Division of Enterprise Technology Strategy and Services

ETSS Policy 300.10

Media Protection Policy (MP)

Publish Date: 23 June 2026
Effective Date: 23 June 2026
Last Review: 22 June 2026

doa.entsec@doit.ri.gov

1. Purpose

This policy establishes enterprise requirements for the protection of information stored on digital and non-digital media throughout its lifecycle. It defines controls for media access, marking, storage, transport, sanitization, and use to protect the confidentiality, integrity, and availability of State information. This policy reflects a cloud-first and Zero Trust security posture, emphasizing enterprise-managed controls, data classification, encryption, and minimization of physical media wherever feasible.

This policy supports the State's compliance with NIST SP 800-53 Revision 5 (Media Protection family), NIST SP 800-88 (Guidelines for Media Sanitization), NIST Cybersecurity Framework 2.0, IRS Publication 1075, and other applicable federal and state regulatory requirements.

2. Applicability

This policy applies to all State of Rhode Island Executive Branch departments, including agencies, boards, and commissions, as well as their employees (permanent, non-permanent, full-time, and part-time), interns, consultants, contractors, vendors, and any entity that has access to State information systems and data, whether operated or maintained by the State or on behalf of the State. For the purposes of this policy, the term "Agency" refers to any department, agency, division, or unit of the Executive Branch.

This policy applies to all digital and non-digital media that stores, previously stored, or may store State information, including internal and external hard disk drives, solid state drives, flash storage, optical media, magnetic media, paper documents, and microfilm.

3. Roles and Responsibilities

3.1. Chief Information Security Officer (CISO)

Responsible for enterprise-level media protection policy oversight, approval of exceptions for non-State media connections, security review of sanitization procedures, and coordination of incident response for media-related security events. Provides oversight and guidance to ensure consistent application of media access restrictions across the enterprise.

3.2. Chief Data and Analytics Officer (CDAO)

Responsible for enterprise data classification and labeling strategy, including the

implementation and governance of Microsoft Purview Information Protection sensitivity labels that support media marking requirements.

3.3. System Owners

Responsible for implementing media protection controls for their information systems, authorizing media transport outside controlled areas, ensuring media sanitization is performed prior to disposal or reuse, maintaining media sanitization logs, and enforcing media use restrictions within their system boundaries.

3.4. ETSS Infrastructure and Operations (I&O)

Responsible for performing or overseeing media sanitization activities, managing enterprise endpoint device control mechanisms that restrict unauthorized removable media, coordinating with DCAMM on surplus and disposal procedures, and maintaining enterprise-approved sanitization equipment.

3.5. Agency Technical Support Managers (TSMs) / Agency Information Managers (AIMs)

Responsible for coordinating media protection activities at the agency level, ensuring agency compliance with media marking, storage, and sanitization requirements, and reporting media-related security concerns to ETSS.

3.6. All Personnel

Responsible for handling media in accordance with its classification and marking, reporting lost or stolen media immediately, refraining from connecting unauthorized media to State systems, and following established sanitization procedures before disposing of or releasing any media containing State information.

4. Procedures for Compliance

The following requirements establish the media protection controls that agencies and ETSS must implement. Security controls are assigned based on the Information Assurance Level (IAL) of the information system, aligned to the NIST SP 800-53 Rev. 5 Moderate baseline.

4.1. Media Protection Policy and Procedures (MP-1)

Applies to: All systems (IAL1, IAL2)

Each agency shall develop, document, disseminate, and review system-specific media protection procedures consistent with this enterprise policy and the applicable System Security Plan (SSP). The policy shall be reviewed and updated at least every three (3) years and following significant changes to technologies, regulatory requirements, or the threat environment. Supporting procedures shall be reviewed in alignment with the policy.

4.2. Media Access (MP-2)

Applies to: All systems (IAL1, IAL2)

Access to media containing non-public information shall be restricted to authorized personnel with a documented business need. Logical access controls, role-based access control (RBAC), and enterprise identity systems shall be used where applicable. Access to portable media (such as USB drives) shall be restricted to read-only access without prior approval for write access. Unauthorized access to system

media is prohibited and subject to investigation in accordance with incident handling and response procedures.

4.3. Media Marking (MP-3)

Applies to: Moderate and above (IAL2)

Media containing non-public information shall be marked or logically labeled to reflect data classification, handling requirements, and distribution limitations in alignment with the ETSS Data Classification Policy (400.1). Each agency shall:

a. Implement digital media marking through enterprise data classification and labeling tools, specifically Microsoft Purview Information Protection. Purview sensitivity labels shall be applied to indicate data classification, required handling and protection requirements, and distribution limitations. Labels persist throughout the data lifecycle and are enforced through integrated enterprise controls including encryption, access restrictions, and policy-based protections.

b. Physically mark non-digital media where feasible to indicate sensitivity and handling requirements when media is stored, transported, or accessed outside of secured environments.

Additional physical marking is not required when media remains within ETSS-defined controlled facilities and logical, physical, and administrative safeguards sufficiently protect the media. If media is removed from controlled areas, appropriate marking requirements apply.

