Policy and Procedure 9-17
Information Security: System and Services Acquisition

Issued By:	Robert W. Farrell, State Forester	DocuSigned by: Robert W. Farrell 2115C3D38FCF4E7... 7/9/2024
Effective Date:	July 8, 2024	
Codes/Mandates:	Code of Virginia, §2.2-2005 Creation of Agency; appointment of Chief Information Officer Code of Virginia: §2.2-2007 Powers of the CIO	
References:	Commonwealth Information Technology Resource Management (ITRM) Information Security Policy SEC 519-00, Commonwealth ITRM Standard SEC502: Audit Security Standard Commonwealth ITRM Standard SEC530: Information Security Standard	
Forms:	N/A	

CONTENTS

PURPOSE 1
SCOPE 2
DEFINITIONS and ACRONYMS 2
BACKGROUND 2
ROLES & RESPONSIBILITY 2
STATEMENT OF POLICY 3
Allocation of Resources (SA-2) 3
System Development Life Cycle (SA-3) 4
Acquisition Process (SA-4) 6
System Documentation (SA-5) 7
Software Usage Restrictions (SA-6-COV) 8
Security and Privacy Engineering Principles (SA-8) 8
External System Services (SA-9) 9
Developer Configuration Management (SA-10) 11
Developer Testing and Evaluation (SA-11) 12
Development Process, Standards and Tools (SA-15) 13
Developer-Provided Training (SA-16) 13
Developer Security and Privacy Architecture Design (SA-17) 13
Unsupported System Components (SA-22) 14
AUTHORITY 14
INTERPRETATION 14
APPROVAL 14
VERSION HISTORY 14

PURPOSE

The purpose of this policy and procedure is to create a prescriptive set of process and procedures, aligned with applicable COV IT security policy and standards, to ensure that Department of Forestry develops, disseminates, and updates the Information System: System and Services Acquisition Policy and Procedure. This policy and procedure establishes the minimum requirements for this policy and procedure.

This policy is intended to meet the control requirements outlined in SEC530, Section 8.15 IT System and Services Acquisition Family, controls SA-1 through SA-22 as well as additional Commonwealth of Virginia controls.

SCOPE

All Department of Forestry employees (classified, hourly, or business partners) as well as all Department of Forestry systems.

DEFINITIONS and ACRONYMS

"Agency" and **"DOF"** means the Virginia Department of Forestry.

"Data owner" means the agency manager or supervisor, designated by the state forester, who defines, manages and controls the use of data and ensures compliance with adopted standards.

"Information security officer" and **"ISO"** means the agency employee who is designated by the state forester to develop and manage the agency's information security program, as required in the Commonwealth's Information Security Standard, SEC530.

"System administrator" means the agency employee who implements, manages, and/or operates a system at the direction of the system owner or data owner.

"System owner" means the agency manager or supervisor who is responsible for the operation and oversight of any given agency business system.

ACRONYMS

CIO:	Chief Information Officer
COV:	Commonwealth of Virginia
CSRM:	Commonwealth Security and Risk Management
DOF:	Department of Forestry
ISO:	Information Security Officer
IT:	Information Technology
ITRM:	Information Technology Resource Management
SEC530:	Information Security Standard 530
SDLC:	System Development Life Cycle
VITA	Virginia Information Technology Agency

BACKGROUND

The Information Security: System and Services Acquisition Policy and Procedure at Department of Forestry is intended to facilitate the effective implementation of the processes necessary to meet the IT system and services acquisition requirements as stipulated by the COV ITRM Security Standard SEC530 and security best practices. This policy directs that Department of Forestry meet these requirements for all IT systems.

