Division of Enterprise Technology Strategy and Services

ETSS Policy 800.1

System and Services Acquisition Policy

Publish Date: 15 July 2026
Effective Date: 15 July 2026
Last Revision Date: 14 July 2026

doa.entsec@doit.ri.gov

1. Purpose

This policy establishes the requirements for acquiring, developing, and managing information systems and services with adequate security controls to safeguard the State's information, infrastructure, and data. It defines requirements for resource allocation, system development lifecycle integration, acquisition processes, system documentation, security engineering principles, external system services, developer configuration management and testing, and the management of unsupported system components.
This policy supports the State's compliance with NIST SP 800-53 Revision 5 (System and Services Acquisition family), NIST SP 800-160 (Systems Security Engineering), NIST Cybersecurity Framework 2.0, IRS Publication 1075, and other applicable federal and state regulatory requirements. Security integration across the SDLC is aligned with the ETSS Operating Model, which embeds security across the Plan, Design, Build, and Run phases.

2. Applicability

This policy applies to all State of Rhode Island Executive Branch departments, including agencies, boards, and commissions, as well as their employees (permanent, non-permanent, full-time, and part-time), interns, consultants, contractors, vendors, and any entity that has access to State network resources, whether operated or maintained by the State or on behalf of the State. For the purposes of this policy, the term "Agency" refers to any department, agency, division, or unit of the Executive Branch.
This policy applies to all information system and service acquisitions, including commercial off-the-shelf products, custom-developed systems, cloud services (IaaS, PaaS, SaaS), managed services, and contractor-provided development and operations.

3. Definitions

The following terms are defined for the purposes of this policy. All other terms should be referenced in the ETSS Glossary of Terms, Acronyms, and Definitions.
System Development Life Cycle (SDLC)
The scope of activities associated with an information system, encompassing the system's initiation, requirements and design, development and configuration, testing and assessment, deployment and authorization, operations and maintenance, and ultimately its decommissioning and disposal.

External System Service
An information system service provided by an external entity, including cloud services, managed security services, outsourced applications, and contractor-provided development, hosting, or operations.
Security Engineering Principles
Design principles applied throughout the SDLC to ensure that information systems are built with security integrated from inception, including defense-in-depth, least privilege, zero trust, secure-by-design, and separation of duties.

4. Procedures for Compliance

The following requirements establish the system and services acquisition controls that agencies and ETSS must implement. Security controls are assigned based on the Information Assurance Level (IAL) of the information system, aligned to the NIST SP 800-53 Rev. 5 Moderate baseline.

4.1 System and Services Acquisition Policy and Procedures (SA-1)

Applies to: All systems (IAL1, IAL2)

Each agency shall develop, document, and disseminate a system and services acquisition policy and supporting procedures to designated personnel identified in the applicable System Security Plan. The ETSS CISO is designated as the official responsible for the enterprise policy. The policy shall be reviewed and updated at least every three (3) years and following significant changes. Supporting procedures shall be reviewed in alignment with the policy.

4.2 Allocation of Resources (SA-2)

Applies to: All systems (IAL1, IAL2)

Each agency shall:

a. Determine high-level security and privacy requirements for the information system or service in mission and business process planning.

b. Identify, document, and allocate the appropriate resources required to protect the information system or service as part of the capital planning and investment control process. Resource determination shall include personnel, technology, licensing, training, and managed service needs, coordinated through the CISO, CTO, CDO, and agency leadership via the ETSS governance structure. ETSS uses ServiceNow for asset inventory and service catalog tracking, JIRA for security project tracking, and Archer for GRC functions including risk management and exception tracking.

c. Establish discrete line items for information security systems or services within the budgeting process, funded via the agency chargeback model. Funding shall include allocation for both initial acquisition and ongoing sustainment of the system or service.