4.4. Media Storage (MP-4)

Applies to: Moderate and above (IAL2)

Each agency shall ensure that media containing non-public information is securely stored:

a. Digital media shall be encrypted using FIPS 140-2, FIPS 140-3 validated, or similar cryptographic modules, stored within enterprise-approved systems or cloud services, and protected using access controls and monitoring mechanisms.

b. Non-digital media shall be stored in locked cabinets, rooms, or containers within controlled areas, with access limited to authorized personnel.

c. Media shall be protected until it is destroyed or sanitized in accordance with ETSS policies, procedures, and standards. Media is not released for reuse, disposal, or removal from organizational control until sanitization requirements are met.

4.5. Media Transport (MP-5)

Applies to: Moderate and above (IAL2)

Each agency shall:

a. Protect and control media containing non-public data when transported outside of controlled areas. At a minimum, media containing sensitive or confidential data shall be: encrypted using a FIPS 140-2, FIPS 140-3 validated, or similar encryption module; transported using tamper-proof packaging (such as a locked container or sealed envelope); if hand-carried, secured within a secure container by authorized personnel; and if shipped, provided a trackable receipt from a commercial carrier.

b. Maintain accountability for media containing non-public data during transport outside

of controlled areas. Use chain-of-custody documentation or similar records that demonstrate physical possession of the media at every stage of the transport process.

c. Document activities associated with the transport of media through enterprise or agency processes such as ServiceNow tickets, chain-of-custody records, or notes within asset tracking systems.

d. Restrict the transport of media to authorized personnel with a documented business need. Authorization shall be granted by the System Owner and enforced in coordination with ETSS Enterprise Support teams.

3.6. Media Sanitization (MP-6)

Applies to: All systems (IAL1, IAL2)

Each agency shall:

a. Sanitize media containing non-public data prior to disposal, reuse, or release out of agency control using techniques and procedures aligned to NIST SP 800-88. This includes media that at any point during its lifecycle contained non-public data without certification of prior sanitization, media requested as part of an investigation or audit, and media under vendor warranty prior to exchange.

b. Employ an ETSS-approved sanitization method appropriate for and commensurate with the security requirements, media operability, and sensitivity of the data. Approved methods include overwriting (minimum three passes for rotating disk storage), degaussing (for magnetic media), and physical destruction (shredding to a maximum particle size of 1mm x 5mm for non-digital media, or pulverization or incineration as appropriate). Solid state and flash media shall be overwritten or physically destroyed; degaussing is not effective on non-magnetic media.

c. Validate media prior to final disposition to ensure data has been erased and no meaningful data is recoverable.

d. Maintain a media sanitization log for final disposition that includes name and agency of the individual authorizing sanitization, name and agency of the individual performing sanitization, date media received, media description and control number, description of contents, sanitization method used, disposition following sanitization, and date of disposition.

e. Ensure that third-party providers contracted to sanitize media are certified by the National Association for Information Destruction (NAID) or adhere to the requirements of this policy.

f. Dispose of electronic equipment in accordance with the Division of Capital Asset Management and Maintenance (DCAMM) surplus policies and standards.

3.7. Media Use (MP-7)

Applies to: All systems (IAL1, IAL2)

Each agency shall:

a. Establish media use restrictions for accessing and connecting media to information systems and system components. Media and storage devices that are not owned by the State or approved as part of an asset reviewed via the ETSS governance process are prohibited from connecting to the State network, devices, equipment, or information systems without prior formal written authorization from the system owner and ETSS CISO. Endpoint protection and device control mechanisms shall be used to monitor or limit the use of unauthorized removable

media, and configuration management settings shall restrict media mounting, execution, or data transfer where feasible.

b. Prohibit the use of portable storage devices within agency information systems when the device does not have an identifiable owner. Unidentified or unapproved devices present an elevated risk of malware introduction and data exfiltration and are blocked or restricted through enterprise endpoint security controls. Any attempted use of such devices is subject to investigation in accordance with incident handling and response procedures.

5. Repercussions for Non-Compliance

Failure to comply with this policy may result in corrective action proportional to the severity of the violation. Consequences may include, but are not limited to:

a. Revocation of access to media, removable storage devices, or information systems.

b. Mandatory retraining on media protection and data handling requirements.

c. Formal counseling or written reprimand.

d. Referral to agency management and human resources for disciplinary proceedings, up to and including termination of employment.

e. Termination of vendor or contractor agreements for external provider personnel.

f. Referral to law enforcement if criminal activity, data theft, or deliberate data destruction is suspected.

Failure to properly sanitize media prior to disposal or release, or unauthorized transport of media containing classified data, may be treated as security incidents and investigated accordingly. Non-compliance findings shall be documented and tracked through ETSS governance processes and may be recorded as findings in the agency Plan of Action and Milestones (POAM).

6. Approval / Review Signatures

Sanjay Gupta
Digitally signed by Sanjay Gupta
Date: 2026.06.22 16:38:55 -04'00'

Chief Technology Officer (CTO)
Division of Enterprise Technology Strategy and Services (ETSS)

Digitally signed by Nathan Loura
Date: 2026.06.23 12:27:20 -04'00'

Chief Information Security Officer (CISO)
Division of Enterprise Technology Strategy and Services (ETSS)

Brian Tardiff
Digitally signed by Brian Tardiff
Date: 2026.06.23 12:43:37 -04'00'

Chief Digital Officer (CDO)
Division of Enterprise Technology Strategy and Services (ETSS)