Maryland Cybersecurity Incident Response Policy

Last Updated: 01/31/2017

Contents

1.0 Purpose

The Maryland Department of Information Technology (DoIT) is committed to managing the confidentiality, integrity, and availability of information technology (IT) networks, systems, applications (IT systems), and data owned and/or operated by the Executive Branch of the State of Maryland, including vendors, contractors, and/or other affiliated entities providing services to the Executive Branch of the State of Maryland. This includes providing timely, efficient, and effective response to **cybersecurity incidents**. This policy contains the requirements for cybersecurity incident response (IR) capabilities within DoIT and other Maryland Executive Branch agencies in accordance with NIST SP 800-53R4 and SP 800-61R2.

2.0 Document and Review History

This policy supersedes the Maryland Information Security Policy v3.1 (2013) Section 6.3: Incident Response and any related policy regarding incident response declared prior to the 2017 Cybersecurity Program Policy. This document will be reviewed annually and is subject to revision.

Date	Version	Policy Updates	Approved By:
01/31/2017	v1.0	Initial Publication	Maryland CISO

3.0 Applicability and Audience

All Maryland Executive Branch agencies will comply with this policy and coordinate with the State CISO for approval of agency security incident management plans.

The Maryland Department of Information Technology will be responsible for establishing technical capabilities as services to Enterprise onboarded agencies in accordance with the requirements of this policy. As data owners, all agencies will be responsible for individual security incident management plans to handle any potential loss or breach of confidential information and will abide by any applicable law, regulation, or standard relating to breach notification, such as requirements of the Md. Code Ann., State Gov't §§ 10-1301 to 1308, HIPAA, and PCI DSS.

4.0 Policy

The Executive Branch of the State of Maryland is committed to establishing policy that incorporates industry standards and best practices while using **forensically sound methodology** to mount an efficient and effective incident response. This policy establishes the minimum requirements for Executive Branch agencies to respond to a cybersecurity incident.

4.1 Establish and Maintain a Cybersecurity Incident Response Capability

Maryland Executive Branch Agencies are considered **data owners** and are required to create and manage a security incident management plan. DoIT Enterprise onboarded agencies will establish a security incident management plan as directed under Section 4.4 and will have access to technical services provided by the DoIT **Incident Response Coordinator** to augment the

investigation of any incident, determine the potential compromise or data loss, and remediate the exploitation. Agencies under the policy authority but not under direct management of DoIT must have a security incident management plan as directed in Section 4.4 to include any technical capability required to address any compromise and remediation of a cybersecurity incident.

NOTE: This policy does not address security incidents that do not have a cybersecurity component, such as the theft of non-computer office supplies or a physical altercation between employees.

4.2 Incident Tracking and Documentation

Information security incidents shall be documented and tracked in accordance with the requirements shown in the table below.

#	Name	Requirement
A	Incident Tracking	All incidents will be recorded.
B	Retention Period	Records of incidents will be maintained for at least a period of 3 years, or longer as required under relevant regulations (e.g., 5 or 7 years for FTI related data and records under IRS-1075).
C	Tracking Method	An automated system or platform will be used to track incidents. This system will allow for: ▪ Tracking of the status and disposition of individual incidents ▪ Reporting to DoIT and the State CISO for all tracked incidents ▪ Correlating between incidents ▪ Tracking and reporting of IR Key Performance Indicators (KPIs)

4.3 Staffing and External Support

Agencies shall establish and maintain an information security incident response staff capability that complies with the requirements in the table below.

#	Name	Requirement
A	Full Time Staffing	Hire or retain staff necessary for a reasonable response to a cybersecurity incident in accordance with the requirements of this policy. Enterprise onboarded agencies shall have access to DoIT technical services in the event of a cybersecurity incident.
B	Surge Support	All agencies, including DoIT, will proactively secure service agreements with external incident handling providers so that additional surge resources can be obtained rapidly, as needed. ▪ DoIT will maintain this capability for onboarded (Enterprise) agencies. ◆ Any Enterprise agency that experiences an incident in which surge support must be utilized will cover costs associated with activating the resources required to investigate the incident, assess the compromise, and remediate the threat.

#	Name	Requirement
C	Vendor Support	Identify and maintain current contact information for major vendors of security solutions, operating systems, and network devices in place at the agency so that solution-specific consulting can be rapidly obtained during an incident.

4.4 Security Incident Management Plan

All Maryland Executive Branch agencies shall establish and maintain a Security Incident Management Plan to comply with the provisions listed in the table below.

