can own multiple IT systems.
- A Data Owner can own data on multiple IT systems.
- System Administrators can assume responsibility for multiple IT systems.

2.2.5. Information Security Officer (ISO)

The ISO is responsible for developing and managing the agency's information security program. The ISO's duties are as follows:

1. Develop and manage an agency information security program that meets or exceeds the requirements of COV IT security policies and standards in a manner commensurate with risk.

2. Verify and validate that all agency IT systems and data are classified for sensitivity.

3. Develop and maintain an information security awareness and training program for agency staff, including contractors and IT service providers. Require that all IT system users complete required IT security awareness and training activities prior to, or as soon as practicable after, receiving access to any system, and no less than annually, thereafter.

4. Implement and maintain the appropriate balance of preventative, detective and corrective controls for agency IT systems commensurate with data sensitivity, risk and systems criticality.

5. Mitigate and report all IT security incidents in accordance with §2.2-603 of the Code of Virginia and VITA requirements and take appropriate actions to prevent recurrence.

6. Maintain liaison with the CISO.

2.2.6. Privacy Officer

An agency must have a Privacy Officer if required by law or regulation, such as the Health Insurance Portability and Accountability Act (HIPAA), and may choose to have one where not required. Otherwise, these responsibilities are carried out by the ISO. The Privacy Officer provides guidance on:

1. The requirements of state and federal Privacy laws.

2. Disclosure of and access to sensitive data.

3. Security and protection requirements in conjunction with IT systems when there is some overlap among sensitivity, disclosure, privacy, and security issues.

2.2.7. System Owner

The System Owner is the agency business manager responsible for having an IT system operated and maintained. With respect to IT security, the System Owner's responsibilities include the following:

1. Require that the IT system users complete any system unique security training prior to, or as soon as practicable after, receiving access to the system, and no less than annually, thereafter.

2. Manage system risk and developing any additional information security policies and procedures required to protect the system in a manner

commensurate with risk.

3. Maintain compliance with COV Information Security policies and standards in all IT system activities.

4. Maintain compliance with requirements specified by Data Owners for the handling of data processed by the system.

5. Designate a System Administrator for the system.

Note: Where more than one agency may own the IT system, and the agency or agencies cannot reach consensus on which should serve as System Owner, upon request, the CIO of the Commonwealth will determine the System Owner.

2.2.8. Data Owner

The Data Owner is the agency manager responsible for the policy and practice decisions regarding data, and is responsible for the following:

1. Evaluate and classify sensitivity of the data.

2. Define protection requirements for the data based on the sensitivity of the data, any legal or regulatory requirements, and business needs.

3. Communicate data protection requirements to the System Owner.

4. Define requirements for access to the data.

2.2.9. System Administrator

The System Administrator is an analyst, engineer, or consultant who implements, manages, and/or operates a system or systems at the direction of the System Owner, Data Owner, and/or Data Custodian. The System Administrator assists agency management in the day-to-day administration of agency IT systems, and implements security controls and other requirements of the agency information security program on IT systems for which the System Administrator has been assigned responsibility.

2.2.10. Data Custodian

Data Custodians are individuals or organizations in physical or logical possession of data for Data Owners. Data Custodians are responsible for the following:

1. Protecting the data in their possession from unauthorized access, alteration, destruction, or usage.

2. Establishing, monitoring, and operating IT systems in a manner consistent with COV Information Security policies and standards.

3. Providing Data Owners with reports, when necessary and applicable.

2.2.11. IT System Users

All users of COV IT systems including employees and contractors are responsible for the following:

1. Reading and complying with agency information security program requirements.

2. Reporting breaches of IT security, actual or suspected, to their agency management and/or the CISO.

3. Taking reasonable and prudent steps to protect the security of IT systems and data to which they have access.

2.3. Business Impact Analysis

2.3.1. Purpose

Business Impact Analysis (BIA) delineates the steps necessary for agencies to identify their business functions, identify those agency business functions that are essential to an agency's mission, and identify the resources that are required to support these essential agency business functions.

Note: The requirements below address only the IT and data aspects of BIA and **do not** require agencies to develop a BIA separate from the BIA that could be used to develop an agency's Continuity of Operations Plan (COOP). Agencies should create a single BIA that meets both the requirements of this *Standard* and can be used to develop the agency COOP. Agencies should consult the VDEM *Continuity of Operations Planning Manual* for COOP requirements.

2.3.2. Requirements

Each agency should:

1. Require the participation of System Owners and Data Owners in the development of the agency's BIA.

2. Identify agency business functions.

3. Identify essential business functions.

   Note: 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.

4. Identify dependent functions, if any. Determine and document any additional functions on which each essential business function depends. These dependent functions are essential functions as well.

5. For each essential business function and dependent function, assess whether the function depends on an IT system to be recovered. Each IT system that is required to recover an essential function or a dependent

function shall be considered sensitive relative to availability. For each such system, each agency shall:

a. Determine and document the required Recovery Time Objective (RTO), based on agency and COV goals and objectives.

b. Determine and document the Recovery Point Objectives (RPO).

6. Use the IT information documented in the BIA report as a primary input to IT System and Data Sensitivity Classification (Section 2.4), Risk Assessment (Section 2.6), IT Contingency Planning (Section 3) and IT System Security Plans (Section 4.2).

7. Conduct periodic review and revision of the agency BIAs, as needed, but at least once every three years.

2.4. IT System and Data Sensitivity Classification

2.4.1. Purpose

IT System and Data Sensitivity Classification requirements identify the steps necessary to classify all IT systems and data according to their sensitivity with respect to the following three criteria:

- Confidentiality, which addresses sensitivity to unauthorized disclosure;
- Integrity, which addresses sensitivity to unauthorized modification; and
- Availability, which addresses sensitivity to outages.

Sensitive data is any data of which the compromise with respect to confidentiality, integrity, and/or availability could have a material adverse effect on COV interests, the conduct of agency programs, or the privacy to which individuals are entitled. Data sensitivity is directly proportional to the materiality of a compromise of the data with respect to these criteria. Agencies must classify each IT system by sensitivity according to the most sensitive data that the IT system stores, processes, or transmits.

2.4.2. Requirements

Each agency ISO shall:

1. Identify or require that the Data Owner identify the type(s) of data handled by each agency IT system.

2. Determine or require that the Data Owner determine whether each type of data is also subject to other regulatory requirements.

   Example: Some IT systems may handle data subject to legal or business requirements such as the Health Insurance Portability and Accountability Act of 1996 (HIPAA); IRS 1075; the Privacy Act of 1974; Payment Card Industry (PCI); the Rehabilitation Act of 1973, § 508, Federal National Security Standards, etc.

3. Determine or require that the Data Owner determine the potential damages to the agency of a compromise of confidentiality, integrity or availability of each type of data handled by the IT system, and classify the sensitivity of the data accordingly.

   Example: Data Owners may construct a table similar to the following table. Data Owners must classify sensitivity requirements of all types of data. The following table is only an illustration of one way to accomplish this.

System ID: ABC123	Sensitivity Criteria		
Type of Data	**Confidentiality**	**Integrity**	**Availability**
HR Policies	Low	High	Moderate
Medical Records	High	High	High
Criminal Records	High	High	High

Table 1: Sample Sensitivity Analysis Results

4. Classify the IT system as sensitive if any type of the data handled by the IT system has a sensitivity of high on any of the criteria of confidentiality, integrity, or availability.

   Note: Agencies should consider classifying IT systems as sensitive even if a type of data handled by the IT system has a sensitivity of moderate on the criteria of confidentiality, integrity, and availability.

5. Review IT system and data classifications with the Agency Head or designee and obtain Agency Head or designee approval of these classifications.

6. Verify and validate that all agency IT systems and data have been reviewed and classified as appropriate for sensitivity.

7. Communicate approved IT system and data classifications to System Owners, Data Owners, and end-users.

8. Require that the agency prohibit posting any data classified as sensitive with respect to confidentiality on a public web site, ftp server, drive share, bulletin board or any other publicly accessible medium unless a written exception is approved by the Agency Head identifying the business case, risks, mitigating controls, and all residual risks.

9. Use the information documented in the sensitivity classification as a primary input to the Risk Assessment process defined in this *Standard*.

2.5. Sensitive IT System Inventory and Definition

2.5.1. Purpose

Sensitive IT System Inventory and Definition requirements identify the steps in listing and marking the boundaries of sensitive IT systems in order to provide

cost-effective, risk-based security protection for IT systems, for the agency as a whole, and for the COV enterprise.

