State of Maryland

STANDARD

INCIDENT RESPONSE

Document No.	Last Updated	Prepared By
MD-STD-308-IR-01	02/18/2026	DOIT OSM

Incident response enables organizations to effectively detect, mitigate, and recover from cybersecurity incidents. Incident response standards help organizations establish roles, procedures, and communication channels in advance, reducing confusion and accelerating recovery when incidents occur.

PURPOSE AND SCOPE

Purpose	This standard provides the technical and operational specifications needed to detect, respond to, and recover from security incidents.
Scope	This standard provides an organizational approach for building an incident response capability to effectively detect, respond to, and recover from security incidents.
Applicability	This policy applies to all units of State government (as defined in SF&P 3.5-101(g)), hereafter referred to simply as "agencies."
Related Policy	MD-POL-209 Incident Response Policy
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

308 State Strategy

These standards establish a baseline of incident response 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.

308-1 Develop Agency-Level Procedures (IR-1)

In alignment with this standard, develop and document agency-level incident response 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.

308-2 Provide Incident Response Training (IR-2)

Provide incident response training to system users consistent with assigned roles and responsibilities as follows:

- Within **30 days** of assuming an incident response role or responsibility or acquiring system access;
- When required by information system changes; and
- At least **annually** thereafter.

Review and update incident response training content **annually** and following security incidents. Include training about recognizing and reporting an event as a potential "privacy incident" (as defined in the MD cybersecurity and privacy glossary), not just a security event, strengthening the first line privacy defense.

308-3 Perform Incident Response Testing (IR-3)

Test the effectiveness of the incident response capability, and document test results, at least **annually** using the tests or exercises as outlined in the agency test plan. For systems deemed High Value State Systems (HVSS) via a Business Impact Analysis (BIA), agencies shall coordinate with the DoIT Office of Security Management (OSM) to determine if functional tests are required that are comprised of a Red Team Assessment or a Penetration Test.

Incident Response Exercises

Agencies may fulfill incident response testing requirements through the use of either tabletop exercises (TTXs) or functional exercises, depending on operational needs and resource availability. TTXs are facilitated, discussion-based exercises where personnel meet to discuss roles, responsibilities, coordination, and decision-making of a given scenario. Functional exercises allow personnel to validate their readiness for emergencies by performing their duties in a simulated environment. NIST SP 800-61 Revision 3 provides sample scenarios for incident response teams to use for TTXs.

IR-3(2): Coordinate incident response testing with organizational elements responsible for related plans. (e.g., Contingency Plan, Continuity of Operations Plan (COOP)).

308-4 Manage Security Incidents (IR-4)

Implement an incident handling capability for incidents that is consistent with the incident response plan and includes preparation, detection and analysis, containment, eradication, and recovery; Coordinate incident handling activities with contingency planning activities; Incorporate lessons learned from ongoing incident handling activities into incident response procedures, training, and testing, and implement the resulting changes accordingly; and Verify that the rigor, intensity, scope, and results of incident handling activities are comparable and predictable across the organization.

IR-4(1): Support the incident handling process using automated mechanisms such as online incident management systems and tools that support the collection of live response data, full network packet capture, and forensic analysis.

308-5 Document Security Incidents (IR-5)

Track and document incidents, retaining incident records for at least **1 year** or longer as required by applicable laws, regulations, contractual obligations, or operational needs.

308-6 Report Security Incidents (IR-6)

Require agency personnel to report suspected or verified security and privacy incidents to the State Chief Information Security Officer (SCISO) and Maryland Security Operations Center (SOC) within **1 hour** of discovery and prior to any communication with internal or external stakeholders. If an agency is unsure whether an event constitutes a reportable cybersecurity incident and is actively investigating the circumstances, it may delay reporting for up to **3 hours** from initial detection while working to conclusively determine whether a reportable cybersecurity incident occurred, for a total of **4 hours** between detection and reporting.

In addition to reporting requirements within the State of Maryland, incidents involving personally identifiable information (PII) or other regulated data may be required to be reported to external entities, based on the type of data involved and the associated reporting requirements as determined by the SCISO and State Chief Privacy Officer (SCPO). Potential reporting entities include, but are not limited to:

Potential Reporting Entities

Entity	Entity
Federal Bureau of Investigation (FBI), Cyber Division	Internal Revenue Service (IRS), Office of Safeguards
US Department of Health and Human Services (HHS), Administration for Children and Families (ACF) Office of Child Support Services (OCSS)	US Department of Homeland Security (DHS), Cybersecurity and Infrastructure Security Agency (CISA)
Appropriate special agent-in-charge at the U.S. Treasury	The Social Security Administration (SSA)
U.S. Department of Treasury, Inspector General for Tax Administration (TIGTA)	

Ensure privacy impacted breach information is securely shared with suppliers holding State PII/privacy protected data to coordinate containment/remediation in alignment with contract and regulatory requirements.

