State of Maryland

STANDARD

PERSONNEL SECURITY

Document No.	Last Updated	Prepared By
MD-STD-314-PS-01	02/18/2026	DOIT OSM

Personnel security is a critical aspect of managing security risks by ensuring individuals with access to systems and data are properly vetted, continuously monitored, and managed through strict identity verification, least-privilege enforcement, and adaptive access controls throughout the employment lifecycle.

PURPOSE AND SCOPE

Purpose	This standard provides the technical and operational specifications needed to manage personnel security measures that protect organizational assets, operations, and information.
Scope	This standard is designed to help agencies implement and oversee cybersecurity and privacy programs at the strategic level.
Applicability	This standard applies to all units of State government (as defined in SF&P 3.5-101(g)), hereafter referred to simply as "agencies."
Related Policy	This standard is part of a broader policy suite. Refer to MD-POL-100 Cybersecurity & Governance Policy, Appendix C for a list of related policies and standards.
Baseline	This standard has been developed using National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 Revision 5 Moderate Baseline[1] and State-specific organizationally defined parameters. Agencies may be required to deviate from this baseline when State statute, executive orders, or applicable regulations establish a conflicting requirement that precludes compliance.
Distribution	This document is approved for public distribution and may be shared with external stakeholders, partners, and regulatory bodies. It reflects the State's commitment to transparency, compliance, and operational excellence. Unauthorized modifications or misrepresentation of this document are strictly prohibited.

[1] NIST SP 800-53 Rev. 5: Security and Privacy Controls for Information Systems and Organizations.

FOREWORD

Agencies that use Department of Information Technology DoIT-managed services automatically receive, or *inherit*, the compliance those services already meet, reducing duplicative work and accelerating their overall compliance efforts. These centrally governed services, such as hosting platforms, identity management, and network infrastructure, are built with robust control frameworks that automatically extend to participating agencies. By leveraging these offerings, agencies not only align with key operational and security standards but also benefit from pre-configured environments, continuous monitoring, and policy enforcement mechanisms maintained by DoIT. Agencies are encouraged to leverage these services to accelerate readiness, gain cost efficiency, simplify compliance efforts, and allow agencies to focus more fully on mission delivery, knowing that foundational requirements are already in place. Agencies should review the scope of each managed service to understand which standards are inherited and where additional agency-specific controls may still be required.

GUIDANCE AND ENFORCEABILITY

Throughout this document, informational call-out boxes are utilized to provide additional context or elaborate on key topics. While these boxes primarily serve an informational purpose, any directives or mandated actions contained within them are authoritative and carry the same enforceability as the core requirements of this document. For the purposes of this document, the term “shall” denotes a mandatory requirement. Terms such as “where feasible”, “encouraged”, or similar phrasing indicate recommended practices that reflect organizational preference but are not enforceable requirements at this time.

CHANGE RECORD

Version	Summary of Changes	Changed By	Date
1.0	Initial Publication	Miheer Khona	02/18/2026

STANDARDS

314 State Strategy

These standards establish a baseline of personnel security lifecycle management activities that each agency must implement to comply with State cybersecurity and privacy policies. Each agency shall designate specific personnel with IT responsibilities to ensure the effective implementation of these standards.

314-1 Develop Agency-Level Procedures (PS-1)

In alignment with this standard, develop and document agency-level personnel security procedures. Agencies must disseminate the procedures to agency personnel with information technology (IT) security responsibilities. Agencies must review and, if needed, update the procedures based on changes and risk at least every **3 years**. At a minimum, the procedures must address purpose, scope, roles and responsibilities, and guidelines.

314-2 Position Risk Designation (PS-2)

Assign a risk designation to all agency positions. Establish screening criteria for individuals filling those positions. Review and update position risk designations at least **annually**.

Risk Designation

The approach to position risk designation can vary across agencies depending on mission scope, regulatory obligations, and operational context. For example, Maryland Department of Health may prioritize Health Insurance Portability and Accountability Act (HIPAA) compliance and require Tier 2 or Tier 3 background checks for roles accessing protected health information, while the DoIT might emphasize system access and cybersecurity posture, aligning designations with NIST or Criminal Justice Information Services (CJIS) standards. Similarly, education and public safety agencies may incorporate fingerprinting or child welfare screenings based on statutory mandates. Despite these differences, the common denominator across agencies is the sensitivity of the systems and data involved.

