Commonwealth of Massachusetts

Executive Office of Technology Services and Security (EOTSS)

Enterprise Risk Management Office

Enterprise Incident Response Policy

Document Name: Incident Response Policy	Effective Date: 1/1/2025
Document ID: IS.005	Last Revised Date: 12/23/2024

Table of Contents

1. Purpose

1.1. The purpose of this ***policy*** is to establish the minimum security requirements that must be implemented to protect the Commonwealth's ***information assets*** in the event of a cybersecurity ***incident***, ***data*** breach, or other security compromise of the Commonwealth's ***information assets***. This ***policy*** reinforces the Commonwealth's commitment to an effective cyber ***incident*** response program, and outlines the framework, principles, and ***controls*** required to ensure the protection of the Commonwealth's ***information*** technology environment.

2. Authority

2.1. Pursuant to M.G.L. Ch. 7d, the Executive Office of Technology Services and Security, (EOTSS), possess the authority to establish ***policies***, ***procedures***, and objectives with respect to activities concerning ***information*** technology. M.G.L. Ch. 7d provides in pertinent part: "Notwithstanding any general or special law, rule, regulation, executive order, policy or procedure to the contrary, all executive department agencies shall, and other state agencies may, adhere to the policies, procedures and objectives established by the executive office of technology services and security with respect to activities concerning information technology."

3. Scope

3.1. This document applies to the use of ***information, information systems***, ***assets***, ***applications***, and network resources used to conduct business on behalf of the Commonwealth. The document applies to the Executive Branch including all executive offices, boards, commissions, ***agencies***, departments, divisions, councils, and bureaus, hereinafter referred to as Commonwealth Agencies and Offices. Other Commonwealth entities that use or participate in services provided by the Executive Office of Technology Services and Security, (EOTSS), by any form of contractual arrangement, are required to comply with this document, as a condition of use. Commonwealth Agencies and Offices are required to implement ***procedures*** that ensure their ***personnel*** comply with the requirements herein to safeguard ***information***.

4. Responsibilities

4.1. The Enterprise Risk Management Office is responsible for the development and ongoing maintenance of this ***policy***. The Enterprise Risk Management Office is responsible for this ***policy*** and may enlist other departments to assist in

maintaining and monitoring compliance with this ***policy***. The owner of this document is the ***Commonwealth CISO***, or his or her designee. The ***document owner*** will review and update this ***policy*** on an annual basis, or when significant ***policy*** or procedural changes necessitate an amendment. Questions regarding this document must be submitted to the ***document owner*** by sending an email to ERM@mass.gov. Additional ***information*** regarding this ***policy*** and its related ***policies*** and ***standards*** may be found at https://www.mass.gov/cybersecurity/***policies***. Definitions of terms in bold may be found in the ***IS Glossary*** at https://www.mass.gov/cybersecurity/***policies***

5. Compliance

5.1. Compliance with this document is mandatory for the Executive Branch and all Commonwealth Agencies and Offices. Violations are subject to disciplinary action in accordance with applicable employment and collective bargaining agreements, up to and including the termination of their employment and/or assignment with the Commonwealth. ***Exceptions*** to any part of this document must be requested online through ServiceNow, https://www.mass.gov.service-now.com). A ***policy exception*** may be granted only if the benefits of the ***exception*** outweigh the increased ***risks***, as determined by the ***Commonwealth CISO,*** or his or her designee. All ***exceptions*** will be for a limited time and will be narrow in scope.

6. Requirements

6.1. Incident Response Plans

6.1.1. Commonwealth Agencies and Offices will establish an ***incident*** response plan, (IRP), to effectively detect, respond and resolve ***incidents*** that affect the security of the Commonwealth's ***information assets***.

6.1.2. Commonwealth Agencies and Offices will document, maintain, and update ***incident*** response plans.

6.1.3. The ***incident*** response plan will be tested not less than annually.

6.1.4. ***Incident*** response plans should, at a minimum, include the following:

6.1.4.1. Roles, responsibilities, communication and contact strategies in the event of a compromise, including notification of required internal and external ***stakeholders***.

