State of Maryland

STANDARD

AWARENESS & TRAINING

Document No.	Last Updated	Prepared By
MD-STD-302-AT-01	02/18/2026	DOIT OSM

Cybersecurity awareness, privacy, and data management training are essential for individuals to understand the unique intersection between cybersecurity, privacy, and data to safeguard against threats, minimize risks, and enhance overall security posture of State systems.

PURPOSE AND SCOPE

Purpose	This standard reduces risk by creating an understanding of the security, privacy, and data management risks associated with individual roles that handle information defined by the State as confidential or restricted and how to properly protect this data. This standard recognizes that data governance, privacy awareness, and effective data management are central to properly protecting State systems and reducing cyber risk across State agencies.
Scope	This standard provides an organizational approach for Awareness & Training and is not specific to any single platform or training solution.
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

302 State Strategy

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

302-1 Develop Agency-Level Procedures (AT-1)

In alignment with this standard, Agencies must develop and document agency-level awareness & training procedures that take into account the enterprise-wide awareness training provided by the DoIT Office of Security Management (OSM), in collaboration with the Office of Enterprise Data (OED), as well as the agency-defined role-based training specific to each agency's unique roles and responsibilities. Agencies must disseminate the procedures to all agency staff with information technology (IT) security, privacy protection, and data management responsibilities. Agencies must review, and if needed, update the procedures as deemed appropriate by the agency based on regulatory or agency changes **at least every 3 years**. The procedures must address how the agency intends to implement the required cybersecurity, privacy, and data management training. The procedures must be approved by the agency's designated Senior Executive or Authorizing Official (AO).

302-2 Provide Awareness Training (AT-2)

Enforce completion of OSM's enterprise-wide cybersecurity, privacy, and data management training as part of initial training for new users before authorizing access to the system, or **within 30 days** of appointment, and at least **annually thereafter**.

Agencies shall supplement OSM's awareness training with agency-level training when required by system changes or following a security incident or breach of personal information with valuable lessons learned.

Agencies are strongly encouraged to take advantage of the standardized cyber training program delivered by OSM, which ensures consistency, accountability, and enterprise-wide alignment. For agencies that currently operate their own training programs, OSM will require at a minimum, submission of training materials and completion records to monitor State-wide completion.

Agency-Supplemental Awareness Training

Agencies may need to create and assign agency-specific training if: a) The agency chooses to add local operational content; b) Additional training is required to meet compliance regulatory requirements; c) Cybersecurity, privacy, or data incidents have occurred that necessitate the need to educate the workforce regarding the lessons learned; or d) Agency cybersecurity, privacy, or data management procedure changes and users must be made aware.

AT-2(2): The annual cybersecurity, privacy, and data management awareness campaign must address insider threat whether part of the State-wide mandatory campaign or agency-led campaigns and must instruct users on how to report insider threat.

Insider Threat Indicators

Potential indicators and possible precursors of insider threat can include behaviors such as: a) long-term job dissatisfaction; b) attempts to gain access to information not required for job performance; c) unexplained access to financial resources; d) bullying or sexual harassment of fellow employees; e) workplace violence; f) significant changes in behavior (i.e., work very late at night); and g) other serious violations of organizational policies, procedures, directives, rules, or practices.

AT-2(3): If the State-wide mandatory annual cybersecurity awareness campaign does not already include training on recognizing and reporting potential and actual instances of social engineering and social mining (e.g., addressing latest techniques such as QR code, MFA fatigue) provide this training as part of the supplemental training.

Social Engineering Examples

Social engineering includes phishing, pretexting, impersonation, baiting, quid pro quo, social media exploitation, and tailgating. Awareness training shall include how to communicate concerns regarding potential and actual instances of social engineering and data mining through reporting channels outlined in the MD-POL-203 Acceptable Use Policy, Section 200.1.9.

302-3 Provide Role-Based Training (AT-3)

Require all agency personnel with assigned security and privacy roles and responsibilities to complete DOIT OSM-provided role-based security training:

- Before authorizing access to any information system;
- Before performing assigned duties that may require access to non-public State data;
- When required by system changes; and
- At least **annually**, thereafter.

The training is based on assigned roles and responsibilities and the specific requirements of the agency and the information systems to which personnel have authorized access.

Agency Role-Based Training

While the State-wide general awareness training establishes baseline understanding of cybersecurity, privacy, and data management principles, agencies are required to equip users with knowledge tailored to their operational risks, roles, and system interactions. Acceptable forms of role-based training include: a) training leading to professional certifications; b) continuing education to maintain certifications; c) conference and webinar attendance related to their role or agency technology; and d) online training associated with one or more area of responsibility.

302-4 Maintain Training Records (AT-4)

OSM and OED will document and monitor information security, privacy, and data management training activities and retain individual training records for **5 years** or as required by applicable regulatory requirements. For agencies that currently operate their own training programs, OSM will require at a minimum, submission of training materials and completion records to monitor State-wide completion.

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 800-50r1	Building a Cybersecurity and Privacy Learning Program	This document provides guidance to develop and manage a life cycle approach to building a Cybersecurity and Privacy Program.	*www.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
302-1	**Develop Agency-Level Procedures (AT-1)**	☐ Yes ☐ No
302-2	**Provide Awareness Training (AT-2)**	☐ Yes ☐ No
302-3	**Provide Role-Based Training (AT-3)**	☐ Yes ☐ No
302-4	**Maintain Training Records (AT-4)**	☐ 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.