2.5.2. Requirements

Each ISO or designated Sensitive System Owner(s) shall:

1. Document each sensitive IT system owned by the agency, including its ownership and boundaries, and update the documentation as changes occur.

   Note: Data and homogenous systems, belonging to a single agency, that have the same technical controls and account management procedures (i.e., Microsoft SharePoint, or PeopleSoft), may be classified and grouped as a single set of data or systems for the purpose of inventory, data classification, risk assessments, security audits, etc.

   Note: Where more than one agency may own the IT system, and the agency or agencies cannot reach consensus on which should serve as System Owner for the purposes of this *Standard,* upon request, the CIO of the Commonwealth will determine the System Owner.

   Note: A sensitive IT system may have multiple Data Owners, and/or System Administrators, but must have a single System Owner.

2. Maintain or require that its service provider maintain updated network diagrams.

2.6. Risk Assessment

2.6.1. Purpose

Risk Assessment requirements delineate the steps agencies must take for each IT system classified as sensitive to:

- Identify potential threats to an IT system and the environment in which it operates;
- Determine the likelihood that threats will materialize;
- Identify and evaluate vulnerabilities; and
- Determine the loss impact if one or more vulnerabilities are exploited by a potential threat.

Note: The Risk Assessment (RA) required by this *Standard* differs from the RA required by the current version of the *Project Management Standard* (CPM112-nn). This *Standard* requires an RA based on operational risk, while the *Project Management Standard* requires an RA based on project risk. Many of the RA techniques described in the *Project Management Standard*, however, may also be applicable to the RA required by this *Standard*.

2.6.2. Requirements

For each IT system classified as sensitive, the data-owning agency shall:

1. Conduct and document a RA of the IT system as needed, but not less than once every three years.

2. Conduct and document an annual self-assessment to determine the continued validity of the RA.

Note: In addition, in agencies that own both sensitive IT systems and IT systems that are exempt from the requirements of this *Standard*, the agency's RAs must include consideration of the added risk to sensitive IT systems from the exempt IT systems.

3. Prepare a report of each RA that includes, at a minimum, identification of all vulnerabilities discovered during the assessment, and an executive summary, including major findings and risk mitigation recommendations.

2.7. IT Security Audits

2.7.1. Purpose

IT Security Audit requirements define the steps necessary to assess whether IT security controls implemented to mitigate risks are adequate and effective.

Note: In accordance with *the* Code of Virginia § 2.2-2009, the requirements of this section apply only to *"all executive branch and independent agencies and institutions of higher education."*

2.7.2. Requirements

For each IT system classified as sensitive, the data-owning agency shall:

1. Require that the IT systems undergo an IT Security Audit as required by and in accordance with the current version of the *IT Security Audit Standard* (COV ITRM Standard SEC502).

2. Assign an individual to be responsible for managing IT Security Audits.

3. *IT Security Audits should only be performed by independent parties who are not associated with the processes or procedures of the system.*

3. IT CONTINGENCY PLANNING

3.1 Purpose

IT Contingency Planning delineates the steps necessary to plan for and execute recovery and restoration of IT systems and data if an event occurs that renders the IT systems and/or data unavailable. This component of the COV Information Security Program defines requirements in the following three areas:

- Continuity of Operations Planning
- Disaster Recovery Planning
- IT System and Data Backup and Restoration

3.2 Continuity of Operations Planning

3.2.1 Purpose

The COV Continuity of Operations Planning (COOP) requirements are outside of the scope of this *Standard*. This section addresses only the IT disaster recovery components of the COOP for IT systems and data. Agencies should consult the *Continuity of Operations Planning Manual* published by VDEM for COOP guidance.

These IT disaster recovery components of the COOP identify the steps necessary to provide continuity for essential agency IT systems and data.

3.2.2 Requirements

Each agency shall:

1. Designate an employee to collaborate with the agency Continuity of Operations Plan (COOP) coordinator as the focal point for IT aspects of COOP and related Disaster Recovery (DR) planning activities.

   Note: Designation of an agency COOP coordinator is included in the COOP planning requirements issued by VDEM.

2. Based on BIA and RA results, develop IT disaster components of the agency COOP which identifies:

   a. Each IT system that is necessary to recover essential business functions or dependent business functions and the Recovery Time Objective (RTO) and Recovery Point Objective (RPO) for each; and
   b. Personnel contact information and incident notification procedures.

   Note: If the COOP contains sensitive data, those components with sensitive data should be protected and stored at a secure off-site location.

3. Require an annual exercise (or more often as necessary) of IT DR components to assess their adequacy and effectiveness.

4. Require review and revision of IT DR components following the exercise (and at other times as necessary).

3.3 IT Disaster Recovery Planning Documentation

3.3.1 Purpose

IT Disaster Recovery Planning is the component of Continuity of Operations Planning that identifies the steps necessary to provide for restoring essential business functions on a schedule that support agency mission requirements. These steps lead to the creation of an IT Disaster Recovery Plan (DRP).

3.3.2 Requirements

Each agency shall:

1. Based on the COOP, develop and maintain an IT DRP, which supports the restoration of essential business functions and dependent business functions.

2. Require approval of the IT DRP by the Agency Head.

3. Require periodic review, reassessment, testing, and revision of the IT DRP to reflect changes in essential business functions, services, IT system hardware and software, and personnel.

4. Establish communication methods to support IT system users' local and remote access to IT systems, as necessary.

3.4 IT System and Data Backup and Restoration

3.4.1 Purpose

IT System and Data Backup and Restoration requirements identify the steps necessary to protect the availability and integrity of COV data documented in backup and restoration plans.

3.4.2 Requirements

For every IT system identified as sensitive relative to availability, each agency shall or shall require that its service provider implement backup and restoration plans to support restoration of systems, data and applications in accordance with agency requirements. At a minimum, these plans shall address the following:

1. Secure off-site storage for backup media.
2. Store off-site backup media in an off-site location that is geographically separate and distinct from the primary location.
3. Performance of backups only by authorized personnel.

4. Review of backup logs after the completion of each backup job to verify successful completion.

5. Approval of backup schedules of a system by the System Owner.

6. Approval of emergency backup and operations restoration plans by the System Owner.

7. Protection of any backup media that is sent off-site (physically or electronically), or shipped by the United States Postal Service or any commercial carrier, in accordance with agency requirements.

8. Authorization and logging of deposits and withdrawals of all media that is stored off-site.

9. Retention of the data handled by an IT system in accordance with the agency's records retention policy.

10. Management of electronic information in such a way that it can be produced in a timely and complete manner when necessary, such as during a legal discovery proceeding.

11. Document and exercise a strategy for testing that IT system and data backups are functioning as expected and the data is present in a usable form.

12. For systems that are sensitive relative to availability, document and exercise a strategy for testing disaster recovery procedures, in accordance with the agency's Continuity of Operations Plan.

4. Information Systems Security

4.1. Purpose

Information Systems Security requirements delineate steps to protect information systems in the following areas:

- IT System Security Plans
- IT System Hardening
- IT Systems Interoperability Security
- Malicious Code Protection
- Systems Development Life Cycle Security
- Application Security
- Wireless Security

4.2. IT System Security Plans

4.2.1 Purpose

IT System Security Plans document the security controls required to demonstrate adequate protection of information systems against security risks.

4.2.2 Requirements

Each System Owner of a sensitive IT system shall:

1. Document an IT System Security Plan for the IT system based on the results of the risk assessment. This documentation shall include a description of:

   a. All existing and planned security controls for the IT system, including a schedule for implementing planned controls;
   b. How these controls provide adequate mitigation of risks to which the IT system is subject.

2. Submit the IT System Security Plan to the Agency Head or designated ISO for approval.

3. Plan, document and implement additional security controls for the IT system if the Agency Head or designated ISO disapproves the IT System Security Plan, and resubmit the IT System Security Plan to the Agency Head or designated ISO for approval.

4. Update the IT System Security Plan every three years, or more often if necessary (i.e., due to material change), and resubmit the IT System Security Plan to the Agency Head or designated ISO for approval.

4.3. IT System Hardening

4.3.1 Purpose

IT System Hardening requirements delineate technical security controls to protect IT systems against security vulnerabilities.