6.1.4.2. Establishment of a ***Security Incident*** Response Team, (***SIRT***).

6.1.4.3. Specific ***incident*** reporting ***procedures***.

6.1.4.4. Specific escalation response ***procedures.***

6.1.4.5. Reportable ***incident*** criteria.

6.1.4.6. Execution of corrective actions and post-***incident*** analysis.

6.1.4.7. Establish criteria to activate business recovery and continuity ***processes.***

6.1.4.8. ***Data*** backup ***processes.***

6.1.4.9. Analysis of legal requirements for reporting compromises.

6.1.4.10. Reference or inclusion of ***incident*** response ***procedures*** from required external parties.

6.2. Incident Response Lifecycle

6.2.1. The ***incident*** lifecycle addresses the preparation, detection, containment, eradication, and recovery phases of the ***incident*** response ***process***:

6.2.1.1. Preparation: Commonwealth Agencies and Offices will prepare for ***incidents*** through the development of documented ***incident*** response plans and ***incident*** handling ***procedures***. ***Incident*** response exercises, (tabletops), should be held on a regular basis, but not less than annually.

6.2.1.2. Detection and Analysis: This phase consists of the identification of events through probable attack vectors, signs of ***incidents***, detection sources such as Security Incident Event Management, (SIEMs), anti-virus, and ***logs***, detailed ***incident*** analysis, ***incident*** documentation, ***incident*** prioritization, and ***incident*** notification.

6.2.1.3. Containment, Eradication and Recovery: This phase consists of mitigating and limiting the scope of impact to systems and ***data*** through containment strategies, evidence gathering, identification of attackers, threat neutralization, and restoration of normal operations.

6.2.1.4. Post Incident Activity: This phase consists of identifying and analyzing historical ***information***, development of lessons learned reports, analysis of ***incident information***, and retention of evidence for investigations and legal requirements and identifying lessons learned.

6.3. Incident Identification

6.3.1. A ***security incident*** is defined as any event which has the potential or has already resulted in the unauthorized acquisition, misappropriation, use or manipulation of ***information*** that compromises the confidentiality, integrity, or availability of the Commonwealth's ***information assets***. Examples include, but are not limited to:

6.3.1.1. Unauthorized and illegal disclosure, destruction and/or alteration of files, Commonwealth IT systems and ***information***, including ***confidential information***.

6.3.1.2. Unauthorized use of a Commonwealth IT system for the transmission, processing, or storage of ***information***.

6.3.1.3. Changes to system hardware, firmware or ***software*** characteristics intentionally concealed from the IT ***Information Owner*** and made without their knowledge or consent.

6.3.1.4. Detection of ***malware*** or malicious code (viruses, worms, etc.).

6.3.1.5. Unauthorized probes, scans, or sniffers on the Commonwealth's internal network.

6.3.1.6. Denial of Service (DOS) or Distributed Denial of Service (DDOS) attacks.

6.3.1.7. Harassment and threats conducted via Commonwealth email resources.

6.3.1.8. Web page defacement, unauthorized use of system privileges and attempts (either failed or successful) to gain unauthorized access to a system or its ***information***.

6.3.1.9. Legal or regulatory violations involving Commonwealth ***information assets***.

6.3.1.10. Violation of the Commonwealth's ***information*** security ***policies***.

6.3.1.11. Cyber-stalking, identity theft or child pornography.
6.3.1.12. Unauthorized physical access to a secure area (e.g., ***data*** centers).

6.4. Incident Reporting and Escalation

6.4.1. Commonwealth Agencies and Offices must establish, document, and distribute ***security incident*** response and escalation ***procedures*** to ensure timely and effective handling of ***incidents***, and to limit further damage to the Commonwealth's ***information assets***. ***Procedures*** will include:

6.4.1.1. Identification of the cause of the ***incident.***

6.4.1.2. Execution of corrective actions.

6.4.1.3. Post-***incident*** analysis.

6.4.1.4. Communication strategy.

6.4.2. ***Information security incident*** reporting and escalation.