314-3 Personnel Screening (PS-3)

Screen individuals (e.g., background checks for criminal history) prior to authorizing access to the system and rescreen individuals when changes in role, assignments, or duties introduce new or elevated risk designations, or at least every **3 years**.

314-4 Personnel Termination (PS-4)

Upon termination or separation of an individual's employment agencies shall:

- Disable system access immediately upon termination notification, not to exceed **2 hours**;
- Terminate or revoke any authenticators and credentials associated with the individual;
- Conduct exit interviews that include a reminder to individuals of nondisclosure agreements and potential limitations on future employment (if any);
- Retrieve all security and system-related State or agency property; and
- Retain access to organizational information and systems formerly controlled by the terminated/separated individual.

314-5 Personnel Transfer (PS-5)

Review and confirm ongoing operational need for current logical and physical access authorizations to systems and facilities when individuals are reassigned or transferred to other positions within the organization. Initiate any required transfer or reassignment actions (e.g., returning old and issuing new keys, identification cards, and building passes; closing system accounts and establishing new accounts; changing system access authorizations) within **48 hours** of the formal transfer action. Modify access authorization as needed to correspond with any changes in operational need due to reassignment or transfer and notify impacted personnel upon completion of the transfer.

314-6 Access Agreements (PS-6)

Develop and document access agreements for organizational systems. Review and update the access agreements at least **annually**. Verify that individuals who require access to organizational information and systems: a) Sign appropriate access agreements prior to being granted access; and b) Re-sign access agreements to maintain access to organizational systems when access agreements have been updated or on an **annual** basis.

Access Agreement vs Acceptable Use Policy

An access agreement is specific to a system being accessed and ensures individuals understand and formally acknowledge their responsibilities before accessing the system. An acceptable use policy (AUP) defines what users can and cannot do when accessing any organizational system. As part of the onboarding process, all users must review and formally acknowledge both the system-specific access agreement (if applicable) and the State Acceptable Use Policy (AUP) before any access is granted.

314-7 External Personnel Security (PS-7)

Establish and document personnel security requirements, including security roles and responsibilities for external providers. Require external providers to comply with personnel security policies and procedures established by the agency. Require external providers to notify agency personnel of any personnel transfers or terminations of external personnel who possess State credentials and/or badges **immediately** upon termination or separation, or who have system privileges prior to transfer or termination. Monitor provider compliance with personnel security requirements.

314-8 Personnel Sanctions (PS-8)

All personnel actions, sanctions, and related employment determinations shall be governed by and deferred to the Maryland Department of Budget and Management (DBM) Office of Human Resources.

314-9 Position Descriptions (PS-9)

Incorporate security and privacy roles and responsibilities into organizational position descriptions.

GUIDELINES

ID	Title	Description	Source
CSF Tools	Cyber Security Framework Tools	This website provides supplemental guidance for each security control listed in this document.	*csf.tools (LINK)*

DEFINITIONS

Each unique term used in this standard is defined in the **State of Maryland Cybersecurity & Privacy Glossary**.

COMPLIANCE CHECKLIST

ID	Standard	Compliance
314-1	**Develop Agency-Level Procedures (PS-1)**	☐ Yes ☐ No
314-2	**Position Risk Designation (PS-2)**	☐ Yes ☐ No
314-3	**Personnel Screening (PS-3)**	☐ Yes ☐ No
314-4	**Personnel Termination (PS-4)**	☐ Yes ☐ No
314-5	**Personnel Transfer (PS-5)**	☐ Yes ☐ No
314-6	**Access Agreements (PS-6)**	☐ Yes ☐ No
314-7	**External Personnel Security (PS-7)**	☐ Yes ☐ No
314-8	**Personnel Sanctions (PS-8)**	☐ Yes ☐ No
314-9	**Position Descriptions (PS-9)**	☐ Yes ☐ No

Note: When assessing the implementation and effectiveness of the security and privacy controls outlined in this standard, DoIT recommends the use of NIST SP 800-53A Rev. 5, to perform evaluations in a manner that is evidence-based, repeatable, and aligned with the system's documented security posture.