4.3.2 Requirements

Each agency shall or shall require that its service provider:

1. Identify, document, and apply appropriate baseline security configurations to all agency IT systems, regardless of their sensitivity.
2. Identify, document, and apply more restrictive security configurations for sensitive agency IT systems, as necessary.

   Note: Agencies may develop agency-specific baseline security configuration standards or may elect to use baseline security configuration standards that are publicly available, such as those developed by the Center for Internet Security (www.cisecurity.org).
3. Maintain records that document the application of baseline security configurations.
4. Monitor systems for security baselines and policy compliance.
5. Review and revise all security configuration standards annually, or more frequently, as needed.

   Note: Agencies should establish a process to review applicable security notifications issued by equipment manufacturers, bulletin boards, security-related web sites, and other security venues, and establish a process to update security baseline configuration standards based on those notifications.
6. Reapply all security configurations to agency IT systems, as appropriate, when the IT system undergoes a material change, such as an operating system upgrade.
7. Require periodic operating system level vulnerability scanning of sensitive IT systems in a frequency commensurate with sensitivity and risk, to assess whether security configurations are in place and if they are functioning effectively.
8. Modify individual IT system configurations or baseline security configuration standards, as appropriate, to improve their effectiveness based on the results of vulnerability scanning.
9. *Apply all software publisher security updates to the associated software products.*
10. *All security updates must be applied as soon as possible after appropriate testing, not to exceed 90 days for implementation.*
11. *Prohibit the use of software products that the software publisher has designated as End-of-Life (i.e., software publisher no longer provides security patches for the software product).*

4.4. IT Systems Interoperability Security

4.4.1 Purpose

IT System Interoperability Security requirements identify steps to protect data shared with other IT systems.

4.4.2 Requirements

For every sensitive agency IT system that shares data with non-Commonwealth entities, the agency shall require or shall specify that its service provider require:

Note: Best practice dictates that Interoperability Agreements should be in place for sensitive IT system interoperability between Commonwealth agencies. However, this *Standard* currently only requires agreements between Commonwealth and non-Commonwealth entities.

1. The System Owner, in consultation with the Data Owner, shall document IT systems with which data is shared. This documentation must include:

   a. The types of shared data;
   b. The direction(s) of data flow; and
   c. Contact information for the organization that owns the IT system with which data is shared, including the System Owner, the Information Security Officer (ISO), or equivalent, and the System Administrator.

2. The System Owners of the IT systems which share data shall develop a written agreement that delineates security requirements for each interconnected IT system and for each type of data shared.

3. The System Owners of the IT systems that share data shall inform one another regarding other IT systems with which their IT systems interconnect or share data, and shall inform one another prior to establishing any additional interconnections or data sharing.

4. The written agreement shall specify if and how the shared data will be stored on each IT system.

5. The written agreement shall specify that System Owners of the IT systems that share data acknowledge and agree to abide by any legal requirements (i.e., HIPAA) regarding handling, protection, and disclosure of the shared data, *including but not limited to Data Breach requirements in this Standard.*

6. The written agreement shall specify each Data Owner's authority to approve access to the shared data.

7. The System Owners shall approve and enforce the agreement.

4.5. Malicious Code Protection

4.5.1 Purpose

Malicious Code Protection requirements identify controls to protect IT systems from damage caused by malicious code.

4.5.2 Requirements

Each agency shall, or shall require that its service provider:

1. Prohibit all IT system users from intentionally developing or experimenting with malicious programs (e.g., viruses, worms, spy-ware, keystroke loggers, phishing software, Trojan horses, etc.).

2. Prohibit all IT system users from knowingly propagating malicious programs including opening attachments from unknown sources.

3. Provide malicious program detection, protection, eradication, logging, and reporting capabilities.

4. Provide malicious code protection mechanisms via multiple IT systems and for all IT system users preferably deploying malicious code detection products from multiple vendors on various platforms.

   Example: An agency may elect to provide protection against malicious code transmitted via email on the email servers and on the desktop.

5. Provide protection against malicious programs through the use of mechanisms that:

   a. Eliminates or quarantines malicious programs that it detects;
   b. Provides an alert notification;
   c. Automatically and periodically runs scans on memory and storage devices;
   d. Automatically scans all files retrieved through a network connection, modem connection, or from an input storage device;
   e. Allows only authorized personnel to modify program settings; and
   f. Maintains a log of protection activities.

6. Provide the ability to eliminate or quarantine malicious programs in email messages and file attachments as they attempt to enter the agency's email system.

7. Provide the ability for automatic download of definition files for malicious code protection programs whenever new files become available, and propagate the new files to all devices protected by the malicious code protection program.

8. Require all forms of malicious code protection to start automatically upon system boot.

9. Provide network designs that allow malicious code to be detected and removed or quarantined before it can enter and infect a production device.

10. Provide procedures that instruct administrators and IT system users on how to respond to malicious program attacks, including shutdown, restoration, notification, and reporting requirements.

11. Require use of only new media (e.g., diskettes, CD-ROM) or sanitized media for making copies of software for distribution.

12. Prohibit the use of common use workstations and desktops (e.g., training rooms) to create distribution media.

13. By written policy, prohibit the installation of software on agency IT systems until the software is approved by the Information Security Officer (ISO) or designee and, where practicable, enforce this prohibition using automated software controls, such as Active Directory security policies.

14. Establish Operating System (OS) update schedules commensurate with sensitivity and risk.

4.6. Systems Development Life Cycle Security

4.6.1 Purpose

Systems Development Life Cycle (SDLC) Security requirements document the security-related activities that must occur in each phase of the development life cycle (from project definition through disposal) for agency IT application systems.

4.6.2 Requirements

Each agency shall:

1. Incorporate security requirements in each phase of the life cycle, as well as for each modification proposed for the IT application system in each stage of its life cycle.

Project Initiation

2. Perform an initial risk analysis based on the known requirements and the business objectives to provide high-level security guidelines for the system developers.

3. Classify the types of data (see *IT System and Data Sensitivity Classification*) that the system will process and the sensitivity of the proposed IT system.

4. Assess the need for collection and maintenance of sensitive data before incorporating such collection and maintenance in IT system requirements.

5. Develop an initial IT System Security Plan (see *IT System Security Plans*) that documents the security controls that the system will enforce to provide adequate protection against security risks.

Project Definition

6. Identify, develop, and document security requirements for the system during the Project Definition phase.

7. Incorporate security requirements in IT system design specifications.

8. Verify that the system development process designs, develops, and implements security controls that meet information security requirements in the design specifications.

9. Update the initial IT System Security Plan to document the security controls included in the design of the system to provide adequate protection against security risks.

10. Develop evaluation procedures to validate that security controls developed for a new system are working properly and are effective.

    Note: Some security controls (primarily those controls of a non-technical nature) cannot be tested and evaluated until after deployment of the system.

Implementation

11. Execute the evaluation procedures to validate and verify that the functionality described in the specification is included in the product.

    Note: Results should be documented in a report, including identification of controls that did not meet design specifications.

12. Conduct a Risk Assessment (see *Risk Assessment*) to assess the risk level of the system.

13. Require that the system comply with all relevant Risk Management requirements in this *Standard*.

14. Update the IT System Security Plan to document the security controls included in the system as implemented to provide adequate protection against information security risks, and comply with the other requirements (see *IT System Security Plans*) of this document.

Disposition

15. Require retention of the data handled by a system takes place in accordance with the agency's records retention policy prior to disposing of the system.

16. Require that electronic media is sanitized prior to disposal, as documented (see *Data Storage Media Protection*), so that all data is removed from the system.

17. Verify the disposal of hardware and software in accordance with the current version of the *Removal of Commonwealth Data from Surplus Computer Hard Drives and Electronic Media Standard* (COV ITRM Standard SEC514).

4.7. Application Security

4.7.1 Purpose

Application security requirements define the high-level specifications for securely developing and deploying Commonwealth applications.

4.7.2 Requirements

Each agency ISO is accountable for ensuring the following steps are documented and followed:

Application Planning

1. Data Classification - Data used, processed or stored by the proposed application shall be classified according to the sensitivity of the data.

2. Risk Assessment – If the data classification identifies the system as sensitive, a risk assessment shall be conducted before development begins and after planning is complete.

3. Security Requirements – Identify and document the security requirements of the application early in the development lifecycle. For a sensitive system, this shall be done after a risk assessment is completed and before development begins.