ROLES & RESPONSIBILITY

This section will provide summary of the roles and responsibility as described in the Statement of Process section. The following Roles and Responsibility Matrix describes 4 role specific activities:

- Responsible (R) – Person working on activity
- Accountable (A) – Person with decision authority and one who delegates the work
- Consulted (C) – Key stakeholder or subject matter expert who should be included in decision or work activity
- Informed (I) – Person who needs to know of decision or action

Roles	Data Owner	System Owner	System Admin/Developer	Information Security Officer
Tasks				
Include requirements in mission/business process planning.		A		R
Determine, document and allocate resources.		A		R
Manage the information system using SDLC.		A		R
Define and document security roles and responsibilities.		A		R
Identify individual role and responsibilities.		A		R
Follow application planning, development and support requirements.		A	R	R
Require system/security documentation.		R		A
Update system/security documentation.		A	R	R
Ensure that software and documentation are used in accordance with contract agreements.		A	R	R
Prohibit peer-to-peer file sharing technology.			R	I/R
Require service provider to document its software license management practices.				A/R
Enforce explicit rules governing the installation of software by users.				A/R
Require that security engineering principles be applied.			R	A
Require that providers of external services comply with DOF information security requirements.				A/R
Define and document government oversight and user roles and responsibilities for external services.				A/R
Monitor and mitigate risks that arise from external services.				A/R
Perform configuration management during information system design, development, implementation and operation.		A	R	R
Document approved changes.		A	R	R
Track security flaws and flaw resolution.		A	R	R
Create and implement a security test and evaluation plan.		A	R	R
Implement a flaw remediation process.		A	R	R
Document the results of the security testing and flaw remediation process.		A	R	R
Perform a vulnerability analysis.		A	R	R

STATEMENT OF POLICY

In accordance with SEC530, SA-1 through SA-22, Department of Forestry shall establish the minimum requirements for this policy and procedure.

Allocation of Resources (SA-2)

1. The IT director shall:
   a. Include a determination of high-level information security and privacy requirements for the information system in mission/business process planning.

b. Determine, document and allocate the resources required to protect the information system as part of its capital planning and investment control process.

c. Establish a discrete line item for information security and privacy in organizational programming and budgeting documentation.

System Development Life Cycle (SA-3)

1. The ISO or designee shall require that information systems follow the following processes:

   a. Acquire, develop and manage the system using system development life cycle methodology that incorporates information security and privacy considerations.

   b. Define and document information security and privacy roles and responsibilities throughout the system development life cycle.

   c. Identify individuals having information security and privacy roles and responsibilities.

   d. Integrate the organizational information security and privacy risk management process into system development life cycle activities.

   e. Protect system preproduction environments commensurate with risk throughout the system development life cycle for the system, system component or system service.

   f. Approve, document and control the use of live data in preproduction environments for the system, system component or system service.

   g. Protect preproduction environments for the system, system component or system service at the same impact or classification level as any live data in use within the preproduction environments.

   h. Plan for and implement a technology refresh schedule for the system throughout the system development life cycle.

2. The IT director is accountable for ensuring the following steps are documented and followed by system owners and system administrators:

   a. Manage the information system using a system development life cycle (SDLC) methodology that includes information security considerations, as follows:

      i. Project Initiation

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

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

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

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

      ii. Project Definition

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

         2. Incorporate IT security requirements in IT system design specifications.

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

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

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

iii. Implementation

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

2. Conduct a Risk Assessment (see Risk Assessment) to assess the risk level of the IT application system.

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

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

iv. Disposition

1. Require retention of the data handled by an IT system in accordance with the agency's records retention policy prior to disposing of the IT system.

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

3. 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).

v. Control gates or established points in the life cycle, must be used to determine whether the project should continue as is, change direction, or be discontinued.

vi. Key outputs, in the form of deliverables or artifacts, for common tasks must be generated.

1. Expected outputs must provide information vital to the system design.

b. Implement and document the following requirements:

i. 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 life cycle. 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.

c. Sensitive information shall not be stored in hidden fields that are part of the application interface.

ii. Application Development

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

1. 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.
2. Session Management - Any user sessions created by an application shall support an automatic inactivity timeout function.
3. Data storage shall be separated either logically or physically, from the application interface (i.e., design two or three tier architectures where possible).
4. Agencies shall not use or store sensitive data in non-production environments.
5. 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.
6. Default Deny – Application access control shall implement a default deny policy, with access explicitly granted.
7. Principle of Least Privilege – All processing shall be performed with the least set of privileges required.
8. 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.
9. Configure applications to clear the cached data and temporary files upon exit of the application or logoff of the system.

iv. Production and Maintenance

1. Production applications shall be hosted on servers compliant with the Commonwealth Security requirements for IT system hardening.
2. Internet-facing applications classified as sensitive shall have periodic (not to exceed 90 days) vulnerability scans run against the applications and supporting server infrastructure as well as anytime a 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.

