Division of Enterprise Technology Strategy and Services

ETSS Policy 300.12

Security Planning

Publish Date: 23 June 2026
Effective Date: 23 June 2026
Last Review: 22 June 2026

doa.entsec@doit.ri.gov

1. Purpose

This policy establishes the requirements for security planning across State of Rhode Island information systems. Security planning ensures that information systems are designed, implemented, operated, and maintained with appropriate security and privacy controls, and that the security posture of each system is documented, reviewed, and authorized. This policy defines the requirements for developing and maintaining System Security Plans (SSPs), establishing rules of behavior, managing security and privacy architectures, and selecting and tailoring control baselines.

This policy supports the State's compliance with NIST SP 800-53 Revision 5 (Planning family), NIST Cybersecurity Framework 2.0, the NIST Risk Management Framework (SP 800-37), IRS Publication 1075, and other applicable federal and state regulatory requirements.

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 information systems and data, 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 systems that process, store, or transmit State data, including enterprise-managed, agency-managed, cloud-hosted, and hybrid environments.

3. Roles and Responsibilities

3.1. Chief Information Security Officer (CISO)

Designated as the official responsible for the enterprise Security Planning policy and procedures. Responsible for oversight of System Security Plan development and maintenance, baseline selection and tailoring decisions, security and privacy architecture reviews, and ensuring consistency of security planning across enterprise systems. Reviews and approves SSPs prior to authorization decisions.

3.2. DOA Chief Privacy Officer

Coordinates with the CISO on privacy-related aspects of System Security Plans, reviews

privacy controls and PII risk assessments, and receives distribution of SSP updates affecting privacy requirements.

3.3. Authorizing Official

Formally assumes responsibility for operating an information system at an acceptable level of risk. Reviews and approves the SSP and authorizes the system to operate. For enterprise systems, the CDO serves as the Authorizing Official.

3.4. System Owners

Responsible for developing, maintaining, and updating the System Security Plan for their information systems. Ensures the SSP accurately reflects the system boundary, security categorization, control implementation, and operational environment. Coordinates with ETSS on security-related planning activities.

3.5. Agency Information Managers (AIMs) / Technical Support Managers (TSMs)

Receive distribution of SSPs and updates. Coordinate security planning activities at the agency level. Assist system owners with control implementation documentation and agency-specific tailoring requirements.

3.6. All Personnel

Responsible for reading, acknowledging, and complying with the Rules of Behavior as documented in the ETSS Technology Acceptable Use Policy. Must re-acknowledge the rules annually and whenever they are updated. Responsible for adhering to social media and external platform usage restrictions.

4. Procedures for Compliance

The following requirements establish the security planning 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 Security Planning Policy and Procedures (PL-1)

Applies to: All systems (IAL1, IAL2)

Each agency shall develop, document, and disseminate a security planning policy and supporting procedures to designated personnel identified in the applicable System Security Plan. The policy shall address purpose, scope, roles and responsibilities, management commitment, coordination among organizational entities, and compliance requirements.

The ETSS CISO is designated as the official responsible for managing the development, documentation, and dissemination of the enterprise security planning policy and procedures.

The agency shall review and update the security planning policy at least every three (3) years and following any significant changes to laws, regulations, technologies, or the threat environment. Supporting procedures shall be reviewed in alignment with the policy and updated following significant changes.

4.2 System Security and Privacy Plans (PL-2)

Applies to: All systems (IAL1, IAL2)

Each agency shall:

a. Develop a System Security Plan (SSP) for the information system that:

(1) Reflects the information security architecture and is consistent with the enterprise architecture.

(2) Explicitly defines the constituent information system components.

(3) Describes the operational context of the information system in terms of mission and business processes.

(4) Identifies the individuals that fulfill information system roles and responsibilities.

(5) Identifies the information types processed, stored, and transmitted by the information system.

(6) Provides the security categorization of the information system, including supporting rationale.