4.3 System Development Life Cycle (SA-3)

Applies to: All systems (IAL1, IAL2)

Each agency shall:

a. Acquire, develop, and manage information systems using an SDLC that incorporates information security and privacy considerations. Risk management integration across SDLC phases shall include: security categorization and initial risk assessment during initiation; threat modeling, security architecture review, and data flow analysis during requirements and design; secure coding practices, automated code scanning, and configuration baseline enforcement during development; security testing, vulnerability scanning, and control assessment during testing; authorization decisions and monitoring integration during

deployment; continuous monitoring and patch management during operations; and secure data disposal and CMDB decommissioning during system retirement.

b. Require a documented business case justification for custom system development projects that supports the rationale for not enhancing current systems, demonstrates the inadequacies of packaged solutions, and justifies the creation of custom software.

c. Implement a Change Enablement program managed through ServiceNow, including multi-tiered deployment environments (development, test, quality control, production) with rollback capabilities.

d. Plan for End-of-Life (EOL) and End-of-Support (EOS) dates for information systems and services to ensure systems can receive security patches throughout the SDLC and the agency is prepared to decommission systems that can no longer be secured.

e. Define and document information security and privacy roles and responsibilities throughout the SDLC and identify qualified individuals to ensure SDLC activities meet security requirements.

f. Integrate information security and privacy risk management processes into all SDLC activities. Agency IT projects and new technology requests shall be guided through the ETSS Office of Digital Excellence (ODE) and Portfolio Management Office (PPMO) to ensure alignment with State priorities.

4.4 Acquisition Process (SA-4)

Applies to: All systems (IAL1, IAL2)

Security functional requirements shall be part of every hardware, software, and firmware acquisition process. Agencies shall comply with State procurement policies and include the following requirements in acquisition contracts:

a. Security and privacy functional requirements, including security capabilities, functions, and mechanisms.

b. Strength of mechanism requirements based on the security categorization of the information system or data. When contracting with external service providers, contracts shall require: the provider supplies security and privacy policies for data handling; non-public data is encrypted in transit and at rest; all encryption uses FIPS 140-2, FIPS 140-3 validated, or similar modules; storage devices are sanitized per ETSS Media Protection Policy (300.x); and outsourced services outside the continental United States are authorized by the ETSS CISO and CTO with CDO approval if required by level of risk.

c. Security and privacy assurance requirements, including evidence from development and assessment activities.

d. Controls needed to satisfy security and privacy requirements, including vendor hardware configuration compliance with State policies and technical specifications.

e. Requirements for protecting security-related documentation.

f. Description of the development and operational environments.

g. Allocation of responsibility for information security, privacy, and supply chain risk management.

h. Acceptance criteria for assessing the system's ability to perform its intended function.

4.4.1 Functional Properties of Controls (SA-4(1))

Applies to: Moderate and above (IAL2)

Each agency shall require the developer to provide a description of the functional properties of the security controls to be employed, describing the functionality

visible at the interfaces of the controls.

4.4.2 Design and Implementation Information for Controls (SA-4(2))

Applies to: Moderate and above (IAL2)

Each agency shall require the developer to provide design and implementation information for the controls, including security-relevant external system interfaces and high-level design documentation in sufficient detail to validate control implementation.

4.4.3 Functions, Ports, Protocols, and Services in Use (SA-4(9))

Applies to: Moderate and above (IAL2)

Each agency shall require the developer to identify, early in the SDLC, the functions, ports, protocols, and services intended for agency use.

4.5 System Documentation (SA-5)

Applies to: All systems (IAL1, IAL2)

Each agency shall:

a. Obtain or develop administrator documentation describing secure configuration, installation, and operation of the system; effective use and maintenance of security functions; and known vulnerabilities regarding administrative or privileged functions.

b. Obtain or develop user documentation describing user-accessible security functions, methods for secure user interaction, and user responsibilities for maintaining security and privacy.

c. Document attempts to obtain documentation when it is unavailable or nonexistent.

d. Distribute documentation to designated officials and maintain secure, current, and accessible documentation libraries available to authorized personnel always. Documentation shall be reviewed annually for accuracy and relevancy.