Acquisition Process (SA-4)

1. The ISO or designee shall include the following requirements, descriptions and criteria, explicitly or by reference, in the acquisition contract for the system, system component or system service:
   a. Security and privacy functional requirements.
   b. Strength of mechanism requirements.
   c. Security and privacy assurance requirements.
   d. Controls needed to satisfy the security and privacy requirements.
   e. Security and privacy documentation requirements.
   f. Requirements for protecting security and privacy documentation.
   g. Description of the system development environment and environment in which the system is intended to operate.
   h. Allocation of responsibilities or identification of parties responsible for information security, privacy and supply chain risk management.
   i. Acceptance criteria.
2. Require the developer of the system, system component or system service to provide a description of the functional properties of the controls to be implemented.

3. Require the developer of the system, system component or system service to provide design and implementation information for the controls that includes security-relevant external system interfaces; high-level design; and design and implementation information at the appropriate level of detail.
4. Require the developer of the system, system component or system service to demonstrate the use of a system development life cycle that includes:
    a. Organization-defined systems engineering methods.
    b. Organization-defined systems and privacy engineering methods.
    c. Organization-defined software development methods; testing, evaluation, assessment, verification and validation methods, and quality control processes.
5. Require the developer of the system, system component or system service to:
    a. Deliver the system, component or service with the organization-defined security configurations implemented.
    b. Use the configurations as the default for any subsequent system, component or service reinstallation or upgrade.
    6. Require the developer of the system, system component or system service to produce a plan for the continuous monitoring of control effectiveness that is consistent with the continuous monitoring program of the organization.
    7. Require the developer of the system, system component or system service to identify the functions, ports, protocols and services intended for organizational use.
    8. Employs only information technology products on the FIPS 201-approved products list for Personal Identity Verification (PIV) capability implemented within organizational systems.
    9. Include COV data breach requirements in the acquisition contract for the operation of a system of records on behalf of an organization to accomplish an organizational mission or function.
    10. Include organizational data ownership requirements in the acquisition contract.
    11. Require all data to be removed from the contractor's system and returned to the organization within a maximum of 30 days.
    12. Limits the use of commercially provided information assurance (IA) and IA-enabled information technology products to those products that have been successfully evaluated against Commonwealth security processed and standards.
    13. Requires, if no Commonwealth approved Protection Profile exists for a specific technology type but a commercially provided information technology product relies on cryptographic functionality to enforce its security policy, that the cryptographic module is FIPS-validated.

System Documentation (SA-5)

1. The ISO or designee shall require information systems to have:
    a. Administrator documentation (i.e., whether published by a vendor/manufacturer or written in-house) for the information system and constituent components must be obtained, protected as required and made available to authorized personnel.
        i. Administrator documentation must include information that describes:
            1. Secure configuration, installation and operation of the information system.
            2. Effective use and maintenance of the system's security features/functions.
            3. Known vulnerabilities regarding configuration and use of administrative (i.e., privileged) functions.

b. User documentation (i.e., whether published by a vendor/manufacturer or written in- house) for the information system and constituent components must be obtained, protected as required and made available to authorized personnel.

   i. User documentation must include information that describes:

      1. User-accessible security features/functions and how to effectively use those security features/functions.

      2. Methods for user interaction with the information system, which enables individuals to use the system in a more secure manner.

      3. User responsibilities in maintaining the security of the information and information system.

c. When information system documentation is either unavailable or non- existent, the following actions must be taken:

   i. Document attempts to obtain such documentation.

   ii. Recreate selected information system documentation if such documentation is essential to the effective implementation and/or operation of security controls.

d. Distribute documentation to the appropriate organization-defined personnel.