4. Security Design – Use the results of the Data Classification process to assess and finalize any encryption, authentication, access control, and logging requirements. When planning to use, process or store sensitive information in an application, agencies must address the following design criteria:

    a. Encrypted communication channels shall be established for the transmission of sensitive information;
    b. Sensitive information shall not be visibly transmitted between the client and the application; and
    c. Sensitive information shall not be stored in hidden fields that are part of the application interface.

Application Development

The following requirements represent a minimal set of coding practices, which shall be applied to all applications under development.

5. Authentication – Application-based authentication and authorization shall be performed for access to data that is available through the application but is not considered publicly accessible.

6. Session Management - Any user sessions created by an application shall support an automatic inactivity timeout function.

7. Data storage shall be separated either logically or physically, from the application interface (i.e., design two or three tier architectures where possible).

8. Agencies shall not use or store sensitive data in non-production environments *(i.e., a development or test environment that does not have security controls equivalent to the production environment)*.

9. Input Validation – All application input shall be validated irrespective of source. Input validation should always consider both expected and unexpected input, and not block input based on arbitrary criteria.

10. Default Deny – Application access control shall implement a default deny policy, with access explicitly granted.

11. Principle of Least Privilege – All processing shall be performed with the least set of privileges required.

12. Quality Assurance – Internal testing shall include at least one of the following: penetration testing, fuzz testing, or a source code auditing technique. Third party source code auditing and/or penetration testing should be conducted commensurate with sensitivity and risk.

    Note: Source code auditing techniques include, but are not limited to:

    a. Manual code review can identify vulnerabilities as well as functional flaws, but most agencies do not have the skilled security resources or time available within the software life cycle that a manual code review requires, and therefore, many agencies who decide to perform manual code reviews can only analyze a small portion of their applications;
    b. Application penetration testing tries to identify vulnerabilities in software by launching as many known attack techniques as possible on likely access points in an attempt to bring down the application or the entire system; and
    c. Automated source code analysis tools make the process of manual code review more efficient, affordable, and achievable. This technique of code audit results in significant reduction of analysis time, actionable metrics, significant cost savings, and can be integrated into all points of the development life cycle.

13. Configure applications to clear the cached data and temporary files upon exit of the application or logoff of the system.

Production and Maintenance

14. Production applications shall be hosted on servers compliant with the Commonwealth Security requirements for IT system hardening.

15. Internet-facing applications classified as sensitive shall have periodic vulnerability scans run against the applications and supporting server infrastructure, and always when any significant change to the environment or application has been made. Any remotely exploitable vulnerability shall be remediated immediately. Other vulnerabilities should be remediated without undue delay.

Note: It is strongly recommended that agencies adopt application vulnerability scanning and remediation for all internal sensitive applications as well.

Note: The Code of Virginia § 2.2-3803 (B) requires every public body in the COV that has an Internet web site to develop an Internet privacy policy and an Internet privacy policy statement that explains the policy to the public and is consistent with the requirements of the Code and is displayed on the public body's web site in a conspicuous manner.

4.8. Wireless Security

4.8.1. Purpose

Wireless security requirements define the high-level specifications for the secure deployment and use of wireless networking.

4.8.2. Requirements

Each agency ISO is accountable for ensuring the following steps are followed and documented:

Wireless LAN (WLAN) Connectivity on the COV Network

1. The following requirements shall be met in the deployment, configuration and administration of WLAN infrastructure connected to any internal Commonwealth of Virginia network.

   a. Client devices connecting to the WLAN must utilize two-factor authentication (i.e., digital certificates);
   b. WLAN infrastructure must authenticate *each* client device prior to permitting access to the WLAN;
   c. LAN user authorization infrastructure (i.e., Active Directory) must be used to authorize access to LAN resources;
   d. Only COV owned or leased equipment shall be granted access to an internal WLAN;
   e. All WLAN communications must utilize a secure encryption algorithm that provides an automated mechanism to change the encryption keys multiple times during the connected session and provide support for secure encryption protocols (i.e., the Counter Mode with Cipher Block Chaining Message Authentication Code Protocol encryption mechanism based on the Advanced Encryption Standard cipher);
   f. Physical or logical separation between WLAN and wired LAN segments must exist;
   g. All COV WLAN access and traffic must be monitored for malicious activity, and associated event log files stored on a centralized storage device;
   h. Configuration and security data associated with the WLAN must not be provided to unauthenticated devices. For example, SSID broadcasting will be disabled; and
   i. WLAN clients will only permit infrastructure mode communication.

WLAN Hotspot (Wireless Internet)

2. When building a wireless network, which will only provide unauthenticated access to the Internet, the following must be in place:

    a. WLAN Hotspots must have logical or physical separation from the agency's LAN;
    b. WLAN Hotspots must have packet filtering capabilities enabled to protect clients from malicious activity;
    c. All WLAN Hotspot access and traffic must be monitored for malicious activity, and log files stored on a centralized storage device; and
    d. Where COV clients are concerned, WLAN clients will only permit infrastructure mode communication.

Wireless Bridging

3. The following network configuration shall be used when bridging two wired LANs:

    a. All wireless bridge communications must utilize a secure encryption algorithm that provides an automated mechanism to change the encryption keys multiple times during the connected session and provide support for secure encryption methods (i.e., the Counter Mode with Cipher Block Chaining Message Authentication Code Protocol encryption mechanism based on the Advanced Encryption Standard cipher);
    b. Wireless bridging devices will not have a default gateway configured;
    c. Wireless bridging devices must be physically or logically separated from other networks;
    d. Wireless bridge devices must only permit traffic destined to traverse the bridge and should not directly communicate with any other network;
    e. Configuration and security data associated with the WLAN must not be provided to unauthenticated devices. For example, SSID broadcasting will be disabled; and
    f. Wireless bridging devices must not be configured for any other service than bridging (i.e., a wireless access point).

5. LOGICAL ACCESS CONTROL

5.1 Purpose

Logical Access Control requirements delineate the steps necessary to protect IT systems and data by verifying and validating that users are who they say they are and that they are permitted to use the IT systems and data they are attempting to access. Users are accountable for any activity on the system performed with the use of their account. This component of the COV Information Security Program defines requirements in the following three areas:

- Account Management
- Password Management
- Remote Access

5.2 Account Management

5.2.1. Purpose

Account Management requirements identify those steps necessary to formalize the process of requesting, granting, administering, and terminating accounts. Agencies should apply these Account Management practices to all accounts on IT systems, including accounts used by vendors and third parties.

The requirements below distinguish between internal and external IT systems. Internal IT systems are designed and intended for use only by COV employees, contractors, and business partners. External IT systems are designed and intended for use by agency customers and by members of the public. COV employees, contractors, and business partners may also use external IT systems.

5.2.2. Requirements

Each agency shall or shall require that its service provider document and implement account management practices for requesting, granting, administering, and terminating accounts. At a minimum, these practices shall include the following components:

Note: It is strongly recommended technical controls be implemented wherever possible to fulfill the following requirements, understanding that manual processes must sometimes be implemented to compensate for technical controls that might not be feasible.

<u>For all internal and external IT systems</u>

1. Grant IT system users' access to IT systems and data based on the principle of least privilege.

2. Define authentication and authorization requirements.

3. Establish policies and procedures for approving and terminating authorization to IT systems.

4. If the IT system is classified as sensitive, require requests for and approvals of emergency or temporary access that:

   a. Are documented according to standard practice and maintained on file;
   b. Include access attributes for the account;
   c. Are approved by the System Owner and communicated to the ISO; and
   d. Expire after a predetermined period, based on sensitivity and risk.

5. Based on risk, consider use of second-factor authentication, such as tokens and biometrics, for access to sensitive IT systems.

6. Review all user accounts *and corresponding privileges* for the user's continued need to access all IT systems.

7. Notify the System Administrator when IT system user accounts are no longer required, or when an IT system user's access level requirements change.

8. If the IT system is classified as sensitive, prohibit the use of guest accounts.

9. Prohibit the use of shared accounts on all IT systems. Those systems residing on a guest network are exempt from this requirement.

10. Prohibit the display of the last logon user ID on multi-user systems. Desktop and laptop systems assigned to a specific user are exempt from this requirement.

11. Lock an account automatically if it is not used for a predefined period.

    Note: Agencies should strongly consider locking accounts that go unused for 90 consecutive days.

12. Disable unneeded accounts.

13. Retain unneeded accounts in a disabled state in accordance with the agency's records retention policy.

14. Associate access levels with group membership, where practical, and require that every system user account be a member of at least one user group.

