GOVERNANCE

This document is governed by the IT Governance policy which provides the following guidance:

a. Roles and Responsibilities
b. Policy Control Application
c. Policy Compliance Requirements
d. Policy Exceptions and Exemptions
e. Policy Reviews and Updates

SCOPE

This policy covers all State information and information systems to include those used, managed, or operated by a contractor, an agency, or other organization on behalf of the State. This policy applies to all State employees, contractors, and all other users of State information and information systems that support the operation and assets of the State.

PS-1 POLICY AND PROCEDURES

All information assets that process, store, receive, transmit or otherwise could impact the confidentiality, integrity, and accessibility of State data must meet the required security controls defined in this policy document based on the National Institute of Standards and Technology (NIST) SP 800-53, r5 Security and Privacy Controls. This addresses the requirements set forth by the State to implement the family of Personnel Security controls at the organization, process, and/or system level for all information assets/State data.

The State has adopted the security principles established in NIST SP 800-53, “Personnel Security” control guidelines as the official policy for this security domain. The “PS” designator identified in each section represents the NIST-specified identifier for the Personnel Security control family. A designator followed by a number in parenthesis indicates a control enhancement that provides statements of security and privacy capability that augment a base control. Only those control enhancements associated with the moderate level controls are listed. Should an executive-branch agency be required to address other control enhancements for a control item, the organization will be responsible for writing an additional policy to meet that requirement.

The following subsections outline the Personnel Security requirements each agency must implement and maintain to remain compliant. This policy and associated procedures shall be reviewed and updated at least every three (3) years, or as State-defined events require more frequent review and update.

PS-2 POSITION RISK DESIGNATION

The State and executive-branch agencies shall assign information security responsibilities as an integral part of each organization’s information security program. Information security policy and job descriptions should provide guidance on security roles and responsibilities within the organization.

A risk designation shall be assigned to all system user positions individually, and an established screening criteria will be used for personnel posted to those positions. Risk designations shall not be assigned at a single level for all personnel; some positions will be riskier than others.

Focused security positions including, but not limited to, security analysts, system custodians, system administrators, and managers with focused security responsibilities shall have the following areas

considered:

a. Identify and clearly define assets and security processes associated with each system for which the position holder will be held responsible;
b. Clearly define and document authorization levels necessary for the position holder to make enhancements, modify source code, and promote updated code; and
c. Detailed description of manager/custodian responsibilities with an annual review/revision or as required by vacancy or position description/scope change.

PS-3 PERSONNEL SCREENING

Personnel screening activities shall reflect applicable federal or State laws, regulations, policies, standards, guidance, and specific criteria established for the risk designations of assigned positions, including:

a. Background investigations of individuals prior to authorizing access to State information and systems;
b. Rescreening of individuals as needed and in compliance with the State's personnel screening procedures; and
c. Ensuring screening is consistent with the risk designation of the position and complies with policies, regulations, and guidance provided by the State and/or federal partners.

PS-4 PERSONNEL TERMINATION

Upon personnel termination, the State shall:

a. Disable information system access within three (3) business days upon notification of termination.
b. Disable user credentials within three (3) business days upon the account owner's termination or when they no longer need system or application access due to a leave of absence or temporary reassignment.
c. Conduct exit interviews to ensure terminated individuals understand the security constraints imposed on former employees and that proper accountability is achieved for information system-related property.
d. Exit interviews shall include, at a minimum, a discussion of nondisclosure agreements (NDAs) and potential limitations on future employment. Exit interviews may not be possible for some terminated individuals.
e. Retrieve all organizational information system-related property including keys, identification badges, State or agency-owned mobile devices including laptops, tablets, cellular phones, and hardware authentication tokens.
f. Ensure appropriate personnel retain access to data stored on a departing employee's information system.
g. Notify the organization's help desk, security office, security guard, and the individual's manager immediately upon notification of termination of an individual or when there is the need to disable the information system accounts of the individual being terminated prior to being notified.