(7) Describes any specific threats to the information system that concern the agency.

(8) Provides the results of a risk assessment for systems that process PII.

(9) Describes the operational environment for the information system and any dependencies on or connections to other information systems or system components.

(10) Provides an overview of the security and privacy requirements for the information system.

(11) Identifies any relevant control baselines or overlays, if applicable.

(12) Describes the controls in place or planned for meeting security and privacy requirements, including the rationale for any tailoring decisions.

(13) Includes risk determinations for the security architecture and design decisions.

(14) Includes security- and privacy-related activities affecting the information system that require planning and coordination with the DOA Chief Privacy Officer, ETSS CISO, and other designated stakeholders, including assessments, audits, inspections, hardware and software maintenance, acquisition and supply chain risk management, patch management, and contingency plan testing.

(15) Is reviewed and approved by the authorizing official or designated representative prior to plan implementation.

b. Distribute copies of the SSP and communicate subsequent changes to plan stakeholders, including the DOA Chief Privacy Officer, ETSS CISO or delegate, Agency Information Managers (AIMs), Agency Technical Support Managers (TSMs), and all personnel designated by the agency that require access to the SSP.

c. Review the SSP at least annually, or more frequently when data sensitivity levels increase, after a serious security violation or significant change to the threat environment, or prior to the previous security authorization expiring.

d. Update the SSP to address changes to the information system, operational environment, or issues identified during plan implementation or security control assessments.

e. Protect the SSP from unauthorized disclosure or modification.

4.3 Rules of Behavior (PL-4)

Applies to: All systems (IAL1, IAL2)

Each agency shall:

a. Establish and make readily available to all individuals requiring access to State

networks or information systems the rules that describe their responsibilities and expected behavior regarding information and information system usage. At a minimum, individuals must adhere to all requirements documented in the ETSS Technology Acceptable Use Policy (00-02). Rules of Behavior apply to employees, contractors, interns, vendors, and any other individuals authorized to access State systems and are communicated prior to granting system access.

b. Receive a documented acknowledgment from individuals requiring access to State networks or information systems, indicating that they have read, understand, and agree to abide by the rules of behavior, before authorizing access. Acknowledgments are captured through enterprise onboarding, access provisioning, or annual compliance processes and are maintained as auditable records. Access may be denied, suspended, or revoked if acknowledgment is not completed.

c. Review and update the Rules of Behavior at least every three (3) years, or sooner in response to changes in technology, regulatory requirements, or identified risks. Updates shall be approved through established ETSS governance processes prior to reissuance.

d. Require individuals who have previously acknowledged the Rules of Behavior to re-read and re-acknowledge the rules at least annually and whenever the rules are revised or materially changed.

4.3.1 Social Media and External Site/Application Usage Restrictions (PL-4(1))

Applies to: All systems (IAL1, IAL2)

At a minimum, all users granted access to the State network are required to adhere to the restrictions and requirements documented in the ETSS Social Media and External Platform Use Policy. Additionally, all users are prohibited from posting classified or sensitive data on any social media, social networking, or other public website. The agency may establish agency-specific usage restrictions to further restrict social media use based on the potential for these technologies to cause damage or disruption to the information system or agency mission. Use of social media platforms for official State business is restricted to authorized personnel only, enforced through membership in a designated security group maintained by ETSS. The Rules of Behavior shall include restrictions on:

a. Use of social media, social networking sites, and external sites and applications.

b. Posting organizational information on public websites.

c. Use of organization-provided identifiers (such as State email addresses) and authentication secrets (such as passwords) for creating accounts on external sites and applications.