15. Require that the System Owner and the System Administrator investigate any unusual system access activities and approve changes to access level authorizations.

16. Require that System Administrators have both an administrative account and at least one user account and require that administrators use their administrative accounts only when performing tasks that require administrative privileges.

17. Prohibit the granting of local administrator rights to users. An Agency Head may grant exceptions to this requirement for those employees whose

documented job duties are primarily the development and/or support of IT applications and infrastructure. These exception approvals must be documented annually and include the Agency Head's explicit acceptance of defined residual risks.

18. Require that at least two individuals have administrative accounts to each IT system, to provide continuity of operations.

For all internal IT systems

19. Require a documented request to establish an account on any internal IT system.

20. Complete any agency-required background checks before establishing accounts, or as soon as practical thereafter.

21. Require confirmation of the account request and approval by the IT system user's supervisor and approval by the *Data* Owner or designee to establish accounts for all sensitive IT systems.

22. Require secure delivery of access credentials to the user based on information already on file.

23. Notify supervisors, Human Resources, and the System Administrator in a timely manner about termination, transfer of employees and contractors with access rights to internal IT systems and data.

24. Promptly remove access when no longer required.

For all external IT systems

25. Require secure delivery of access credentials to users of all external IT systems.

26. Require confirmation of the user's request for access credentials based on information already on file prior to delivery of the access credentials to users of all sensitive external IT systems.

27. Require delivery of access credentials to users of all sensitive external IT systems by means of an alternate channel (i.e., U.S. Mail).

For all service and hardware accounts

28. Document account management practices for all agency created service accounts, including, but not limited to granting, administering and terminating accounts. *If the service or hardware account is not used for interactive login with the system, the service or hardware account is exempt from the requirement to change the password at the interval defined in the Password Management section of this Standard.*

5.3 Password Management

5.3.1. Purpose

Password Management requirements specify the means for password use to protect IT systems and data.

5.3.2. Requirements

Each agency shall or shall require that its service provider document and implement password management practices. At a minimum, these practices shall include the following components:

1. Require the use of a non-shared and a unique password on each account on IT systems, including local, remote access and temporary accounts.

2. Require passwords *with a minimum of four characters on smart phones or PDAs accessing or containing COV data.*

3. Require password complexity:

   a. At least eight characters in length; and
   b. Utilize at least three of the following four:
      1) Special characters,
      2) Alphabetical characters,
      3) Numerical characters,
      4) Combination of upper case and lower case letters.

Note: It is considered best practice not to base passwords on a single dictionary word. It is strongly recommended that system users be educated not to base passwords on a single dictionary word.

4. Require that default passwords be changed immediately after installation.

5. Prohibit the transmission of identification and authentication data (e.g., passwords) without the use of industry accepted encryption standards (see *Encryption*).

6. Require IT system users to maintain exclusive control and use of their passwords, *and* protect them from inadvertent disclosure to others.

7. Configure all sensitive IT systems to allow users to change their password at most, once per 24-hour period.

8. Require users of all sensitive IT systems, to include network systems, to change their passwords after a period of 90 days. *An Agency sponsoring an Internet-facing system containing sensitive data provided by private citizens, which is accessed by only those citizens providing the stored data, may determine the appropriate validity period of the password, commensurate with sensitive and risk. The account holder must be provided with information on the importance of changing the account password on a regular and frequent basis.*

9. Require that IT system users immediately change their passwords and notify the ISO if they suspect their passwords have been compromised.

10. Configure all sensitive IT systems to maintain at least the last 24 passwords used in the password history files to prevent the reuse of the same or similar passwords. *An Agency sponsoring an Internet-facing system containing sensitive data provided by private citizens, which is accessed by only those citizens providing the stored data, may determine the appropriate number of passwords to be maintained in the password history file, commensurate with sensitive and risk. The account holder must be provided with information on the importance of changing the account password on a regular and frequent basis.*

Note: Reference CIS standards for Windows - http://www.cisecurity.org/tools2/windows/CIS_Win2003_DC_Benchmark_v2.0.pdf .

11. Provide a unique initial password for each new account of sensitive IT systems and require that the IT system user *change* the initial password upon the first login attempt. *An Agency sponsoring an Internet-facing system containing sensitive data provided by private citizens, which is accessed by only those citizens providing the stored data, may allow the citizen to continue to use the initial password so long as the Agency provides a mechanism to the citizen that allows the citizen to create a unique initial password.*

12. For sensitive IT systems, deliver the initial password to the IT system user in a secure and confidential manner.

13. Require that forgotten initial passwords be replaced rather than reissued.

14. Shared passwords shall not be used on any IT systems.

15. Prohibit the storage of passwords in clear text.

16. Limit access to files containing passwords to the IT system and its administrators.

17. Suppress the display of passwords on the screen as they are entered.

18. *Implement a screen saver lockout period after a maximum of 30 minutes of inactivity for COV devices*.

19. Require passwords to be set on device management user interfaces for all network-connected devices.

20. Document and store hardware passwords securely.

21. Implement procedures to handle lost or compromised passwords and/or tokens.

22. Set an account lockout threshold of not greater than 10 invalid attempts and the lockout duration for at least 15 minutes.

5.4 Remote Access

5.4.1. Purpose

Remote Access requirements identify the steps necessary to provide for the secure use of remote access to resources used by the COV.

5.4.2. Requirements

Each agency shall or shall require that its service provider:

1. Protect the security of all remote access to the agency's sensitive IT systems and data by means of encryption, in a manner consistent with Section 6.3.

   Note: This encryption requirement applies both to session initiation (i.e., identification and authentication) and to all exchanges containing sensitive data.

2. Protect the security of remote file transfer of sensitive data to and from agency IT systems by means of encryption, in a manner consistent with Section 6.3.

3. Document requirements for use of remote access and for remote access to sensitive data, based on agency and COV policies, standards, guidelines, and procedures.

4. Require that IT system users obtain authorization and a unique user ID and password prior to using the agency's remote access capabilities.

5. Document requirements for the physical and logical hardening of remote access devices.

6. Require maintenance of auditable records of all remote access.

7. Where supported by features of the system, session timeouts shall be implemented after a period of not longer than 30 minutes of inactivity and less, commensurate with sensitivity and risk. Where not supported by features of the system, mitigating controls must be implemented.

6. DATA PROTECTION

6.1 Purpose

Data Protection requirements delineate the steps necessary to protect COV data from improper or unauthorized disclosure. This component of the COV Information Security Program defines requirements in the following two areas:

- Data Storage Media Protection
- Encryption

6.2 Data Storage Media Protection

6.2.1. Purpose

Data Storage Media Protection requirements identify the steps necessary for the appropriate handling of stored data to protect the data from compromise.

6.2.2. Requirements

Each agency shall or shall require that its service provider document and implement Data Storage Media Protection practices. At a minimum, these practices must include the following components:

1. Define protection of stored sensitive data as the responsibility of the Data Owner.

2. Prohibit the storage of sensitive data on any non-network storage device or media, except for backup media, unless the data is encrypted and there is a written exception approved by the Agency Head accepting all residual risks. The exception shall include the following elements:

   a. The business or technical justification;
   b. The scope, including quantification and duration (not to exceed one year);
   c. A description of all associated risks;
   d. Identification of controls to mitigate the risks, one of which must be encryption; and
   e. Identification of any residual risks.

   Note: Non-network storage device or media, includes removable data storage media and the fixed disk drives of all desktops and mobile workstations, such as laptop and tablet computers, USB drives, CDs, etc.

3. Prohibit the storage of any Commonwealth data on *IT systems that are not under the contractual control of the Commonwealth of Virginia. The owner of the IT System must adhere to the latest Commonwealth of Virginia information security policies and standards as well as the latest Commonwealth of Virginia auditing policies and standards.*

4. Require logical and physical protection for all data storage media containing sensitive data, commensurate with sensitivity and risk.

5. Prohibit the connection of any non-COV owned *or leased* data storage media or device to a COV-owned *or leased* resource, unless connecting to a guest network or guest resources. This prohibition, at the agency's discretion need not apply to an approved vendor providing operational IT support services under contract.

   Note: Such media include, but are not limited to, USB drives, cell phones, personal digital assistants, desktops, laptops, and digital music players owned by employees, contractors, and students.

6. Prohibit the auto-forwarding of emails to external accounts to prevent data leakage unless there is a documented business case disclosing residual risk approved in writing by the Agency Head.