Software Usage Restrictions (SA-6-COV)

1. DOF ISO shall require that its service provider document software license management practices that address the following components, at a minimum:

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

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

Security and Privacy Engineering Principles (SA-8)

1. The ISO or designee shall require that CSRM’s information system security and privacy engineering principles be applied in the specification, design, development, implementation and modification of the information system.

   a. The application of security engineering principles must be integrated into the SDLC.

   b. Security engineering principles are primarily targeted at information systems under new development and information systems undergoing major upgrades.

   c. For legacy information systems, security engineering principles must be applied to system upgrades and modifications, to the extent feasible, given the current states of the hardware, software and firmware components within the system.

2. Security engineering principles must include, but are not limited to:

   a. The use in organization-defined systems of the following principles:

      i. Clear abstractions

      ii. Least common mechanism

      iii. Modularity and layering

      iv. Partially ordered dependencies

      v. Efficiently mediated access

      vi. Minimized sharing

      vii. Reduced complexity

      viii. Secure evolvability

ix. Trusted components

x. Hierarchical trust in organization

xi. Inverse modification threshold

xii. Hierarchical protection

xiii. Minimized security elements

xiv. Least privilege

xv. Predicate permission

xvi. Self-reliant trustworthiness

xvii. Secure distributed composition

xviii. Trusted communications channels

xix. Continuous protection

xx. Secure metadata management

xxi. Partially ordered dependencies

xxii. Self-analysis

xxiii. Accountability and traceability

xxiv. Secure defaults

xxv. Secure failure and recovery

xxvi. Economic security

xxvii. Performance security

xxviii. Human factored security

xxix. Acceptable security

xxx. Repeatable and documented procedures

xxxi. Procedural rigor

xxxii. Secure system modification

xxxiii. Sufficient documentation

xxxiv. Minimization

External System Services (SA-9)

1. The ISO or designee shall:

   a. Require that providers of external information system services comply with organizational information security requirements and employ appropriate security controls in accordance with Virginia Information Technologies Agency’s specified controls.

   b. Define and document organizational oversight and user roles and responsibilities with regard to external information system services.

      i. Documents that solicit and implement external information system services must:

         1. Identify specific drivers for soliciting the services.

         2. Specify responsibilities for each security control or for specific activities within a control.

         3. Identify associated reporting requirements for each security control.

4. Require the provider of external information system services to conform to the same security control and documentation requirements as would apply to the Department of Forestry's internal systems.

ii. The following process, methods and techniques, defined by VITA, must be included in the procurement and monitoring of compliance of external information system services:

1. Conduct an organizational assessment of risk prior to the acquisition or outsourcing of information security services.
2. Verify that the acquisition or outsourcing of dedicated information security services is approved by the chief information security officer designee.
3. Require providers of the following external system services to identify the functions, ports, protocols and other services required for the use of such services: organization-defined external system services.
4. Establish, document and maintain trust relationships with external service providers based on CSRM requirements.
5. Verify that the interests of DOF external providers are consistent and reflect DOF interests including possible concerns as background checks for personnel, examining ownership records, employing trustworthy service providers.
6. Restrict the location of information processing; information or data; system services to locations within the Unites States of America based on the location of storing or processing of COV data.
7. Provide the capability to check the integrity of information while it resides in the external system.
8. Restrict the geographic location of information processing and data storage to facilities located within in the legal jurisdictional boundary of the United States.
9. Establish the exact geographically location of all data if not stored within the Commonwealth. The Commonwealth will define the parameters and costs for data location options prior to making any contractual commitments.
10. Confirm the exact geographically location of the sensitive data on at least a monthly basis and report the location to the appropriate regulatory authority at least every 90 days.
11. Establish a Data Escrow policy to address the data recovery process in case of system failure or facility issues and ensure all copies of data are returned to the Commonwealth at the end of contract.
12. Establish a validated copy of any data elements classified as sensitive with respect to integrity or availability or are considered components in a system of record for the Commonwealth. The validated copy must be stored within a secured environment maintained by the Commonwealth.
13. Perform an annual security audit of the environment or review the annual audit report of the environment conducted by an independent, third-party audit firm on an annual basis.
14. Perform at least a monthly review of activity logs related to the operation of the service. At a minimum, the activity review must include the access time and action of each individual using the system during the review period.
15. Receive reports from the vendor on vulnerability scans of the operating system and supporting software at least once every 90 days.
16. Ensure that the vendor conduct an independent vulnerability scan of the service at least once every 90 days and provide the results to the agency within 10 business days.
17. Submit a summary of all findings from the monthly activity log review once every 90 days to the appropriate regulatory authority.
18. Submit the vulnerability scan information within 30 days of receipt from the vendor to the appropriate regulatory authority.

