State of Maryland

STANDARD

MEDIA PROTECTION

Document No.	Last Updated	Prepared By
MD-STD-310-MP-01	02/18/2026	DOIT OSM

Media Protection is important for safeguarding both digital and non-digital media from unauthorized access, loss, or misuse by enforcing strict access controls, continuous monitoring, and encryption to preserve data integrity and security.

PURPOSE AND SCOPE

Purpose	This standard provides the technical and operational specifications needed to protect the confidentiality, integrity, and availability of State Data stored on various media formats.
Scope	This standard addresses the handling, storing, transporting, and disposing of media.
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

310 State Strategy

These standards establish a baseline of media protection 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.

310-1 Develop Agency-Level Procedures (MP-1)

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

310-2 Restrict Media Access (MP-2)

Restrict access to digital and non-digital media to authorized users through an approved access list. Enforce role-based access control (RBAC), based on the principle of least privilege, and multi-factor authentication (MFA) for media access where possible.

Principle of Least Privilege

The principle of least privilege is a foundational security concept in IT that ensures users, systems, and applications are granted only the minimum level of access necessary to perform their specific tasks. By limiting permissions to the bare essentials, organizations reduce the attack surface and mitigate the risk of accidental or malicious misuse of data and resources. This approach aligns with Zero Trust Architecture (ZTA) principles by enforcing granular access policies. Implementing this principle involves regularly auditing roles, refining access controls, and using automation to adjust privileges dynamically based on behavior, context, or job function changes.

310-3 Apply Media Marking (MP-3)

Mark system media indicating the distribution limitations, handling caveats, and applicable security markings (if any) of the information in strict alignment with the State Data Classification Policy. Media that contain only public data may be exempted from marking if the media remains within an agency-controlled area.

310-4 Secure Media Storage (MP-4)

Physically control and securely store digital and non-digital media within agency-controlled areas using approved access control lists. Protect all media that contains State data until the media are destroyed or sanitized using approved equipment, techniques, and procedures.

Safeguarding Stored Assets

Data-at-rest encryption refers to the process of encrypting digital information while it is stored on physical media (e.g., hard disk drives (HDDs), solid state drives (SSDs), tapes, or cloud-based object storage). This applies to block storage (e.g., storage area network (SAN), network attached storage (NAS)), object storage (e.g., Amazon Simple Storage Service (S3), Azure Blob), file systems, backup tapes, and removable drives. Ensure adequate strength of encryption consistent with the State's minimum standards defined in MD-STD-318-SC System & Communication Protection Standard, Section 318-6.

310-5 Control Media Transport (MP-5)

Protect and control digital and non-digital media during transport outside of controlled areas using agency-established safeguards (e.g., minimum encryption standards as defined in MD-STD-318-SC, Section 318-6). Maintain accountability for system media during transport outside of controlled areas. Document activities associated with the transport of system media. Restrict the activities associated with the transport of system media to authorized personnel.

State data in hardcopy or removable media must not be removed from agency premises without prior authorization from the appropriate Authorizing Official (AO).

Traveling outside the United States and its Territories with State equipment must be pre-approved. Requests may be denied due to elevated cybersecurity risk conditions, U.S. export laws or import restrictions enforced by the destination country. For approved requests, a set of security configuration requirements and post-travel requirements will be defined and shall be adhered to.

310-6 Perform Media Sanitization (MP-6)

Sanitize digital and non-digital media prior to disposal, release out of organizational control, or release for reuse, using sanitization techniques and procedures consistent with the *NIST Special Publication 800-88 Guidelines for Media Sanitization*. Employ sanitization mechanisms with the strength and integrity commensurate with the security category or classification of the information.

For cloud services, agencies must verify that the cloud provider uses acceptable methods to prevent State data remanence (e.g., strong contractual language that ensures data deletion, letters of attestation).

Restrict Media Use (MP-7)

Restrict the use of removable media on all workstations and mobile devices using agency-approved technical safeguards (e.g., device control software, group policy, data loss prevention tools) and non-technical safeguards (asset ownership registry, procurement controls); and Prohibit the use of portable storage devices in organizational systems when such devices have no identifiable owner.

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 800-88	Guidelines for Media Sanitization	This document provides guidelines for media sanitization, ensuring that non-pubilc data is securely erased or destroyed before media is reused or disposed of.	*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
310-1	**Develop Agency-Level Procedures (MP-1)**	☐ Yes ☐ No
310-2	**Restrict Media Access (MP-2)**	☐ Yes ☐ No
310-3	**Apply Media Marking (MP-3)**	☐ Yes ☐ No
310-4	**Secure Media Storage (MP-4)**	☐ Yes ☐ No
310-5	**Control Media Transport (MP-5)**	☐ Yes ☐ No
310-6	**Perform Media Sanitization (MP-6)**	☐ Yes ☐ No
310-7	**Restrict Media Use (MP-7)**	☐ 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.