7. Restrict the pickup, receipt, transfer, and delivery of all data storage media containing sensitive data to authorized personnel.

8. Procedures must be implemented and documented to safeguard handling of all backup media containing sensitive data. Encryption of backup media shall be considered where the data is sensitive as related to confidentiality. Where encryption is not a viable option, mitigating controls and procedures must be implemented and documented.

9. Implement processes to sanitize data storage media prior to disposal or reuse.

   Note: Agencies and any service provider should implement procedures to instruct Administrators and users on the disposal of data storage media when no longer needed in accordance with the current version of the *Removal of Commonwealth Data from Surplus Computer Hard Drives and Electronic Media Standard* (COV ITRM Standard SEC514).

6.3 Encryption

6.3.1. Purpose

Encryption requirements provide a framework for selecting and implementing encryption controls to protect sensitive data. See the *Data Breach Notification* section for notification requirements regarding a breach of unencrypted sensitive data.

6.3.2. Requirements

Each agency or their service provider shall:

1. Define and document practices for selecting and deploying encryption technologies and for the encryption of data.

2. Document appropriate processes before implementing encryption. These processes must include the following components:

a. Instructions in the Security Incident Response Plan on how to respond when encryption keys are compromised;
b. A secure key management system for the administration and distribution of encryption keys; and
c. Requirements to generate all encryption keys through an approved encryption package and securely store the keys in the event of key loss due to unexpected circumstances.

3. Require encryption for the transmission of data that is sensitive relative to confidentiality or integrity over non-Commonwealth networks or any publicly accessible networks, or any transmission outside of the data's broadcast domain. *Digital* signatures may be utilized for data that is sensitive solely relative to integrity.

6.4 Protection of Sensitive Information on Non-Electronic Media

6.4.1. Purpose

This section outlines the best practice steps that should be taken to protect sensitive Commonwealth information that may be stored or transmitted on non-electronic media such as, the spoken word, paper documents, white or black boards, photographs, etc.

6.4.2. Recommended Best Practices

These recommendations apply to non-electronic media:

1. While in use, limit access based on a need to know basis by physically controlling access. For example, sensitive documents printed to a global printer should be retrieved without delay.

2. While not in use, store in a secure location with appropriate physical controls.

3. When no longer needed, securely destroy using appropriate destruction methods such as erasing white or black boards and shredding paper.

7. FACILITIES SECURITY

7.1 Purpose

Facilities Security requirements identify the steps necessary to safeguard the physical facilities that house IT equipment, systems, services, and personnel.

7.2 Requirements

Each agency shall or shall require that its service provider document and implement facilities security practices. At a minimum, these practices must include the following components:

1. Safeguard IT systems and data residing in static facilities (such as buildings), mobile facilities (such as computers mounted in vehicles), and portable facilities (such as mobile command centers).

2. Design safeguards, commensurate with risk, to protect against human, natural, and environmental threats.

3. Require appropriate environmental controls such as electric power, heating, fire suppression, humidity control, ventilation, air-conditioning and air purification, as required by the IT systems and data.

4. Protect against physical access by unauthorized personnel.

5. Control physical access to essential computer hardware, wiring, displays, and networks by the principle of least privilege.

6. Provide a system of monitoring and auditing physical access to sensitive IT systems.

7. Require that the ISO or designee periodically review the list of persons allowed physical access to sensitive IT systems.

8. PERSONNEL SECURITY

8.1 Purpose

Personnel Security requirements delineate the steps necessary to restrict access to IT systems and data to those individuals who require such access as part of their job duties. This component of the COV Information Security Program defines requirements in the following four areas:

- Access Determination and Control
- Information Security Awareness and Training
- Acceptable Use
- Email Communications

8.2 Access Determination and Control

8.2.1 Purpose

Access Determination and Control requirements identify the steps necessary to restrict access to IT systems and data to authorized individuals.

8.2.2 Requirements

Each agency shall or shall require that its service provider document and implement access determination and control practices for all sensitive agency IT systems and all third-party IT systems with which sensitive agency IT systems interconnect. At a minimum, these practices shall include the following components:

1. Perform background investigations of all internal IT System users based on access to sensitive IT systems or data. Existing users may be grandfathered under the policy and may not be required to have background investigations.

   Note: Agencies should consult the Code of Virginia § 2.2-1201.1 and Department of Human Resource Management (DHRM) Policy 2.10.

2. Restrict visitor access from facility areas that house sensitive IT systems or data.

3. Require non-disclosure and security agreements for access to IT systems and data, based on sensitivity and risk.

4. Remove physical and logical access rights upon personnel transfer or termination, or when requirements for access no longer exist, as required in Section 5.2 and Section 7.2.

5. Establish termination and transfer practices that require return of agency logical and physical assets that provide access to sensitive IT systems and data and the facilities that house them.

6. Temporarily disable physical and logical access rights when personnel do not need such access for a prolonged period in excess of 30 days because they are not working due to leave, disability or other authorized purpose.

7. Disable physical and logical access rights upon suspension of personnel for greater than 1 day for disciplinary purposes.

8. Establish separation of duties in order to protect sensitive IT systems and data, or establish compensating controls when constraints or limitations of the agency prohibit a complete separation of duties.

   Example: Such compensating controls may include increased supervisory review; reduced span of control; rotation of assignments; independent review, monitoring, and/or auditing; and timed and specific access authorization with audit review, among others.

9. Explicitly grant physical and logical access to sensitive IT systems and data and the facilities that house them based on the principle of least privilege.

8.3 Information Security Awareness and Training

8.3.1 Purpose

Security Awareness and Training requirements identify the steps necessary to provide IT system managers, administrators, and users with awareness of system security requirements and of their responsibilities to protect IT systems and data.

8.3.2 Requirements

Each agency ISO shall:

1. Include any agency-specific information security training requirements in the agency information security awareness and training program.

   Example: An agency that processes data covered by the Health Insurance Portability and Accountability Act (HIPAA) must have an information security awareness training program that addresses specific HIPAA data security requirements.

2. Require that all IT system users, including employees and contractors, receive information security awareness training annually, or more often as necessary. Generally, best practice is that annual security awareness training lasts at least one hour.

3. Require additional role-based information security training commensurate with the level of expertise required for those employees and contractors who manage, administer, operate, and design IT systems, as practicable and necessary.

   Example: Agency employees and contractors who are members of the Disaster Recovery Team or Security Incident Response Team require specialized training in these duties.

4. Implement processes to monitor and track completion of information security training.

5. Require information security training before (or as soon as practicable after) IT system users receive access rights to the agency's IT systems, and in order to maintain these access rights.

6. Develop an information security training program so that each IT system user is aware of and understands the following concepts:

   a. The agency's policy for protecting IT systems and data, with a particular emphasis on sensitive IT systems and data;
   b. The concept of separation of duties;
   c. Prevention and detection of information security incidents, including those caused by malicious code;
   d. Proper disposal of data storage media;
   e. Proper use of encryption;
   f. Access controls, including creating and changing passwords and the need to keep them confidential;

      Note: It is considered best practice not to base passwords on a single dictionary word. It is strongly recommended that system users be educated not to base passwords on a single dictionary word.

   g. Agency acceptable use policies;
   h. Agency Remote Access policies;
   i. Intellectual property rights, including software licensing and copyright issues;
   j. Responsibility for the security of COV data;
   k. Phishing; and
   l. Social engineering.

   Note: Over a period of *not more than two* years, security awareness training should include the concepts above based on the needs of the agency relative to the sensitivity of the agency's data and IT systems.

7. Require documentation of IT system users' acceptance of the agency's security policies after receiving information security training.

8.4 Acceptable Use

8.4.1 Purpose

Acceptable Use requirements identify the steps necessary to define acceptable and permitted use of IT systems.

8.4.2 Requirements

Each agency shall:

1. Document an agency acceptable use policy. Executive branch agencies must adhere to Virginia Department of Human Resource Management

(DHRM) *Policy 1.75 – Use of Internet and Electronic Communication Systems.* Each Executive branch agency shall supplement the policy as necessary to address specific agency needs.

Note: This policy can be found at http://www.dhrm.virginia.gov/hrpolicy/policy/pol1_75.pdf.

2. Direct the proper use of encryption for transmitting sensitive data.

3. Direct the use of an agency authorized COV warning banner to communicate that IT systems and their use may be monitored and viewed by authorized personnel; and there is no expectation of privacy when using a Commonwealth IT system.

