1. Purpose

To establish a personnel security policy that provides effective governance of personnel to ensure the security of sensitive information systems and data. Personnel security is a highly challenging area within information security due to the unpredictable nature of individuals. The insider threat is considered one of the key risks to information security because system users require access to sensitive data and, too often, lack the knowledge or awareness of how to handle this data. Actions performed by personnel, whether malicious or accidental, that result in data breaches are detrimental to organizations and frequently lead to financial and reputational loss. Controlling this risk is critical to maintain the confidentiality, integrity, and availability of information systems and data.

2. Applicability

This policy is applicable to all State of Rhode Island Executive Branch Departments1 (including agencies, boards and commissions), and their employees (including permanent, non-permanent, full-time, and part-time) and interns, consultants, contractors, vendors, contracted individuals, and any entity having access to state information systems and data, whether operated or maintained by the state or on behalf of the state. For this policy, the term "Agency" is used to refer to any department, agency, division, or unit of the Executive branch of the State of Rhode Island.

3. Definitions

Access Agreement
An agreement between the state and personnel detailing expectations for use, behavior, and conduct while using information systems, applications, infrastructure, and other components. Examples include non-disclosure agreements, acceptable use agreements, rules of behavior, and conflict-of-interest agreements.

Position Risk Designation
The relative risk of a given position based on the information, data, systems, applications, devices, etc., that the position is authorized to have access to. In determining a position’s risk designation, physical access requirements to information system hardware or software, the

---

1 State of Rhode Island Executive Branch Departments does not include the University of Rhode Island, the State Colleges, the General Treasurer, the Attorney General, or the Secretary of State.
ability to override or bypass security controls, and the scope of IT resources that may be impacted by security violations should all be primary considerations.

Screening
The process by which personnel are verified or checked to determine their fitness for a given position. This process may include a simple criminal record search or may include detailed background checks conducted with the aid of third parties.

Termination
The process by which persons or personnel are separated or discharged from service, including voluntary or involuntary discharge, contract revocation or fulfillment, retirement, resignation, etc. Contractors, vendors, and third-party personnel may have their contracts terminated or other actions taken.

Transfer
A change in position typically associated with a change of responsibilities, access needs, system or device access, and information and data required for job completion.

4. Procedures for Compliance

Security controls in this policy will be implemented in accordance with the security categorization of the information system. The security categorization is based on the Information Assurance Level (IAL) requirements of the information system.

Low Risk Systems (IAL1)
Information systems that only contain data that is public by law or directly available to the public via mechanisms such as the internet. In addition, desktops, laptops, and supporting systems used by agencies are Low Risk unless they store, process, transfer, or communicate private or sensitive data.

Moderate Risk Systems (IAL2)
Information systems that store, process, transfer, or communicate private or sensitive data or have a direct dependency on a Moderate system. At a minimum, any information system that stores, processes, transfers, or communicates PII or other sensitive data types is classified as a Moderate system.

[IAL1, IAL2] Personnel Security Policy and Procedures (PS-1). The agency will develop, document, disseminate, review, and annually update a personnel security policy and procedures. Personnel security policy and procedures will be disseminated to designated personnel defined in the applicable system security plan, agency information managers (AIM), technical support managers (TSM), data owners, system owners, system administrators, and any other personnel or roles the agency determines require access.
4.1. \[IAL1, IAL2\] Position Risk Designation (PS-2). The agency will assign a risk designation to all agency positions, establish screening criteria for individuals filling those positions, and review and update position risk designations annually. In determining a position’s risk designation, 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:

**Low Position Risk** – Position has the potential to produce some limited harm to the state network, information system, or public trust.

**Moderate Position Risk** – Position 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** – Position 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.

4.2. \[IAL1, IAL2\] Personnel Screening (PS-3). The agency will screen individuals prior to authorizing access to the information system and rescreen individuals when there is a change to the position’s current risk designation (i.e. from low to moderate or from moderate to high), when individuals change positions, or other agency-defined criteria and conditions that merit rescreening.

4.3. \[IAL1, IAL2\] Personnel Termination (PS-4). Upon termination of individual employment, the agency will (i) disable information system access within one (1) day of termination, (ii) terminate/revoke any authenticators/credentials associated with the individual, including ID badges, Active Directory (AD) accounts, and accounts that do not leverage single sign-on AD credentials for identification and authentication, (iii) perform an exit interview that includes a discussion of information security topics relevant to the agency, its mission and business requirements, and individual being terminated, including non-disclosure agreements, (iv) retrieve and retain access to all agency information and security-related or information system-related property, including laptops, monitors, printers, smartphones, jetpacks, hard tokens, keys, and ID badges, and (v) notify agency personnel within one (1) business day upon termination of the employee, including ETSS enterprise support teams, agency technical support team, and system administrators, as appropriate. Employees that are terminated for cause will immediately be escorted out of agency premises.

4.4. \[IAL1, IAL2\] Personnel Transfer (PS-5). Upon reassignment or transfer to other agency positions, the agency will (i) review and confirm ongoing operational needs for current logical and physical access authorizations to information systems and facilities, (ii) initiate transfer or reassignment actions, (iii) modify access authorizations, as required, to
correspond with any changes in operational needs, and (iv) notify designated agency personnel within one (1) business day.

4.5. [IAL1, IAL2] Access Agreements (PS-6). Prior to granting information system access, the agency will (i) document access agreements for agency information systems, (ii) review and update access agreements annually, and (iii) require individuals needing access to sign appropriate access agreements prior to being granted access and re-sign the access agreements annually to maintain access to agency information systems. Access agreements should require that individuals signing the agreement acknowledgement that they have read, understand, and agree to abide by the constraints of the agreement, as well as indicate the penalties for non-compliance.

4.6. [IAL1, IAL2] Third-Party Personnel Security (PS-7). The agency will (i) establish personnel security requirements, including security roles and responsibilities for third-party providers, (ii) require third-party providers to comply with personnel security policies and procedures established by the agency, (iii) document personnel security requirements; explicitly include personnel security requirements in acquisition-related documents, (iv) require third-party providers to notify the agency of any personnel transfers or terminations of third-party personnel who possess agency credentials or badges, or who have information system privileges, within three (3) business days, and (v) monitor provider compliance. Third-party providers include contractors and other organizations providing information system development, IT services, outsourced applications, and network or security management.

4.7. [IAL1, IAL2] Personnel Sanctions (PS-8). The agency will (i) employ a formal sanctions process for individuals failing to comply with established information security policies and procedures and (ii) notify designated agency personnel and system administrators, as appropriate, a minimum of one (1) day prior to initiating a formal employee sanctions process, identifying the individual sanctioned and the reason for the sanction.

5. Approval / Review Signature

[Signature]
Digitally signed by Brian Tardiff
Date: 2021.10.25 12:33:39 -04'00'

Chief Information Security Officer