IR-6(1): Report incidents using automated mechanisms.

IR-6(3): Provide incident information to the provider of the product or service and other organizations involved in the supply chain or supply chain governance for systems or system components related to the incident.

308-7 Leverage Response Assistance (IR-7)

Seek assistance from Maryland State SOC and related teams (i.e., Core Cyber Response Team (CCRT), and State Incident Response Team (SIRT)), as incident response support resources, to obtain technical advice and response assistance for users of the system and those handling and reporting on the incident.

In addition to response assistance from DoIT, incidents may necessitate engagement with other internal and external assistance resources as determined by the SCISO and SCPO. Other potential resources for assistance include, but are not limited to:

Potential Response Assistance Resources

Entity	Area of Assistance
Maryland State Police	Investigation
Assistant Attorney Generals	Legal Counsel
Office of Communications	External Communication
Human Resources	Personnel Investigations
Call Center/Fulfillment Services	Breach Notification
National Guard	Technical Response Assistance

IR-7(1): Increase the availability of incident response information and support using automated mechanisms.

Automated Mechanisms

Automated mechanisms can provide a push or pull capability for users to obtain incident response assistance. For example, individuals may have access to a website to query the assistance capability, or the assistance capability can proactively send incident response information to users (general distribution or targeted) as part of increasing understanding of current response capabilities and support.

308-8 Develop an Incident Response Plan (IR-8)

Develop an incident response (IR) plan that aligns to the Statewide Cybersecurity Incident Response Plan maintained by the SCISO and that:

- Provides the agency with a roadmap for implementing its incident response capability;
- Incorporates Business Impact Analysis (BIA) to drive prioritization of systems;
- Describes the structure and organization of the incident response capability;
- Provides a high-level approach for how the incident response capability fits into the overall DoIT Incident Response Plan;
- Meets the unique agency requirements of the organization, which relate to mission, size, structure, and functions driven by an incident classification/severity matrix to guide;
- Defines reportable incidents;
- Provides metrics for measuring the incident response capability within the agency (i.e., Mean Time to Detect (MTTD), Mean Time to Contain (MTTC), and Mean Time to Recover (MTTR);
- Defines the resources and management support needed to effectively maintain and mature an incident response capability;

- Addresses the sharing of incident information;
- Is reviewed and approved by designated DoIT officials;
- Is configuration (i.e., version) controlled;
- Explicitly designates responsibility for incident response to agency personnel; and
- Includes playbooks developed by the agency to address various types of incidents.

Distribute copies of the incident response plan to System Owners, Managers, CISO, Chief Technology Officer (CTO), and other key personnel as deemed necessary.

Review and update the IR plan to address system and organizational changes or problems encountered during plan implementation, execution, or testing at least **annually**;

Communicate IR plan changes to System Owners, Managers, CISO, and CTO and protect the IR plan from unauthorized disclosure and modification.

NIST defines several common incident categories that can be considered when developing the IR plan. The categories include but are not limited to:

Common Incident Categories

Category	Description
Unauthorized Access	Gaining access to systems or data without permission.
Malicious Code	Includes viruses, worms, trojans, ransomware, and spyware.
Denial of Service (DoS)	Disrupting normal operations by overwhelming resources.
Improper Usage	Violations of acceptable use policies (e.g., using systems for personal gain).
Scans/Probes/Attempted Access	Reconnaissance or attempts to exploit vulnerabilities.

REFERENCES

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 800-61	Incident Response Recommendations and Considerations for Cybersecurity Risk Management	This document provides updated guidance on handling cybersecurity incidents.	*csrc.nist.gov (LINK)*
CISA Publication	Cybersecurity Incident & Vulnerability Response Playbooks	This document provides sample operational procedures for planning and conducting response activities.	*cisa.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
308-1	**Develop Agency-Level Procedures (IR-1)**	☐ Yes ☐ No
308-2	**Provide Incident Response Training (IR-2)**	☐ Yes ☐ No
308-3	**Perform Incident Response Testing (IR-3)**	☐ Yes ☐ No
308-4	**Manage Security Incidents (IR-4)**	☐ Yes ☐ No
308-5	**Document Security Incidents (IR-5)**	☐ Yes ☐ No
308-6	**Report Security Incidents (IR-6)**	☐ Yes ☐ No
308-7	**Leverage Response Assistance (IR-7)**	☐ Yes ☐ No
308-8	**Develop an Incident Response Plan (IR-8)**	☐ 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.