4. Require acknowledgement that monitoring of IT systems and data may include, but is not limited to, network traffic; application and data access; keystrokes (only when required for security investigations and approved in writing by the Agency Head); and user commands; email and Internet usage; and message and data content.

5. Prohibit users from:

   a. Installing or using proprietary encryption hardware/software on Commonwealth systems;
   b. Tampering with security controls configured on COV workstations;
   c. Installing personal software on a Commonwealth system;
   d. Adding system hardware to, removing system hardware from, or modifying system hardware on a COV system; and
   e. Connecting non-COV devices to a COV IT system or network, such as personal computers, laptops or handheld devices, except in accordance with the current version of the *Use of Non-Commonwealth Computing Devices to Telework Standard* (COV ITRM Standard SEC511).

6. Prohibit the storage, use or transmission of copyrighted and licensed materials on COV systems unless the COV owns the materials or COV has otherwise complied with licensing and copyright laws governing the materials.

7. When connected to internal networks from COV guest networks or non-COV networks, data transmission shall only use full tunneling and not use split tunneling.

8. Require documentation of IT system users' acceptance of the agency's Acceptable Use Policy before, or as soon as practical after, gaining access to agency IT systems.

8.5 Email Communications

8.5.1 Purpose

Email shall not be used to send sensitive data unless encryption is used. As stated in the Encryption section of this S*tandard*, encryption may be required for the transmission of data that is sensitive relative to confidentiality and

integrity. The ISO should consider and plan for the issue of agency email being intercepted, incorrectly addressed, or infected with a virus. An email disclaimer is a set of statements that are either pre-pended or appended to emails. These statements are frequently used to create awareness of how to treat the data in the email. An email disclaimer is not a substitute for judgment on what content to put into an email.

8.5.2 Requirements

Each agency shall:

1. Require encryption for the transmission of email and attached data that is sensitive relative to confidentiality or integrity; however, digital signatures may be utilized for data that is sensitive solely relative to integrity as stated in the encryption component of this *Standard*. The ISO should consider and plan for the issue of agency email being intercepted, incorrectly addressed, or infected with a virus.

2. Consult with the agency's legal counsel before adopting an email disclaimer. Emails sent from Commonwealth systems are public records of the Commonwealth of Virginia and must be managed as such.

   The following text is an example of an email disclaimer for consideration when meeting with your agency's legal counsel.

   The information in this email and any attachments may be confidential and privileged. Access to this email by anyone other than the intended addressee is unauthorized. If you are not the intended recipient (or the employee or agent responsible for delivering this information to the intended recipient) please notify the sender by reply email and immediately delete this email and any copies from your computer and/or storage system. The sender does not authorize the use, distribution, disclosure or reproduction of this email (or any part of its contents) by anyone other than the intended recipient(s).

   No representation is made that this email and any attachments are free of viruses. Virus scanning is recommended and is the responsibility of the recipient.

9. THREAT MANAGEMENT

9.1 Purpose

Threat Management delineates the steps necessary to protect IT systems and data by preparing for and responding to information security incidents. This component area defines requirements for the following:

- Threat Detection
- Information Security Monitoring and Logging
- Information Security Incident Handling
- Data Breach Notification

9.2 Threat Detection

9.2.1 Purpose

Threat Detection requirements identify the practices for implementing intrusion detection and prevention.

9.2.2 Requirements

Each agency shall or shall require that its service provider document and implement threat detection practices that at a minimum include the following:

1. Designate an individual responsible for the agency's threat detection program, including planning, development, acquisition, implementation, testing, training, and maintenance.

2. Implement Intrusion Detection System (IDS) and Intrusion Prevention System (IPS).

3. Conduct IDS and IPS log reviews to detect new attack patterns as quickly as possible.

4. Develop and implement required mitigation measures based on the results of IDS and IPS log reviews.

5. Maintain regular communication with security research and coordination organizations, such as US CERT, to obtain information about new attack types, vulnerabilities, and mitigation measures.

6. *Provide quarterly summary reports of IDS and IPS events to Commonwealth Security.*

9.3 Information Security Monitoring and Logging

9.3.1 Purpose

Information Security Monitoring and Logging requirements identify the steps necessary to monitor and record IT system activity.

9.3.2 Requirements

Each agency shall, or shall require that its service provider, document and implement information security monitoring and logging practices that include the following components, at a minimum:

1. Designate individuals responsible for the development and implementation of information security logging capabilities, as well as detailed procedures for reviewing and administering the logs.

2. Enable event logging on all IT systems. At a minimum, logs will include:
   a. The event;
   b. The user ID associated with the event; and
   c. The time the event occurred

   Note: Examples of events might include logons, invalid access attempts or data deleted, changed or added.

3. Routinely monitor IT system event logs, correlate information with other automated tools, identify suspicious activities, and provide alert notifications.

4. Document standards that specify the type of actions an IT system should take when a suspicious or apparent malicious activity is taking place.

   Example: Possible actions include stopping the event, shutting down the IT system, and alerting appropriate staff.

   Note: Multiple actions may be warranted and advisable, based on sensitivity and risk.

5. Prohibit the installation or use of unauthorized monitoring devices.

6. Prohibit the use of keystroke logging, except when required for security investigations and a documented business case outlining the need and residual risk has been approved in writing by the Agency Head.

   Note: For investigative purposes, the CISO or ISO has the responsibility to authorize monitoring or scanning activities for network traffic; application and information access; user commands; email and Internet usage; and message and information content for IT systems and data.

9.4 Information Security Incident Handling

9.4.1 Purpose

Information Security Incident Handling requirements identify the steps necessary to respond to suspected or known breaches to information security safeguards.

9.4.2 Requirements

Each agency shall document information security incident handling practices and where appropriate the agency shall incorporate its service provider's procedures for incident handling practices that include the following, at a minimum:

1. Designate an Information Security Incident Response Team that includes personnel with appropriate expertise for responding to cyber attacks.

2. Identify controls to deter and defend against cyber attacks to best minimize loss or theft of information and disruption of services.

3. Implement proactive measures to defend against new forms of cyber attacks and zero-day exploits.

4. Establish information security incident categorization and prioritization based on the immediate and potential adverse effect of the information security incident and the sensitivity of affected IT systems and data.

5. Identify immediate mitigation procedures, including specific instructions, based on information security incident categorization level, on whether or not to shut down or disconnect affected IT systems.

6. Establish a process for reporting information security incidents to the CISO. All COV agencies are encouraged to report security incidents; however, Executive branch agencies must establish a reporting process for information security incidents in accordance with §2.2-603(F) of the Code of Virginia so as to report "*to the Chief Information Officer within 24 hours from when the department discovered or should have discovered their occurrence*," "*all known incidents that threaten the security of the Commonwealth's databases and data communications resulting in exposure of data protected by federal or state laws, or other incidents compromising the security of the Commonwealth's information technology systems with the potential to cause major disruption to normal agency activities.*"

7. Establish requirements for internal agency information security incident recording and reporting requirements, including a template for the incident report.

8. Establish procedures for information security incident investigation, preservation of evidence, and forensic analysis.

9. Report information security incidents only through channels that have not been compromised.

   Note: The CISO, in conjunction with the Agency Head through the agency ISO or other Administration authorities as necessitated by circumstances, may authorize the confiscation and removal of any IT resource suspected to be the object of inappropriate use or violation of laws, regulations, policies or standards in order to preserve evidence that might be utilized in forensic analysis of a security incident.

9.5 Data Breach Notification

9.5.1 Purpose

To specify the notification requirements for agencies by identifying the triggering factors and necessary responses to unauthorized release of unencrypted sensitive information.

9.5.2 Requirements

All of the following are industry best practices. Where electronic records or IT infrastructure are involved, the following are requirements that each agency shall adhere to. Based on their business requirements, some agencies may need to comply with regulatory and/or industry requirements that are more restrictive. Where non-electronic records are involved or implied, the following are advisory in nature, but are strongly recommended:

Each agency shall:

1. Identify and document all agency systems, processes, and logical or physical data storage locations (whether held by the agency or a third party) that contain personal information *or medical information*.
   a. Personal information means the first name or first initial and last name in combination with and linked to any one or more of the following data elements *that relate to a resident of the Commonwealth*, when the data elements are neither encrypted nor redacted:
      1) Social security number;
      2) Drivers license number or state identification card number issued in lieu of a driver's license number; or
      3) Financial account number, or credit card or debit card number, in combination with any required security code, access code, or password that would permit access to a resident's financial accounts;
   b. *Medical information means the first name or first initial and last name in combination with and linked to any one or more of the following data elements that relate to a resident of the Commonwealth, when the data elements are neither encrypted nor redacted*:
      1) *Any information regarding an individual's medical or mental health history, mental or physical condition, or medical treatment or diagnosis by a health care professional*; or
      2) An individual's health insurance policy number or subscriber identification number, any unique identifier used by a health insurer to identify the individual, or any information in an individual's application and claims history, including any appeals records.