4.6 Security and Privacy Engineering Principles (SA-8)

Applies to: All systems (IAL1, IAL2)

Each agency shall apply information system security and privacy engineering principles in the specification, design, development, implementation, and modification of information systems, including new systems and major upgrades. Per the ETSS Security and Risk Program Management Policy (PM-1), control implementation shall follow the principles of least privilege, zero trust, defense-in-depth, and secure-by-design. Engineering principles include:

a. Developing a layered (defense-in-depth) approach to securing the information system.

b. Establishing sound security policy, architecture, and controls as the foundation for design.

c. Incorporating security requirements into all SDLC phases.

d. Delineating physical and logical security boundaries.

e. Training system developers to build secure software.

f. Performing threat modeling to identify use cases, threat agents, attack vectors, and compensating controls.

g. Reducing risk to acceptable levels to enable informed risk management decisions.

4.7 External System Services (SA-9)

Applies to: All systems (IAL1, IAL2)

Each agency shall:

a. Require that providers of external information system services comply with statewide information security requirements, including applicable federal and

State laws, ETSS policies and standards, and established service-level agreements. For outsourced services that process non-public data and reside outside the continental United States, the agency shall notify the ETSS CTO, CISO, and CDO for authorization prior to contract award and notify the CDO and CISO no less than forty-five (45) days prior to initial data transmission.

b. Require external providers to demonstrate compliance with State standards, including providing annual third-party risk assessment reports (SOC 2 Type II, ISO 27001, or FedRAMP Moderate authorization) for offsite hosting or cloud services.

c. Define and document how external services comply with statewide security controls, including user roles, responsibilities, and compliance auditing requirements.

d. Include in outsourcing agreements: remedies for inadequate security controls, vendor contingency and disaster recovery capabilities, all relevant security requirements for compliance with State standards and record retention, and annual review of external services and deliverables.

e. Monitor third-party service performance against contract requirements, manage identified problem areas, maintain a list of all service providers who store or share classified data, and control changes to SLAs through formal change management.

4.7.1 Identification of Functions, Ports, Protocols, and Services (SA-9(2))

Applies to: Moderate and above (IAL2)

Each agency shall require providers of external system services to identify the functions, ports, protocols, and other services required for the use of such services.

4.8 Developer Configuration Management (SA-10)

Applies to: Moderate and above (IAL2)

Each agency shall require the developer of the information system, system component, or system service to:

a. Perform configuration management during design, development, implementation, and operation for both internal and external system development and integration.

b. Document, manage, and control changes to the system or configuration items under configuration management.

c. Implement only agency-approved changes. Source code in custom-developed applications shall be protected to mitigate risks of exploitation.

d. Document approved changes and the potential security and privacy impacts of those changes.

e. Track security flaws and flaw resolution and report findings to the system administrator, Agency Information Manager (AIM), and agency Technical Support Manager (TSM).

4.9 Developer Testing and Evaluation (SA-11)

Applies to: Moderate and above (IAL2)

Each agency shall require the developer, at all post-design stages of the SDLC, to:

a. Develop and implement a plan for ongoing security and privacy control assessments, including requirements for retesting after significant changes and documented rollback plans.

b. Perform system testing during each phase of development and prior to production deployment. Actual PII shall not be used for testing. Production data may be used only when no alternative exists and with equivalent security controls applied. Data anonymization or masking tools shall be used where available.

c. Produce evidence of the execution of the security assessment plan and results.

d. Implement a verifiable flaw remediation process to correct weaknesses identified during testing. Use a formal recording system to track faults from reporting through resolution, monitor status, and provide metrics to management.

e. Correct flaws and perform regression testing. Require vulnerability assessments, verify remediations, certify software in test environments before production deployment, remove test data and accounts prior to production, and document acceptance testing results including capacity, error response, security controls, business continuity impact, and training readiness.

4.10 Development Process, Standards, and Tools (SA-15)

Applies to: Moderate and above (IAL2)

Each agency shall:

a. Require the developer to follow a documented development process that explicitly addresses security and privacy requirements, identifies standards and tools used, documents tool configurations, and ensures the integrity of changes to the process.

b. Review the development process, standards, tools, and configurations every three (3) years to determine if they satisfy security and privacy requirements.