#	Name	Requirement
A	Process	Incorporate forensically sound methodology to be used by the agency during information security incidents, which shall be flexible enough to account for a wide-range of potential cybersecurity incident types.
B	Organizational Structure, Roles & Responsibilities	Define and describe an organizational structure, including: ▪ Identifying DoIT Enterprise Incident Response Coordinator for technical services; DoIT Enterprise Incident Response Coordinator will determine the technical team(s) and roles ▪ Identifying the agency Incident Response Coordinator ▪ Defining oversight and management team(s)/roles ▪ Defining roles and responsibilities for team members ◆ Including the identification of those individuals authorized to communicate to the public, if required. ▪ Defining approval authorities for all major incident response decisions
C	Required Technology Support	Define and describe the hardware and software necessary to conduct incident response, as well as the required deployment of such assets to support response efforts.
D	Incident Severity Levels	Incorporate MEMA incident severity levels as described in Section 4.5.
E	KPIs	Define and describe the key performance indicators that will be used to measure incident response performance.
F	Review and Revision	Review and revise this plan annually and as needed if deficiencies are noted after a major incident, a training exercise, or an audit finding.
G	Coordination with State Agencies	Establish coordination with state agencies in accordance with mission/business roles, including but not limited to the Department of Information Technology (for non-Enterprise agencies), Maryland Emergency Management Agency (MEMA), the Maryland State Police (MSP), and the Maryland Coordination and Analysis Center (MCAC).
H	Coordination with Other Plans	Identify guidelines for coordinating with related plans, including but not limited to disaster recovery and business continuity plans.
I	Legal Counsel	Identify guidelines for any conditions requiring the advice of legal counsel to ensure that legal and regulatory obligations are assessed and met during incidents.
J	Approval	Requires written approval from the State CISO, or a delegated authority.
K	Reporting	Determine guidelines for interim and post-incident report contents.

#	Name	Requirement
L	Internal Notification	Data owners will establish and maintain response strategies that incorporate DoIT notification requirements as shown in Section 4.7.
M	Breach Notifications	Data owners will establish and maintain response strategies for handling breach notification requirements as shown in Section 4.8.

4.5 Cybersecurity Incident Severity Levels

Cybersecurity severity levels must be tied to the Maryland Emergency Management Agency (MEMA) State Response Activation Levels (SRAL) index. Depending upon the severity level an incident may be reported to the Maryland Emergency Management Agency (MEMA) for tracking and review. The MEMA Joint Operation Group may escalate the incident to a State emergency and assume operational control should their assessment warrant such action.

4.6 Exercises and Training

Agencies shall conduct incident response exercises and trainings in accordance with the requirements shown in the table below.

#	Name	Requirement
A	Organization-wide Exercises	Conduct an organization-wide, table-top incident response exercises at least annually. In addition: ▪ DoIT may facilitate this exercise for some agencies, and may combine the exercises for multiple agencies into a single exercise. ▪ The Secretary of IT will participate in DoIT's exercise at least biennially (every other year) and the Director of Cybersecurity/State CISO will participate annually. ▪ The Secretary of IT may request the participation of other cabinet-level or agency specific officials as deemed necessary.
B	Agency Table-Top Exercise	Agencies that maintain a dedicated security team will conduct a table-top, incident response exercise at least annually within that team. ▪ Agencies without a dedicated security team will review established security incident management plans at least annually (as described in section 3.0).
C	Post-exercise Reports	Reports will be drafted for all exercises that will include any capability gaps identified along with other lessons learned.
D	Training Events	Exercises will include sufficient training in order to enable participants to understand and execute their functions/roles.

4.7 Incident Reporting and Notification

Information security incidents will be reported in accordance with requirements to be outlined by DoIT in process level documentation and provided -- at least -- to all onboarded agencies as part of the continuous monitoring initiative.

4.8 Breach Notifications

2013 Maryland Code §10-1301 (Md. State Govt. Code §§ 10-1301 to -1308) defines the breach requirements of Personally Identifiable Information. Under the Maryland statute, a breach is considered to be any "unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of the personal information maintained by a unit." Additionally, if a unit discovers or is notified of a breach, it must conduct in good faith a reasonable and prompt investigation to determine whether the unauthorized acquisition of personal information of the individual has resulted in or is likely to result in the misuse of the information.

After an investigation is concluded, the unit must determine if notification is required under the specific circumstances. A unit or nonaffiliated third party is not required to notify an individual of a breach if the personal information of the individual was secured by encryption or redacted and the encryption key has not been compromised or disclosed. See 2013 Maryland Code §§10-1301-1308 for further information on notification requirements.

NOTE: This policy provides guidance for compliance with specific portions of the Maryland Code §§10-1301-1308, but does not supplement, replace or supersede the Maryland law itself. Executive agencies and the associated vendors or contractors are responsible for independently complying with all provisions of Maryland law and other regulations/standards that affect specific types of Confidential Data, such as those required under HIPAA. PCI DSS, or IRS-1075.

