Division of Enterprise Technology Strategy and Services

ETSS Policy 300.14

Personnel Security Policy (PS)

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 personnel security requirements for the State of Rhode Island to ensure that individuals who access State information systems and data are trustworthy, qualified, and aware of their security responsibilities. Personnel security is a foundational element of the State's information security program because system users require access to sensitive data and, whether through malicious intent or lack of awareness, can introduce significant risk to the confidentiality, integrity, and availability of that data.

This policy defines the requirements for position risk designation, personnel screening, access agreements, personnel termination and transfer processes, external provider personnel security, personnel sanctions, and the integration of security responsibilities into position descriptions. It supports the State's compliance with NIST SP 800-53 Revision 5 (Personnel Security family), NIST Cybersecurity Framework 2.0, 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 also applies to external providers, including contractors and other organizations that provide information system development, IT services, outsourced applications, and network or security management on behalf of the State.

3. Roles and Responsibilities

3.1. Chief Information Security Officer (CISO)

Owns the Personnel Security Policy at the enterprise level. Responsible for policy development, approval, dissemination, and oversight. Receives notification of all formal personnel sanctions related to information security policy violations. Coordinates with the CDO, CTO, and Agency leadership to ensure personnel security controls are consistently applied across the enterprise.

3.2. Agency Heads

Responsible for ensuring agency-level compliance with this policy, including assignment of position risk designations, initiation of personnel screening, execution of termination and transfer processes, maintenance of access agreements, and enforcement of the formal sanctions process within their agency.

3.3. Agency Human Resources (HR)

Responsible for initiating screening activities prior to granting information system access, conducting or coordinating exit interviews, initiating transfer and reassignment workflows through the ERP system, and coordinating with ETSS IAM and agency management on termination and transfer actions.

3.4. ETSS Identity and Access Management (IAM)

Responsible for executing access provisioning, modification, and revocation actions in enterprise identity systems (Active Directory, Entra ID, CyberArk) in response to personnel termination, transfer, and screening events. Ensures that credential revocation is completed within required timeframes.

3.5. System Owners

Responsible for ensuring that personnel security requirements are met for individuals accessing their systems, including coordinating with ETSS IAM on access changes, documenting personnel security requirements in System Security Plans, and retaining access to data and resources formerly controlled by terminated individuals.

3.6. Agency Technical Support Managers (TSMs) / AIMs

Responsible for coordinating personnel security actions at the agency level, including receiving notifications of terminations and transfers, facilitating access changes for agency-managed systems, and serving as the liaison between agency HR and ETSS for personnel security matters.

3.7. All Personnel

Responsible for complying with access agreements, reporting changes in personal circumstances that may affect security eligibility, safeguarding credentials and access devices, and completing required security awareness training. Personnel are expected to report suspected policy violations promptly.

4. Procedures for Compliance

The following requirements establish the personnel security controls that agencies and ETSS must implement. All controls in this policy apply to all information systems regardless of Information Assurance Level (IAL), as personnel security requirements under the NIST SP 800-53 Rev. 5 Moderate baseline are universally applicable to Low, Moderate, and High impact systems.

4.1 Personnel Security Policy and Procedures (PS-1)

Applies to: All systems (IAL1, IAL2)

Each agency shall develop, document, and disseminate a personnel security 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 policy shall be consistent with applicable laws, executive orders, directives, regulations, and standards.

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

The agency shall review and update the personnel security policy at least every three (3) years and immediately following significant changes to hiring, screening, onboarding, offboarding, or access provisioning processes, or following changes to the threat environment or regulatory requirements. Supporting procedures shall be reviewed in alignment with the policy and updated following significant changes.

4.2 Position Risk Designation (PS-2)

Applies to: All systems (IAL1, IAL2)

Each agency shall:

a. Assign a position risk designation to all agency positions. The agency should consider physical access requirements to information system hardware or software, the ability to override or bypass security controls, and the scope of IT resources that may be impacted by security violations. Position risk designations shall adhere to the following criteria:

Low Position Risk: A position that has the potential to produce some limited harm to the State network, information system, or public trust.

Moderate Position Risk: A position that has the potential to produce moderate to serious impact to the State network, information system, or public trust. The position has duties and responsibilities of considerable importance to the agency or business mission.

High Position Risk: A position that has the potential to produce exceptionally serious impact to the State network, information system, or public trust. The position has duties and responsibilities that are especially critical to the agency or business mission.

b. Establish screening criteria for individuals filling those positions, appropriate to the assigned risk level.

c. Review and update position risk designations at least annually or when position descriptions are rewritten.

4.3 Personnel Screening (PS-3)

Applies to: All systems (IAL1, IAL2)

Each agency shall:

a. Screen individuals prior to authorizing access to information systems. At a minimum, criminal history checks shall be performed for all employees, vendors, and contractors with access to the State network. All individuals requiring access to classified data must meet personnel suitability standards based on valid need-to-know requirements. Access eligibility shall not be assumed from position or title alone and requires favorable results from a background check.

b. Rescreen individuals when there is a change to the position's current risk

designation (for example, from low to moderate or from moderate to high), when individuals change positions, or under other agency-defined criteria and conditions that merit rescreening. When an employee moves to a new position, all access and authentication credentials associated with the previous position shall be reviewed and revoked as required.

4.3.1 Information Requiring Special Protective Measures (PS-3(3))

Applies to: Moderate and above (IAL2)

Each agency shall ensure that individuals accessing information systems that process, store, or transmit data requiring special protection (such as Federal Tax Information, Social Security Administration data, or Criminal Justice Information) satisfy additional personnel screening criteria as mandated by the applicable federal program. These additional requirements shall be documented in the System Security Plan and coordinated with the relevant federal oversight body.

