State of Maryland

STANDARD

PLANNING

Document No.	Last Updated	Prepared By
MD-STD-312-PL-01	02/18/2026	DOIT OSM

Cybersecurity planning, as a foundational element of Zero Trust Architecture (ZTA), is necessary to align security objectives with business goals and regulatory requirements, enforcing continuous verification, least privilege access, and adaptive security controls to mitigate evolving threats.

PURPOSE AND SCOPE

Purpose	This standard provides the technical and operational specifications needed to establish a structured approach to strategic planning.
Scope	This standard provides an organizational approach for establishing a structured approach to security and privacy.
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

312 State Strategy

These standards establish a baseline of cybersecurity planning practices 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.

312-1 Develop Agency-Level Procedures (PL-1)

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

312-2 Develop System Security and Privacy Plans (PL-2)

Develop system security and privacy plans, either as a combined plan or as two separate documents:

- Explicitly define the security architecture using system diagrams and data flow diagrams;
- Describe the operational context of the system in terms of mission and business processes;
- Identify the individuals who fulfill system security roles and responsibilities;
- Leverage the Digital Identity Risk Assessment (DIRA) Playbook[2] as a guide for evaluating identity-related risks;
- Identify the information types processed, stored, and transmitted by the system;
- Provide the security categorization of the system, including supporting rationale;
- Describe any specific threats to the system that are of concern to the organization;
- Provide the results of a privacy risk assessment for systems processing personally identifiable information (PII);
- Describe the operational environment for the system and any dependencies or connections to other systems or system components;
- Provide an overview of the security and privacy requirements for the system;

[2] DIRA Playbook: https://www.idmanagement.gov/playbooks/dira/

- Identify any relevant control baselines or overlays, if applicable;
- Describe the controls in place or planned for meeting the security and privacy requirements, including a rationale for any tailoring decisions;
- Include relevant privacy threshold analysis (PTA) and privacy impact assessment (PIA) required by the State Chief Privacy Officer (SCPO);
- Include risk determinations for security and privacy architecture and design decisions;
- Include security and privacy-related activities affecting the system that require planning and coordination with the State Chief Information Security Officer (SCISO), SCPO, and State Chief Data Officer (SCDO); and
- Obtain review and approval by the agency's designated Senior Executive or Authorizing Official (AO) prior to plan implementation.

Distribute copies of the plans and communicate subsequent changes to the plans to the SCISO, agency's designated Senior Executive, and AO. Review the plans at least **annually** or upon significant system changes whichever occurs first. Update the plans to address changes to the system or environment and problems identified during plan implementation, or control assessments. Protect the plans from unauthorized disclosure and modification.

312-3 Establish Rules of Behavior (PL-4)

Provide the MD-POL-203 Acceptable Use Policy (AUP) and any system specific rules of behavior (if applicable) to individuals requiring access to any State system to describe their responsibilities and expected behavior for information and system usage, security, and privacy. Receive a documented acknowledgment of the AUP from such individuals, indicating that they have read, understand, and agree to abide by the rules of behavior, before authorizing access to information and the system. Require individuals who have acknowledged a previous version of the rules of behavior to read and re-acknowledge when the rules are revised or updated. The AUP is reviewed and updated **annually** by DoIT.

PL-4(1): The AUP outlines required behaviors and prohibited actions to ensure responsible use of State IT resources and protection of State data.

Develop Security and Privacy Architectures (PL-8)

Develop security architectures for each information system (i.e., existing, planned, and newly acquired) that:

- Describe the requirements and approach to be taken for protecting the confidentiality, integrity, and availability of State information;

- Describe the resiliency measures required (e.g., redundant, diverse, and tested recovery mechanisms) to ensure continuity of critical functions under adverse conditions, including hardware failures, cyberattacks, and loss of primary services;
- Describe the requirements and approach to be taken for personal information to minimize privacy risk to individuals;
- Describe how the security and privacy architectures are integrated into and support the enterprise architecture;
- Incorporate ZTA measures such as micro-segmentation, identity-based access controls, and automated threat detection where feasible;
- Include privacy by design principles and controls that support applicable Fair Information Practice Principles (FIPP); and
- Describe any assumptions about, and dependencies on, external systems and services.

Fair Information Privacy Practices

The FIPP[3] are a foundational framework for privacy and data protection, originally developed in the 1970s and widely adopted across government and industry. They guide how organizations should collect, use, and manage personal information responsibly using the following principles: a) Transparency (Notice); b) Individual Participation (Access); c) Purpose Specification; d) Data Minimization; e) Use Limitation; f) Security Safeguards; g) Accountability; h) Data Quality; and i) Integrity.

Review and update the security and privacy architectures at least **annually** to reflect changes in the enterprise architecture. Update the System Security Plan (SSP), privacy plans, and any associated PTA or PIA to reflect changes to systems, processes, or regulations. Ensure all related documentation (e.g., concept of operations, business impact analysis, organizational procedures, and acquisitions) is updated accordingly.

312-4 Baseline Selection (PL-10)

Select a control baseline for each system by determining the system's impact level, High, Moderate, or Low, based on the potential adverse effects on confidentiality, integrity, and availability.

[3] Fair Information Practice Principles (FIPPs) | FPC.gov

High Water Mark

Federal Information Processing Standard Publication 199 (FIPS 199) provides a standardized approach for categorizing systems based on the potential consequences of a security breach. The process begins by identifying the types of information processed, stored, or transmitted by the system. For each information type, assess the potential impact of a loss of confidentiality, integrity, and availability using the categories Low, Moderate, or High. These assessments should consider organizational mission, legal obligations, and potential harm to individuals or operations. The final impact level of the system is set using the high-water mark principle, meaning the highest impact rating among the three security objectives becomes the overall system categorization. Supporting resources like NIST SP 800-60 provide mappings between information types and impact levels to guide this process.

312-5 Baseline Tailoring (PL-11)

Tailor the selected control baseline by determining and documenting in the system security plan:

- Controls that are inapplicable and therefore removed;
- Compensating controls where the control is impractical and an equivalent alternative exists;
- Organizationally defined parameters within each control, that are specific to the agency;
- Common controls that are inheritable from enterprise level systems or shared services; and
- Supplemental controls that are added for unique threats or compliance requirements such as overlays.

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)*
NIST SP 800-37	Risk Management Framework (RMF) for Information Systems and Organizations.	This document provides guidance on how to perform adequate planning (Reference RMF Step 0).	*csrc.nist.gov (LINK)*
NIST SP 800-61	Risk Management Framework for Privacy,	A tool for improving privacy through an enterprise risk management program.	*nist.gov (LINK)*

DEFINITIONS

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

COMPLIANCE CHECKLIST

ID	Standard	Compliance
312-1	**Develop Agency-Level Procedures (PL-1)**	☐ Yes ☐ No
312-2	**System Security and Privacy Plans (PL-2)**	☐ Yes ☐ No
312-3	**Rules of Behavior (PL-4)**	☐ Yes ☐ No
312-4	**Security and Privacy Architectures (PL-8)**	☐ Yes ☐ No
312-5	**Baseline Selection (PL-10)**	☐ Yes ☐ No
312-6	**Baseline Tailoring (PL-11)**	☐ 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.