Maryland

DEPARTMENT OF INFORMATION TECHNOLOGY

Office of Security Management

Cybersecurity & Privacy Incident Response Policy

Distribution Statement: 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.

TABLE OF CONTENTS

100 INTRODUCTION 1
200 POLICY 3
200.1 INCIDENT MANAGEMENT 3
200.2 INCIDENT RECORDS 4
200.3 INCIDENT AFTER-ACTIONS 5
300 APPROVAL 6
APPENDIX A: POLICY MAPPING MATRIX 7
APPENDIX B: DEFINITIONS 8

CHANGE RECORD

Version	Summary of Changes	Changed By	Date
1.0	Initial Publication	Miheer Khona	02/18/2026

State of Maryland

INCIDENT RESPONSE POLICY

MD-POL-209-01	Last Updated: 02/18/2026

100 INTRODUCTION

Purpose:	This policy establishes a structured and effective approach for identifying, managing, and mitigating the risk of cybersecurity and privacy incidents that threaten the confidentiality, integrity, or availability of information and State assets.
Scope:	This policy addresses security and privacy incidents impacting State systems and data whether operated by the State or by a third-party provider.
Authorization:	This policy is authorized by State Finance & Procurement Article (SF&P) § 3.5-303 and § 3.5-2A-04.
Applicability:	This policy applies to all "units of State government" (as that term is defined in SF&P 3.5-101(g)), hereafter referred to as “agencies.”
Superseded Policy:	The full policy suite outlined in MD-POL-100 Cybersecurity & Governance Policy, Appendix C supersedes the State of Maryland Information Technology Security Manual Version 1.2, June 28, 2019.
Waivers:	Refer to the MD-POL-100 Cybersecurity Governance Policy guidance on exception requests and waivers related to this policy.
Stakeholder Roles:	**Department of IT (DoIT) -** The Department responsible for developing, maintaining, revising, and enforcing information technology policies, procedures, and standards.
	State Chief Information Security Officer (SCISO) - The appointed individual responsible for overseeing the State's cybersecurity strategy and ensuring the protection of its information systems.
	State Chief Privacy Officer (SCPO) - The individual responsible for supporting agencies in the development and implementation of effective privacy programs, developing privacy policies, and promoting compliance with data protection best practices.

	Executive Branch Secretaries, Executive Directors, and Administrators (or equivalent) – The individuals who oversee specific departments and agencies responsible for ensuring the implementation of this policy and any related standards for their respective agencies.
	IT Managers – Any staff with the responsibility of procuring or operating IT systems and equipment within an agency.
	Information Security Officers (ISO) - The individuals assigned to provide agencies with security expertise, guidance, and resources to assist agencies in meeting State and Federal cybersecurity compliance requirements.
	Information User (hereafter referred to simply as "user") - Any person who interacts with a State computer system, software application, network service, or data to include State employees, contractors, vendors, third-party providers.
Stakeholder Responsibilities:	Following the policy statements in each area, a RACI matrix is provided to clearly address responsibility for each policy statement as follows:
	[R] Responsible: The person or people within each agency who are tasked with completing the work.
	[A] Accountable: The person or people within each agency who authorize and assign the work and validate that the work is completed.
	[C] Consulted: The person or people within each agency whose input is sought during the completion of the task.
	[I] Informed: The person or people within each agency who need to be kept up to date on the progress or completion of the task.

All requirements in this policy remain in effect unless an applicable State Statute or Executive Order establishes a conflicting requirement that precludes compliance

200 POLICY

The following sections detail the required actions regarding a suspected or detected cybersecurity or privacy incident.

A security **event** is any observable activity or occurrence that could affect a system or network, whereas a security **incident** is a confirmed event or violation that causes harm or poses an imminent threat of violation of security policies or practices. A **breach** is unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information.

200.1 INCIDENT MANAGEMENT

200.1.1 Incident Response Plan: The SCISO will develop and maintain a Statewide Cybersecurity Incident Response Plan. All agencies shall develop and strictly follow an Agency Incident Response Plan that aligns to the State plan and relevant standards published by the SCISO. The plan shall identify agency and system-specific detection and response tools, escalation & reporting procedures, and incident handling team roles and assignments. Ensure the plan is legally sound and incorporates the handling laws and regulations associated with information defined by the State as either confidential (Data Classification Level 3) or restricted (Data Classification Level 4) (e.g., State Law, HIPAA, FERPA, PCI DSS, CJIS, and FTI).

200.1.2 Incident Triage: Incident response activities shall include analysis of events to determine the following:

- Validation that it is truly an incident/breach;
- Identification of data exposed (e.g., privacy related);
- Assessment of impact and severity level;
- Categorization by type of incident/breach; and
- Prioritization, based on risk.