4.4 Personnel Termination (PS-4)

Applies to: All systems (IAL1, IAL2)

Upon termination of individual employment, the agency shall:

a. Disable information system access within four (4) hours of notification and notify appropriate agency personnel, including ETSS enterprise support teams, agency IT technical support, and system administrators. For individuals terminated for cause, the agency shall immediately escort the individual from agency facilities and, when feasible, disable information system and network access prior to notifying the individual of the termination. Access and privileges to information systems, networks, and facilities shall be suspended when an employee or contractor is temporarily separated from the agency (for example, leave of absence or military leave).

b. Terminate or revoke all authenticators and credentials associated with the individual, including ID badges, Active Directory accounts, federated identities, privileged and administrative credentials, multi-factor authentication tokens, certificates, and application-specific accounts that do not leverage enterprise single sign-on.

c. Where conducted by Agency Human Resources, perform an exit interview that includes a discussion on information security topics relevant to the agency, its mission and business requirements, and the departing individual, including non-disclosure obligations and post-employment confidentiality requirements.

d. Retrieve all agency information and security-related or information system-related property, including State-issued devices, access badges, keys, authentication tokens, and other assets that enable logical or physical access to State systems. Recovered assets shall be returned, inventoried, and handled in accordance with enterprise asset management and media protection policies.

e. Retain access to agency information systems and data formerly controlled by the terminated individual. ETSS and system owners shall ensure continuity of operations by reassigning ownership of data, files, and system resources, preserving audit logs and records, and ensuring business processes are not dependent on individual user accounts.

4.5 Personnel Transfer (PS-5)

Applies to: All systems (IAL1, IAL2)

Upon reassignment or transfer to other positions within the agency, the agency shall:

a. Review and confirm ongoing operational needs for current logical and physical access authorizations to information systems and facilities.

b. Initiate transfer or reassignment activities within twenty-four (24) hours of notification, including collecting and issuing keys, ID badges, and facility access cards as appropriate. Agency Human Resources shall initiate transfer actions through established enterprise workflows within the ERP system, in coordination with ETSS IAM, agency AIMs/TSMs, and relevant system owners.

c. Modify access authorizations as necessary to correspond with changes in operational need. Access shall not be cumulatively granted; privileges associated with the former position shall be removed prior to authorizing new access, reinforcing least-privilege principles.

d. Notify appropriate stakeholders, including ETSS IAM, agency AIMs/TSMs, system owners, and access control personnel responsible for affected systems, within twenty-four (24) hours of the transfer.

4.6 Access Agreements (PS-6)

Applies to: All systems (IAL1, IAL2)

Each agency shall:

a. Develop and document access agreements for information systems. Access agreements are fulfilled through the Acceptable Use Policy (AUP) and its embedded Rules of Behavior, as defined in control PL-4.

b. Review and update access agreements at least annually, in alignment with the Acceptable Use Policy review cycle.

c. Require individuals needing access to information systems to sign appropriate access agreements prior to being granted access and re-sign access agreements when they are updated, at least annually, or any time there is a change to the user's level of access. Access agreements require that individuals acknowledge they have read, understand, and agree to abide by the terms of the agreement, and shall indicate the penalties for non-compliance.

4.7 External Personnel Security (PS-7)

Applies to: All systems (IAL1, IAL2)

External providers include contractors and other organizations providing information system development, IT services, outsourced applications, and network or security management. Each agency shall:

a. Establish personnel security requirements for external providers, including security roles and responsibilities. At a minimum, external personnel security requirements shall align with the personnel security requirements defined in this policy.

b. Require external providers to comply with personnel security policies and procedures established by the agency.

c. Document personnel security requirements, including explicitly

documenting these requirements in acquisition-related documents.

d. Require external providers to notify the agency, including access control personnel responsible for the system and facilities, of any transfers or terminations of external provider personnel who possess agency credentials, ID badges, or information system privileges within twenty-four (24) hours of the transfer or termination.

e. Monitor provider compliance with personnel security requirements. Third-party personnel shall be provided with the minimum system and physical access necessary to perform contracted services.

4.8 Personnel Sanctions (PS-8)

Applies to: All systems (IAL1, IAL2)

Each agency shall:

a. Employ a formal sanctions process for individuals who fail to comply with established information security and privacy policies and procedures.

b. Notify the CISO or designated delegate within twenty-four (24) hours when a formal employee sanctions process is initiated, identifying the individual sanctioned and the reason for the sanction.

4.9 Position Descriptions (PS-9)

Applies to: All systems (IAL1, IAL2)

Each agency shall incorporate security and privacy roles and responsibilities into agency position descriptions. Position descriptions shall reflect the security requirements commensurate with the position's risk designation and the sensitivity of the information systems and data the position is authorized to access.

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. Suspension or revocation of information system access.

b. Mandatory retraining on personnel security requirements and responsibilities.

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. Referral to law enforcement if criminal activity is suspected.

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). The formal sanctions process described in Section 4.8 shall be followed for all personnel security policy violations.

6. Approval / Review Signatures

The appropriate signatories for this policy will be identified through the governance process to ensure accountability and formal authorization.

Sanjay Gupta

Digitally signed by Sanjay Gupta
Date: 2026.06.22 16:40:46 -04'00'

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

Digitally signed by Nathan Loura
Date: 2026.06.23 12:37:36 -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 12:44:08 -04'00'

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