6.4.2.1. ***Security incidents***, whether potential or actual, will be reported immediately to agency management, the agency ***SIRT*** team, the agency helpdesk, and/or the EOTSS Security Operations Center (SOC). More ***information*** on ***Security Incident*** reporting ***procedures*** may be found in the EOTSS or Secretariat ***Security Incident*** Response Plans.

6.4.2.2. All Commonwealth ***personnel*** are required to fully cooperate with the ***SIRT*** team and the EOTSS SOC. All Commonwealth ***personnel*** will provide accurate and timely ***information***. All Commonwealth Agencies and Offices must ensure that all ***personnel*** are available to the ***SIRT*** team and/or EOTSS SOC when needed.

6.4.2.3. As the first line of defense, Commonwealth Agencies and Offices must ensure that ***personnel*** are responsible for reporting suspicious activities.

6.4.3. Management reporting and escalation.

6.4.3.1. The ***SIRT*** team will notify EOTSS' SOC about ***security incidents*** that have an impact rating of "high." The report will include, but is not limited to the following (as applicable):

6.4.3.1.1. Date and time ***incident*** detected.

6.4.3.1.2. Date and time ***incident*** reported to supervisor(s) and/or upper management.

6.4.3.1.3. Name(s) and contact ***information*** of the person(s) who discovered the ***incident***.

6.4.3.1.4. Dated and time of notification.

6.4.3.1.5. Type of ***incident*** detected.

6.4.3.1.6. Description of the ***incident.***

6.4.3.1.7. ***Incident*** response status.

6.4.3.1.8. Location of the ***incident.***

6.4.3.1.9. Affected systems and ***user*** groups.

6.4.3.1.10. Recovery time expectations.

6.4.3.1.11. Internal and external ***stakeholder*** contacts that need to be notified.

6.4.3.1.12. Identification, containment, and eradication measures.

6.4.3.1.13. Evidence collected.

6.4.3.1.14. Pending actions (if any).

6.4.4. ***Information security incident*** response times will comply with the following impact rating table:

Impact	Characteristics	Response time[1]	Notification Level	Post-*incident* report req.
High	Threat to human safety. Adverse impact on a "Critical" or "High" ***risk*** rated ***information asset***, including infrastructure, ***applications,*** and services. Financial or legal liability equal to $1 million and above to the Commonwealth. Potential compromise of ***information*** classified as ***restricted***, or ***confidential information,*** including ***PII*** and other regulated ***information***.	Immediate	Security Operations Center (SOC), Commonwealth CIO, ***CISO*** and agency heads	Yes
Medium	Adverse impact on a "Medium" ***risk*** rated ***information asset***, including infrastructure, ***applications***, and services. Financial or legal liability between $100,000 and $1 million. Potential compromise of ***information*** not intended for public disclosure.	4 hours	Commonwealth ***CISO***, agency heads	Yes
Low	Adverse impact on a "Low" ***risk*** rated ***information asset***, including infrastructure, ***applications***, and services. Financial or legal liability of less than $100,000.	Next business day	Technical support for impacted ***information asset***	No, unless decided otherwise by the IR Coordinator

1 Note: This is not resolution time but the start time of the incident response process.

6.4.5. Communication protocols

6.4.5.1. All ***information*** pertaining to an ***incident*** investigation will be handled with discretion and disclosed only on a need-to-know basis.

6.4.5.2. ***Incident*** reports will be categorized as ***confidential*** at the discretion of the ***Commonwealth CISO,*** or his or her designee, and the Enterprise Security Office.

6.4.5.3. The ***Commonwealth CISO,*** or his or her designee, will be designated the owner for all ***incident*** investigation related documentation.

6.5. Security Incident Response and Investigation

6.5.1. When a security event is identified, the Enterprise Security Office, and relevant ***stakeholders,*** will take all necessary measures in order to minimize the ***risk*** to the Commonwealth and to limit further damage to the Commonwealth's ***information assets***.