19. Submit the results from the data owning agency vulnerability scan of the service within 30 days of scan completion.

iii. SLAs must:

1. Define expectations of performance for each required security control.
2. Describe measurable outcomes.
3. Specify remedies and response requirements for any identified instance of non-compliance.

iv. A chain of trust or level of confidence must be established with external service providers to ensure adequate protection of services rendered.

1. Risks must be assessed in the risk assessment process.
2. Risks must be documented.
3. The extent and nature of the chain of trust varies based on the relationship between DOF and the external provider.

a. Where a sufficient level of trust cannot be established in the external services and/or service providers, the organization employs compensating security controls or accepts the greater degree of risk.

c. Mitigate any risks that arise from the use of external information system services.

d. Monitor security control compliance by external service providers.

Developer Configuration Management (SA-10)

1. The ISO shall require that information system developers/integrators:

a. Perform configuration management during information system, component or service design, development, implementation, operation and disposal.

b. Document, manage and control the integrity of changes to the configuration items under configuration management.

c. Implement only organization-approved changes to the system, component or service.

d. Document approved changes to the system, component or service and the potential security and privacy impacts of such changes.

e. Track security flaws and flaw resolution within the system, component or service and report findings to the ISO.

f. Provide an alternate configuration management process using organizational personnel in the absence of a dedicated developer configuration management team.

g. Enable integrity verification of software, firmware and hardware components.

h. Employ tools for comparing newly generated versions of security-relevant hardware descriptions, source code and object code with previous versions.

i. Maintain the integrity of the mapping between the master build data describing the current version of security-relevant hardware, software and firmware and the on-site master copy of the data for the current version.

j. Execute procedures for ensuring that security-relevant hardware, software and firmware updates distributed to the organization are exactly as specified by the master copies.

k. Include the ISO or designee in the configuration change management and control process.

Developer Testing and Evaluation (SA-11)

1. The ISO or designee shall require the developer of the system, system component, or system service, at all post-design stages of the system development life cycle, to:
    a. Develop and implement a plan for ongoing security and privacy control assessments;
        i. Testing requirements must be included in:
            1. Contractual documents for development and system integration.
            2. Internal development procedures.
        ii. The plan must include requirements for retesting after significant changes occur.
    b. Perform unit, integration, system and regression testing/evaluation before moving the development content to production at the appropriate depth and coverage.
    c. Produce evidence of the execution of the assessment plan and the results of the testing and evaluation.
    d. Implement a verifiable flaw remediation process which includes:
        i. The employment of static code analysis tools to identify common flaws and the documentation of the results of the analysis.
    e. Correct flaws identified during testing and evaluation.
    f. Document the results of the security testing/evaluation and flaw remediation processes.
    g. Require the developer of the system, system component or system service to employ static code analysis tools to identify common flaws and document the results of the analysis.
    h. Require the developer of the system, system component or system service to perform threat modeling and vulnerability analyses during development and the subsequent testing and evaluation of the system, component or service that:
        i. Uses the following contextual information: Business Impact Analysis, Risk Assessment and organization-defined information concerning impact, environment of operations, known or assumed threats and acceptable risk levels.
        ii. Employs the following tools and methods: approved tools and methods.
        iii. Conducts the modeling and analyses at the following level of rigor: organization-defined breadth and depth of modeling and analyses.
        iv. Produces evidence that meets the following acceptance criteria: Information Security Officer-defined acceptance criteria.
    i. Require the developer of the system, system component or system service to perform a manual code review of organization-defined code using the following processes, procedures and/or techniques: organization-defined processes, procedures, and/or techniques.
    j. Require the developer of the system, system component or system service to perform penetration testing:
        i. At the following level of rigor: inputs; and
        ii. Under the following constraints: constraints as approved by the ISO.
    k. Require the developer of the system, system component or system service to perform attack surface reviews.
    l. Require the developer of the system, system component or system service to verify that the scope of testing and evaluation provides complete coverage of required controls at the following level of rigor: appropriate depth of testing/evaluation as approved by the ISO.
    m. Require the developer of the system, system component or system service to employ dynamic code analysis tools to identify common flaws and document the results of the analysis.

n. Require the developer of the system, system component or system service to employ interactive application security testing tools to identify flaws and document the results.