Ensure that privacy harm (e.g., violation of privacy rights, risk of individual harm, regulatory fines) is a defined, measured, and prioritized factor in the incident categorization, making data breaches that impact information defined by the state as either confidential (Data Classification Level 3) or restricted (Data Classification Level 4) automatically high priority.

200.1.3 Reporting & Communication: Agencies shall track and validate status throughout the life of the incident. Incidents (suspected or verified) shall be escalated to the SCISO and Maryland Security Operations Center (SOC) within **one (1) hour** of discovery 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 **four (4) hours** between detection and reporting.

The SCPO shall be notified **immediately** of any incident impacting information defined by the State as either confidential (Data Classification Level 3) or restricted (Data Classification Level 4) and consulted regarding privacy incident investigation, breach analysis, and legally required breach notification procedures to regulators (e.g., DHHS, SSA), and affected individuals, which are triggered solely by the involvement of personal information.

Agencies shall ensure the SCPO and agency and State Legal Counsel are included in the escalation path to authorize or restrict external communication, mitigating legal risk and reputational harm.

200.1.4 Response Assistance: The SCISO is responsible for engaging the MD SOC, the Core Cyber Response Team (CCRT), and the State Incident Response Team (SIRT) to assist agencies impacted by an incident.

Table 1 RACI Matrix – Incident Management

	DOIT	SCISO/ SCPO	Secretaries/ Directors	IT Managers	ISOs
Incident Response Plan	C	C	A	R	C
Incident Triage	C	C	A	R	C
Reporting & Communication	C	C	A	R	C
Response Assistance	R	A	I	I	C

[R] Responsible, [A] Accountable, [C] Consulted, [I] Informed

200.2 INCIDENT RECORDS

200.2.1 Incident Report: All incidents shall be documented in a standardized incident report to include, at a minimum, each of the following elements:

- Sequence of events that occurred during the incident/breach;
- Impact (e.g., system disruption, data loss, impacted records);

- Threat actors involved (if discernable);
- Initial attack vector (or vulnerability that was exploited);
- Root cause analysis; and
- Indicators of compromise and evidence of persistence.

200.2.2 Incident Artifacts: All records and artifacts shall be preserved and protected from unauthorized access or manipulation to include but not limited to the following:

- Incident data;
- Metadata; and
- Sources of all information.

200.2.3 State Records: DOIT Office of Security Management (OSM) shall maintain records for incidents that have occurred across the State. Agencies shall maintain records related to privacy incidents, breach risk analyses, and breach notifications.

Table 2 RACI Matrix – Incident Records

	DOIT	SCISO/ SCPO	Secretaries/ Directors	IT Managers	ISOs
Incident Report	C	I	A	R	C
Incident Artifacts	C	I	A	R	C
State Records	R	A	C	I	I

[R] Responsible, [A] Accountable, [C] Consulted, [I] Informed

200.3 INCIDENT AFTER-ACTIONS

200.3.1 Lesson Learned: Incidents shall be analyzed for lessons learned and mitigations identified and applied to reduce the risk of future incidents. Training and awareness shall be updated to promote lessons learned from security and privacy incidents.

Table 3 RACI Matrix – Incident After-Actions

	DOIT	SCISO/ SCPO	Secretaries/ Directors	IT Managers	ISOs
Lessons Learned	C	I	A	R	C

[R] Responsible, [A] Accountable, [C] Consulted, [I] Informed

300 APPROVAL

Katie Savage
Secretary & State Chief Information Officer
Maryland Department of Information Technology

James Saunders
State Chief Information Security Officer
Maryland Department of Information Technology

APPENDIX A: POLICY MAPPING MATRIX

This matrix provides a mapping of NIST CSF[1] Best Practices to the sections in this policy for reference.

NIST CSF Category	NIST CSF Sub-Categories	Maryland Policy Mapping
Respond	RS.MA: Incident Management	Section 200.1
Respond	RS.AN: Incident Analysis	Section 200.1, 200.2
Respond	RS.CO: Incident Response Reporting and Communication	Section 200.1.1, 200.1.3
Respond	RS.MI: Incident Mitigation	Section 200.1, 200.3
Govern	GV.OC: Organizational Context	Section 200.1.1
Govern	GOV.RM: Risk Management	Section 200.1.2
Govern	GV.RR: Risk Response	Section 200.1.3
Identify	ID.AM: Asset Management	Section 200.1.2

[1] NIST Cyber security Framework 2.0

APPENDIX B: DEFINITIONS

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