4.10.1 Criticality Analysis (SA-15(3))

Applies to: Moderate and above (IAL2)

Each agency shall require the developer to perform a criticality analysis at critical points of the SDLC process, including development, implementation, and maintenance phases, and the supply chain. Analysis shall cover functional specifications, high-level and low-level designs, source code, and hardware schematics of high-value assets.

4.11 Unsupported System Components (SA-22)

Applies to: All systems (IAL1, IAL2)

Each agency shall:

a. Replace information system components when security patches, updates, or support from the manufacturer or vendor are no longer available.

b. Provide alternative sources for continued support of unsupported components, such as increased personnel, customized patching, or contracted external providers who specialize in supporting unsupported components or legacy systems. Continued operation of unsupported components shall be documented through the ETSS risk acceptance process and tracked via the POAM.

5. Repercussions for Non-Compliance

Failure to comply with this policy may result in corrective action proportional to the severity of the violation. Consequences may include, but are not limited to:

a. Denial of system authorization (Authority to Operate) for systems acquired or developed without adequate security controls.

b. Suspension or termination of vendor or contractor agreements for non-compliant external service providers.

c. Mandatory remediation of acquisition or development security deficiencies within defined timelines.

d. Referral to agency management for disciplinary proceedings for personnel who bypass security requirements in the acquisition process.

e. Escalation to ETSS leadership and the CDO for systemic non-compliance affecting enterprise security posture.

Non-compliance findings shall be documented and tracked through ETSS governance processes and may be recorded as findings in the agency Plan of Action and Milestones (POAM).

6. Roles and Responsibilities

The following roles are accountable for the implementation, monitoring, and enforcement of this policy:

Chief Information Security Officer (CISO)
Responsible for enterprise-level system and services acquisition policy oversight, security review of acquisition contracts, approval of outsourced services outside the continental United States (jointly with CDO), and oversight of security engineering principles and developer security requirements.

Chief Digital Officer (CDO)
Approves the allocation of resources for information security. Authorizes outsourced information system services that process non-public data outside the continental United States. Program Owner per PM-1 who approves frameworks, technologies, processes, and staffing necessary for program execution.

Chief Technology Officer (CTO)
Ensures enterprise platforms implement inheritable controls and tracks exceptions centrally with enterprise POAMs. Oversee infrastructure and platform teams responsible for executing SDLC deployment and operations phases.

ETSS Office of Digital Excellence (ODE) and Portfolio Management Office
Guides agency IT projects and new technology requests through execution to ensure alignment with State priorities and strategy. Manages project intake, governance reviews, and coordination with Centers of Excellence and the IT Governance Board.

ETSS Vendor Management Office (VMO)
Manages vendor contracts, SLA compliance monitoring, and third-party risk assessment requirements. Coordinates with agencies on procurement of IT systems and services to ensure security requirements are incorporated into acquisition documents.

System Owners
Responsible for ensuring security requirements are incorporated into system acquisitions and development activities, maintaining system documentation, coordinating security testing, and managing outsourcing agreements and third-party deliverable monitoring for their systems.

Agency Information Managers (AIMs) / Technical Support Managers (TSMs)
Coordinate acquisition and development activities at the agency level, receive developer security flaw reports, and ensure agency compliance with this policy.

7. Approval / Review Signatures

Ramesh madhavan
Digitally signed by Ramesh madhavan
Date: 2026.07.15 08:27:14 -04'00'

Chief, IT Vendor Management (VMO)
Division of Enterprise Technology Strategy and Services


Digitally signed by Nathan Loura
Date: 2026.07.15 10:50:52 -04'00'

Chief Information Security Officer (CISO)
Division of Enterprise Technology Strategy and Services

Brian Tardiff

Digitally signed by Brian Tardiff
Date: 2026.07.15 11:26:47 -04'00'

Chief Digital Officer (CDO)
Division of Enterprise Technology Strategy and Services