4.4 Security and Privacy Architectures (PL-8)

Applies to: Moderate and above (IAL2)

Each agency shall:

a. Develop security and privacy architectures for the information system that: (1) describe the overall philosophy, requirements, and approach for protecting the confidentiality, integrity, and availability of agency information; (2) describe the requirements and approach for processing personally identifiable information (PII) to minimize privacy risk to

individuals; (3) describe how the architectures are integrated into and support the enterprise architecture; and (4) describe assumptions about and dependencies on external systems and services. Security and privacy architectures shall be informed by enterprise standards, approved technologies, and the State's adopted NIST Risk Management Framework and 800-53 Moderate controls baseline.

b. Review and update the security and privacy architectures at least annually and whenever a significant change occurs, as defined in NIST SP 800-37 Revision 2, Appendix F. Significant changes may include major system architecture or hosting changes, introduction of new technologies or services, material changes to data types processed, or changes to trust relationships or external service dependencies.

c. Ensure that planned information security architecture changes are reflected in System Security Plans, organizational procedures and operating documentation, and procurement and acquisition activities.

4.5 Baseline Selection (PL-10)

Applies to: All systems (IAL1, IAL2)

Each agency shall select a security and privacy control baseline for the information system in accordance with the ETSS Security and Risk Program Management Policy (PM-1). ETSS has adopted NIST SP 800-53 Revision 5 as the authoritative control catalog, with predefined Low (IAL1) and Moderate (IAL2) baselines established and maintained through PM-1. The selected baseline shall be documented within the System Security Plan, including identification of inherited enterprise controls and system-specific responsibilities.

Although not mandatory, the agency may select additional controls documented in PM-1 or NIST SP 800-53 Rev. 5 to increase the security posture of the information system, to meet federal or state laws, executive orders, directives, regulations, policies, standards, or guidelines, to address privacy concerns, or to comply with program requirements. The ETSS CISO is responsible for oversight of baseline selection and ensuring consistency across enterprise systems.

4.6 Baseline Tailoring (PL-11)

Applies to: All systems (IAL1, IAL2)

Each agency shall tailor the selected control baseline in accordance with the ETSS Security and Risk Program Management Policy (PM-1) and the NIST Risk Management Framework. Baseline tailoring is performed to ensure controls are risk-appropriate, agency function-aligned, and technically feasible, while maintaining compliance with enterprise standards and regulatory requirements. The tailoring process includes:

a. Applying scoping considerations based on system architecture, hosting model, and operational context.

b. Selecting or excluding controls and enhancements that are not applicable to the system.

c. Defining system-specific parameters for controls requiring organization-defined values.

d. Implementing compensating controls where standard controls cannot be

fully implemented.

e. Supplementing baseline controls with additional controls or enhancements from NIST SP 800-53 Rev. 5 as warranted by the risk environment.

The agency must evaluate the information system and identify each control as being one of the following types: Common controls (controls implemented by ETSS and inherited by the agency), System-specific controls (controls providing security or other services specific to the agency information system), or Hybrid controls (controls shared between ETSS, cloud service providers, and the agency).

Any deviations from the enterprise baseline that result in residual risk shall be formally tracked through the Plan of Action and Milestones (POAM) process and are subject to risk acceptance by the appropriate Authorizing Official or designated authority. The ETSS CISO provides oversight of baseline tailoring to ensure consistency across systems and alignment with the State's enterprise risk posture.

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. Revocation or suspension of information system access.

b. Mandatory retraining on security planning requirements and rules of behavior.

c. Formal counseling or written reprimand.

d. Referral to agency management and human resources for disciplinary proceedings, up to and including termination of employment.

e. Termination of vendor or contractor agreements for external provider personnel.

f. Denial of system authorization (Authority to Operate) for systems that do not have a current, approved System Security Plan.

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. Approval / Review Signatures

Sanjay Gupta
Digitally signed by Sanjay Gupta
Date: 2026.06.22 16:39:52 -04'00'

Chief Technology Officer (CTO)
Division of Enterprise Technology Strategy and Services (ETSS)

Digitally signed by Nathan Loura
Date: 2026.06.23 12:30:06 -04'00'

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

Brian Tardiff
Digitally signed by Brian Tardiff
Date: 2026.06.23 12:43:52 -04'00'

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