2. "Redact" *for personal information* means alteration or truncation of data such that no more than the following are accessible as part of the personal information:
   a. Five digits of a social security number; or
   b. The last four digits of a driver's license number, state identification card number, or account number.

3. "*Redact" for medical information means alteration or truncation of data such that no information regarding the following are accessible as part of the medical information:*
   a. *An individual's medical history; or*
   b. *Mental or physical condition; or*
   c. *Medical treatment or diagnosis; or*
   d. *No more than four digits of a health insurance policy number, subscriber number; or*
   e. *Other unique identifier.*

   Note: The terms *for personal information or medical information* do not include information that is lawfully obtained from publicly available information, or from federal, state, or local government records lawfully made available to the general public.

4. Include provisions in any third party contracts requiring that the third party and third party subcontractors:
   a. Provide immediate notification to the agency of suspected breaches; and
   b. Allow the agency to both participate in the investigation of incidents and exercise control over decisions regarding external reporting.

5. Provide appropriate notice to affected individuals upon the unauthorized release of unencrypted and/or un-redacted personal information *or medical information* by any mechanism, including, but not limited to:
   a. Theft or loss of digital media including laptops, desktops, tablets, CD's, DVD's, tapes, USB drives, SD cards, etc.;
   b. Theft or loss of physical hardcopy; and
   c. Security compromise of any system *containing personal or medical information (i.e., social security numbers, credit card numbers, medical records, insurance policy numbers, laboratory findings, pharmaceutical regimens, medical or mental diagnosis, medical claims history, medical appeals records, etc.).*

   An individual or entity shall disclose the breach of the security of the system if encrypted information is accessed and acquired in an unencrypted form, or if the security breach involves a person with access to the encryption key.

   If a Data Custodian is the entity involved in the data breach, they must alert the Data Owner so that the Data Owner can notify the affected individuals.

   The agency shall provide this notice without undue delay as soon as verification of the unauthorized release is confirmed, except as delineated in #9, below.

6. In the case of a computer found to be infected with malware that exposes data to unauthorized access, individuals that may have had their personal *or medical information* exposed due to use of that computer must be alerted in accordance with data breach rules. Agencies shall notify the CISO when notification of affected individuals has been completed.

7. Provide notification that consists of:
   a. A general description of what occurred and when;

b. The type of personal or medical information that was involved;
c. What actions have been taken to protect the individual's information from further unauthorized access;
d. A telephone number that the person may call for further information and assistance, if one exists; and
e. What actions the agency recommends that the individual take. The actions recommended should include monitoring account statements (i.e., *credit report*, medical insurance Explanation of Benefits (EOB), etc.).

8. Provide this notification by one or more of the following methodologies, listed in order of preference:
   a. Written notice to the last known postal address in the records of the individual or entity;
   b. Telephone notice;
   c. Electronic notice; or
   d. Substitute notice - if the individual or the entity required to provide notice demonstrates that the cost of providing notice will exceed $50,000, the affected class of Virginia residents to be notified exceeds 100,000 residents, or the individual or the entity does not have sufficient contact information or legal consent to provide notice. Substitute notice consists of all of the following:
      1) Email notice if the individual or the entity has email addresses for the members of the affected class of residents;
      2) Conspicuous posting of the notice on the web site of the individual or the entity if the individual or the entity maintains a web site; and
      3) Notice to major statewide media.

9. Hold the release of notification immediately following verification of unauthorized data disclosure only if law-enforcement is notified and the law-enforcement agency determines and advises the individual or entity that the notice would impede a criminal or civil investigation, or homeland security or national security. Notice shall be made without unreasonable delay after the law-enforcement agency determines that the notification will no longer impede the investigation or jeopardize national or homeland security.

10. IT ASSET MANAGEMENT

10.1 Purpose

IT Asset Management delineates the steps necessary to protect IT systems and data by managing the IT assets themselves in a planned, organized, and secure fashion. This component area defines requirements for the following:

- IT Asset Control
- Software License Management
- Configuration Management and Change Control

10.2 IT Asset Control

10.2.1 Purpose

IT Asset Control requirements identify the steps necessary to control and collect information about IT assets.

10.2.2 Requirements

Commensurate with sensitivity and risk, each agency shall or shall require that its service provider document and implement inventory management practices that address the following components, at a minimum:

1. Identify whether IT assets may be removed from premises that house IT systems and data, and if so, identify the controls over such removal.

2. Identify whether personal IT assets are allowed onto premises that house IT systems and data, and if so, identify the controls necessary to protect these IT systems and data.

3. Remove data from IT assets prior to disposal in accordance with the current version of the *Removal of Commonwealth Data from Surplus Computer Hard Drives and Electronic Media Standard* (COV ITRM Standard SEC514).

4. Require creation and periodic review of a list of agency hardware and software assets.

10.3. Software License Management

10.3.1. Purpose

Software License Management requirements identify the steps necessary to protect against use of computer software in violation of applicable laws.

10.3.2. Requirements

Each agency shall or shall require that its service provider document and implement software license management practices that address the following components, at a minimum:

1. Require the use of only agency approved software and service provider approved systems management software on IT systems.

2. Assess periodically whether all software is used in accordance with license agreements.

10.4. Configuration Management and Change Control

10.4.1. Purpose

Configuration Management and Change Control requirements identify the steps necessary to document and monitor the configuration of IT systems, and to control changes to these items during their life cycles. While the full extent of Configuration Management and Change Control is beyond the scope of this document, agencies are advised to institute structured practices in this area, based on industry standard frameworks such as the IT Infrastructure Library (ITIL) (www.itil.co.uk) or Control Objectives for Information and related Technology (COBIT) (www.isaca.org), among others.

10.4.2. Requirements

Each agency shall, or shall require that its service provider, document and implement configuration management and change control practices so that changes to the IT environment do not compromise security controls.

This page intentionally left blank

GLOSSARY OF SECURITY DEFINITIONS

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

INFORMATION SECURITY ACRONYMS

AITR: Agency Information Technology Representative

BIA: Business Impact Analysis

CAP: Corrective Action Plan

CIO: Chief Information Officer

CISO: Chief Information Security Officer

COOP: Continuity of Operations Plan

DHRM: Department of Human Resource Management

DRP: Disaster Recovery Plan

ESG: Enterprise Solutions and Governance

FTP: File Transfer Protocol

HIPAA: Health Insurance Portability and Accountability Act

IDS: Intrusion Detection Systems

IPS: Intrusion Prevention Systems

ISO: Information Security Officer

ISO/IEC: International Organization for Standardization/

International Electrotechnical Commission

ITRM: Information Technology Resource Management

MOU: Memorandum of Understanding

PCI: Payment Card Industry

PDA: Personal Digital Assistant

PI: Personal Information

PIN: Personal Identification Number

RA: Risk Assessment

RPO: Recovery Point Objective

RTO: Recovery Time Objective

SDLC: Systems Development Life Cycle

Solutions Directorate (VITA)

SSID: Service Set Identifier

SSP: Security Program Plan

VDEM: Virginia Department of Emergency Management

VITA: Virginia Information Technologies Agency

APPENDIX – INFORMATION SECURITY POLICY AND STANDARD EXCEPTION REQUEST FORM

The form an Agency must submit to request an exception to any requirement of this *Standard* and the related *Information Security Policy* is on the following page.

COV Information Security Policy & Standard Exception Request Form

Agency Name: _____Contact for Additional Information: _____

Policy/Standard requirement to which an exception is requested:_____

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

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

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

3. Describe all associated risks:

4. Identify the controls to mitigate the risks:

5. Identify all residual risks:

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

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

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

Approved_____ Denied_____ Comments:

_____ _____
CISO Date

Agency Request for Appeal Use Only

Approved_____ Comments:

_____ _____
Agency Head Date

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

Appeal Approved_____ Appeal Denied_____ Comments:

_____ _____
CIO Date