6.5.2. The ***SIRT*** team will:

6.5.2.1. Investigate and confirm the validity of the reported ***incident.***

6.5.2.2. Contain and minimize the impact of the ***incident.***

6.5.2.3. Determine the root cause of the ***incident***, including motive and type of attack.

6.5.2.4. Document the facts of the ***incident and*** gather system events and/or audit records.

6.5.2.5. Determine the scope, severity, impact, and nature of the ***incident.***

6.5.2.6. Remove or quarantine the affected ***asset*** from all Commonwealth networks as soon as possible, where technically feasible.

6.5.2.7. Determine response and recovery timelines.

6.5.2.8. The SIRT team will consult with EOTSS Legal and follow applicable chain of custody requirements for all ***incidents*** which may have potential legal implications.

6.5.2.9. Collect and preserve all relevant evidence of the ***incident*** in whichever form it exists (digital, physical, original, or copied) Evidence will be collected and preserved in a manner that is consistent with legal and record retention requirements.

7. Roles and Responsibilities

Role	Responsibility
EOTSS Secretary and Commonwealth Chief Information Officer (CIO)	The person responsible for the management, implementation, security and usability of information, technologies, processes, and users within the Commonwealth's IT environment. The Commonwealth CIO has authority over all activities concerning information technology by all Commonwealth Agencies and Offices.
Commonwealth Chief Information Security Officer (CISO)/Chief Risk Officer (CRO)	The person responsible to ensure compliance with this policy across all Commonwealth Agencies and Offices and Agencies. The CISO/CRO leads the ERM Office and is responsible for aligning security initiatives with enterprise programs and business objectives. The CISO/CRO ensures that the Commonwealth's information assets are securely protected.
Enterprise Risk Management Office (ERM)	The office within EOTSS responsible for risk strategy, identification, assessment, analysis, monitoring, reporting and mitigation. Under the direction of the Commonwealth CISO/CRO, ERM establishes the Commonwealth's information security policies, standards, guidelines and directives to create an effective risk governance program that determines acceptable levels of risk tolerance and implements cybersecurity best practices to mitigate operational, reputational, security and financial risk.
Chief Technology Officer (CTO)	The person responsible for the management, implementation, security and internal operations of the entire information technology department. The CTO identifies weaknesses and vulnerabilities within the Commonwealth's IT environment and implements controls to protect information assets and reduce risks. The CTO leads technological advancements, determines technology strategy, drives research and develops technology initiatives.
Security Operations Center (SOC)	The office within EOTSS responsible for monitoring and analyzing the state's security posture, and for detecting, analyzing and responding to cybersecurity incidents. The SOC coordinates with municipal, state, and federal agencies, as well as other stakeholders, in the event of a cybersecurity incident. The SOC is

	also responsible for communicating any high or critical situations to leadership, and for sharing information and resources as needed, to mitigate the effect of an incident.
Security Incident Response Team (SIRT)	The team responsible to prepare for, respond to, mitigate and recover from cybersecurity incidents. The SIRT will receive, review and investigate cybersecurity related incident reports and activity. They are responsible to protect the confidentiality, integrity and availability (CIA) of the Commonwealth's IT environment.
Commonwealth Agencies and Offices	Commonwealth Agencies and Offices are responsible to adhere to this policy and to comply with the requirements in this document in addition to any supporting documentation issued by the Secretary of EOTSS/Commonwealth CIO, the Commonwealth CISO/CRO, and/or the ERM office.

8. Control Mapping

Section	NIST SP 800-53	CIS 18	NIST CSF
Incident Response	IR-2, IR-2, IR-3, IR-4, IR-6, IR-8	17.1, 17.2, 17.3, 17.4, 17.5, 17.6, 17.7, 17.8, 17.9	RC.RP, RC.CO, RS.CO, PR.PS-04, DE.AE, RS.MA, RS.AN, RS.CO, RS.MI, RC.RP, RC.CO,

9. Document Change Control

Version No.	Revised By	Effective Date	Description of Changes
1.0	Thomas E. McDermott	7/9/2024	Initial Draft
1.1	Miklos Lavicska	8/2/2024	Corrections and Formatting
1.2	Thomas E. McDermott	12/23/2024	Revisions, Corrections, and Formatting
1.3	Anthony J. O'Neill	1/1/2025	Final Review