PS-5 PERSONNEL TRANSFER

Information systems facilities access authorizations shall be reviewed and confirmed when personnel are reassigned or transferred to other positions within the State with the following required actions:

a. Returning old and issuing new keys.
b. Issuing identification badges
c. Closing old accounts and establishing new accounts.
d. Changing system access authorizations.
e. Providing access to data and accounts created or controlled by the employee at the previous work location.
f. Notify agency personnel as required.

PS-6 ACCESS AGREEMENTS

All personnel will complete and sign access agreements prior to being authorized and granted access to information and information systems. The agreements shall be reviewed, updated, and acknowledged at least annually to maintain access to information and information systems, or when access agreements change. Access agreements should include Non-Disclosure Agreements (NDAs), acceptable use, facility use, and conflict of interest agreements. The agreement must be clear that the individual signing acknowledges they have read, understand, and agree to abide by the access constraints.

Securely generated electronic signatures (e.g., Adobe Sign, DocuSign, etc.) are acceptable for acknowledging access agreements unless specifically prohibited by agency policy.

All State employee badge authorizations shall be reviewed at least monthly to verify the correct level of facility access for each employee and shall be conducted by the employee’s manager and/or appropriate director.

PS-7 EXTERNAL PERSONNEL SECURITY

Personnel security requirements shall be established, documented, and disseminated, including security roles and responsibilities for third-party providers.

a. Third-party providers include vendors, suppliers, service bureaus, contractors, interns, and other organizations providing information system development, information technology services, outsourced applications, and network and security management.
b. External providers shall comply with State personnel security policies and procedures and shall be fully accountable to the State for any actions during their assignments.
c. Agency staff overseeing external providers' work shall be responsible for communicating and enforcing applicable laws, as well as State and agency security policies and procedures.
d. Nondisclosure statements shall be signed by authorized representatives of the external provider before any information technology services are delivered.
e. State operational and/or restricted information must not be released to external providers without properly executed contracts and confidentiality agreements. These contracts must specify conditions of use, security requirements, and the access, roles, and responsibilities of the third party before access is granted.
f. Access must be granted to external provider users only when required for performing work and

with the full knowledge and prior approval of the information asset owner.

g. All new connections between external providers and State agencies shall be documented in an agreement, including information technology security requirements for the connections.
h. The agreement shall be signed by an agency employee who is legally authorized to sign on behalf of the agency and by a representative from the external provider who is legally authorized to sign on behalf of the external provider. The signed document must be kept on file with the relevant group.
i. External providers shall notify designated State personnel within 48 hours of any transfers or terminations of external provider personnel possessing organizational credentials, badges, or information system privileges.
j. Agencies shall define the transfers and terminations deemed reportable by security-related characteristics, including but not limited to functions, roles, and credentials/privileges associated with transferred individuals.
k. Contracts with external providers providing offsite hosting or cloud services shall require the external provider to provide the State with an annual independent risk assessment report.
l. The State shall monitor external provider compliance with personnel security requirements.

PS-8 PERSONNEL SANCTIONS

A formal sanctions process shall be used for personnel, contractors or other third parties failing to comply with established information security policies and procedures.

a. Notify OIT Personnel Management *as soon as possible* when a formal employee sanctions process is initiated, identifying the individual sanctioned and the reason for the sanction.
b. Ensure that the sanctions process is consistent with the State Personnel Progressive Disciplinary Process.

PS-9 POSITION DESCRIPTIONS

Security and privacy roles and responsibilities shall be incorporated into State and executive-branch position descriptions.

POLICY OWNER

Secretary of Office of Information Technology (OIT)

MATERIAL SUPERSEDED

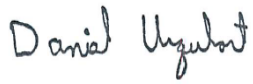
This current policy supersedes all previous versions. All State agencies and contractors/vendors of the State are expected to comply with the current implemented version.

REVISION HISTORY

Revision Date	Summary of Change
12/31/2024	Policy Update

REMAINDER OF PAGE LEFT INTENTIONALLY BLANK

APPROVED BY

Signature	
Approved by	Daniel Urquhart
Title	Secretary of Office of Information Technology (OIT)
Date Approved	01/15/2025

REMAINDER OF PAGE LEFT INTENTIONALLY BLANK