5.0 Exemptions

This policy applies to all Maryland Executive Branch agencies. If an agency under the policy authority of DoIT requires an exemption from this policy, that agency must submit a DoIT Policy Exemption Request Form and clearly articulate the reason for the exemption. An operational risk assessment will be conducted to identify the risks and the agency's mitigation strategy associated with the exemption. If the agency can accept the risk, an exemption to this policy may be granted.

6.0 Policy Mandate and References

This policy is mandated by the Cybersecurity Program Policy. The following documents are references for this policy:

- DoIT Security Incident Management Plan (Mandated by this policy)
- DoIT Continuous Monitoring Policy
- DoIT Account Management Policy (See section on Training and Awareness)
- NIST SP 800-53R4 "Security and Privacy Controls for Federal Information Systems and Organizations"
- NIST SP 800-61R2 "Computer Security Incident Handling Guide"
  - Can be used by agencies to formulate a Security Incident Management Plan and associated processes

7.0 Definitions

Term	Definition
Cybersecurity Incident	A verified event or set of events that has or may result in a change to the confidentiality, availability or integrity of State information systems, networks, or data, and for which a directed response may be required to mitigate the associated damage or risk. An occurrence that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies may also be considered an incident.
Data Owner	Official(s) with statutory or operational authority for specified information and responsibility for establishing the controls for its generation, collection, processing, dissemination, and disposal.
Forensically Sound Methodology	The application of reliable and accurate digital forensic processes and procedures, including the underlying technology used to collect and analyze information, that, when followed, does not diminish the authenticity or veracity of the data and preserves the original meaning of the data; the processes and procedures should maintain legal evidentiary weight, be testable, and independently verifiable for use in a court of law.
Incident Response Coordinator	Responsible for ensuring the IR response process moves forward, as well as: ▪ Tracking the progress of the IR process during the security incident; ▪ Coordinating and tasking IR team members and support staff, disseminating information as necessary, and ensuring the IR process is followed and effective; ▪ Providing status updates to relevant parties who are not members of the IR team; and ▪ Providing expertise where necessary by either offering guidance from personal knowledge and experience or by channeling such information from the subject matter expert.

8.0 Enforcement

The Maryland Department of Information Technology is responsible for managing cybersecurity incident response policy and processes for all agencies managed by the DoIT Enterprise. DoIT will manage cybersecurity incident response according to agency-created IR Plans and established requirements described in Section 4.0 of this policy unless an agency has completed a Policy Exemption Request Form and received approval from DoIT. Agencies under the policy authority, but not under direct management, of DoIT must exercise due diligence and due care to independently comply with the minimum requirements of this policy or complete a Policy Exemption Request Form.

If DoIT determines that an agency is not compliant with this policy, the agency will be given a sixty (60) day notice to become compliant or at least provide DoIT a detailed plan to meet compliance within a reasonable time before the issue is reported to the Secretary of Information Technology. The Secretary of Information Technology, or a designated authority, may extend a non-compliant agency's window of resolution or authorize DoIT to shutdown external and internal network connectivity until such time the agency becomes compliant.

Appendix A: Breach Response Guide

Organizations have a legal and ethical responsibility to protect the privacy and security of confidential information. Prompt response to a data breach allows the organization to minimize further data loss and mitigate consequences of the breach, especially to affected individuals. The following sections of this Appendix provide a general outline of critical breach response components and should be used by agencies to create, develop, or further refine their own breach response plans.

A data breach is a cyber event that results in a loss of confidential information to an unauthorized entity (e.g., cyber attacker). A data breach can occur whether the organization or agency has direct custody of the data or stores and manages information through a contractor or vendor. Not all cybersecurity incidents are data breaches.

It is critical for agencies, and their contractors and vendors, to understand which Federal, State, and local breach-notification laws apply to them, and for agencies to comply with data response, reporting, and notification requirements of all applicable laws. To prepare for a breach, an agency must determine its legal responsibility to notify affected parties. The type of system or data compromised can affect the determination of whether a breach occurred, response to a breach, and notification requirements to stakeholders and other data owners.

NOTE: Agencies must be aware of relevant contractual obligations, regulatory requirements, and private industry standards affecting specific data that the entity creates, processes, transmits, or stores that may require breach response and notification.

1.0 Breach Response Guide

1.1 Before a Breach

Proactive operational protections and processes can reduce the likelihood of a breach. Agencies should exercise due care to take the actions outlined below to reduce the risk of a breach.