Development Process, Standards and Tools (SA-15)

Development tools include programming languages and computer-aided design systems. Reviews of development processes include the use of maturity models to determine the potential effectiveness of such processes. Maintaining the integrity of changes to tools and processes facilitates effective supply chain risk assessment and mitigation. Such integrity requires configuration control throughout the system development life cycle to track authorized changes and prevent unauthorized changes.

The DOF ISO will require the following from system developers:

1. Require the developer of the system, system component, or system service to follow a documented development process that:
    a. Explicitly addresses security and privacy requirements.
    b. Identifies the standards and tools used in the development process.
    c. Documents the specific tool options and tool configurations used in the development process.
    d. Documents, manages and ensures the integrity of changes to the process and/or tools used in development.
2. Review the development process, standards, tools, tool options and tool configurations on at least an annual basis and following an environmental change to determine if the process, standards, tools, tool options and tool configurations selected and employed can satisfy the following security and privacy requirements: organization-defined security and privacy requirements.
3. Require the developer of the system, system component, or system service to:
    a. Reduce attack surfaces to the requirements set forth by the Enterprise Architecture Standard.
    b. Use threat modeling and vulnerability analyses from similar systems, components or services to inform the current development process.
    c. Be released or delivered together with the corresponding evidence supporting the final security and privacy review.
    d. Minimize the use of personally identifiable information in development and test environments.

Developer-Provided Training (SA-16)

1. The ISO or designee will require the developer of the system, system component or system service to provide the following training on the correct use and operation of the implemented security and privacy functions, controls, and/or mechanisms:
    a. Organization-defined training which may include:
        i. web-based and computer-based training
        ii. classroom-style training
        iii. hands-on training (including micro-training)
        iv. in-house training
        v. self-training to organizational personnel

Developer Security and Privacy Architecture Design (SA-17)

1. The ISO or designee shall require the developer of the system, system component or system service to produce a design specification and security and privacy architecture that:
    a. Is consistent with the organization’s security and privacy architecture that is an integrated part of the organization’s enterprise architecture.

b. Accurately and completely describes the required security and privacy functionality and the allocation of controls among physical and logical components.

c. Expresses how individual security and privacy functions, mechanisms and services work together to provide required security and privacy capabilities and a unified approach to protection.

d. Defines security-relevant hardware, software and firmware.

e. Provides a rationale that the definition for security-relevant hardware, software and firmware is complete.

f. Structures security-relevant hardware, software and firmware to facilitate testing.

g. Structures security-relevant hardware, software and firmware to facilitate controlling access with least privilege.

Unsupported System Components (SA-22)

1. The system owner or designee shall:

   a. Replace system components when support for the components is no longer available from the developer, vendor or manufacturer.

   b. Provide the following options for alternative sources for continued support for unsupported system components:

      i. An approved contract with an external provider.

AUTHORITY

This policy and procedure is issued by the Virginia state forester.

INTERPRETATION

The director of information technology and the chief of administration are responsible for the interpretation of this policy and procedure.

APPROVAL

I certify that this policy and procedure is approved and ready for publication.

Parik Patel
Director of Information Technology Name (Print)

DocuSigned by:
Parik Patel
3448F7C5358F457...
7/8/2024
Director of Information Technology Signature

Amanda Davis
Chief of Administration Name (Print)

DocuSigned by:
amanda davis
C2CCAB60F85A4A6...
7/9/2024
Chief of Administration Signature

VERSION HISTORY

Version History

Date	Version	Details	Author/Contributors
July 8, 2024	1	Original – CSRM template and updated with SEC530	Catherine Shefski, ISO