- Establish and maintain a breach response plan by:
  - Documenting relevant breach notification requirements
  - Specifying incident handling procedures
  - Identifying an incident response team
  - Identifying an incident manager who will direct incident and breach response
- Review information systems and data to identify where confidential information resides by:
  - Documenting what type of confidential information is maintained by an agency, how it is stored, and how it is secured
  - Conducting regular risk assessments
  - Reviewing who has access to confidential information
  - Implementing controls to prevent unauthorized access
  - Implementing security controls, where feasible, such as encryption of confidential information at rest or in motion
- Continuously monitor for confidential information leakage by:

- Implementing automated tools such as intrusion detection and intrusion prevention systems, firewalls, and anti-virus and anti-malware tools to monitor and alert on suspicious activity
- Using data-loss-prevention solutions to track the movement of confidential information throughout the system and prevent the unintentional disclosure of confidential information
- Conducting tabletop exercises to periodically test and check the validity of established security controls

- Conduct frequent privacy and security awareness training by:
  - Providing training and awareness on privacy and security topics during employee onboarding
  - Providing (at least) annual privacy and security training and awareness programs to keep employees current with changing technology and threat vectors
  - Clearly defining and deploying an accessible mechanism for reporting incidents and complaints

1.2 After the Breach

Effective breach-response can minimize damage. Agencies should exercise due care to take the actions outlined below after a breach occurs.

- Verify a breach occurred by:
  - Recognizing that not all cybersecurity incidents are considered breaches
  - Examining what information and systems were affected by the cybersecurity incident to determine whether information affected is covered by relevant breach statutes
- Determine the scope and composition of the breach by:
  - Consulting with legal counsel to examine applicable Federal, State, and local breach reporting requirements to determine whether it is appropriate to involve authorities or law enforcement
  - Identifying all assets and information affected by the breach
  - Interviewing key personnel associated with the incident to gather facts regarding the incident
- Seek legal assistance to determine breach response and notification requirements by:
  - Consulting with legal counsel to assess the data and assets affected and determine what breach response statutes, regulations, or industry standards apply
- Investigate breach and ensure that evidence is preserved by:
  - Deciding whether to investigate a breach of information with internal resources or whether an external vendor is necessary to conduct a proper investigation
  - Consulting with legal counsel to ensure that the agency is using methods that are considered forensically sound to properly preserve and document all evidence in case it is required in a court of law
  - Consulting with external authorities or law enforcement to ensure that internal investigation does not impede their activities

- Preserving evidence for forensic examination once an investigation has been completed

- Determine whether and how to notify individuals or organizations affected by:
  - Consulting with legal counsel to determine:
    (1) whether notification is warranted
    (2) when it should be made
    (3) how that notification should be made

    NOTE: Some large-scale breach notifications may allow for public notice instead of individual notice.
  - Notifying affected individuals in accordance with the timeliness and methods outlined in relevant Federal, State, or local breach laws, regulatory requirements, private industry standards, or contractual obligations
  - Providing notifications in plain and clear language
- Review breach response plans and processes by:
  - Conducting lessons-learned
  - Identifying any improvements or changes and incorporating them into the process

2.0 Breach Response Personnel

Agencies should document personnel to contact in the event that a breach occurs. Agencies may use the following chart to document and file relevant personnel and contact information or use it as a basis from which to create their own documentation as long as the documentation retains at least the same level of detail.

NOTE: Agencies may not have all roles outlined below.

Role	(Internal or External) Name	Title	Contact Info*
Incident Leads			
Incident Lead	(Internal) [contact name]		O: M: OM: Email:
Incident Lead, Secondary	(Internal)		O: M: OM: Email:
Executive Leadership			
State CISO	(Internal)		O: M: OM: Email:
Deputy CIO	(Internal)		O: M: OM: Email:
Chief Privacy Officer	(Internal)		O: M: OM: Email:
Chief Compliance Officer	(Internal)		O: M: OM: Email:
Response Team Members			
IT Primary	(Internal)		O: M: OM: Email:
IT Secondary	(Internal)		O: M: OM: Email:
Security Primary	(Internal)		O: M: OM: Email:

Role	(Internal or External) Name	Title	Contact Info*
Security Secondary	(Internal)		O: M: OM: Email:
Legal	(Internal)		O: M: OM: Email:
Public Relations	(Internal)		O: M: OM: Email:
Law Enforcement			
Police Department	(External)		O: M: OM: Email:
FBI	(External)		O: M: OM: Email:
External Resources			
Forensics	(External)		O: M: OM: Email:
Vendor #1	(External)		O: M: OM: Email:
Vendor #2	(External)		O: M: OM: Email:
Card Processor #1	(External)		O: M: OM: Email:
Card Processor #2	(External)		O: M: OM: Email:

*O = Office; M = Mobile; OM = Work Mobile