IT Security Incident Reporting Policy

Effective Date:
January 06, 2025

Category:
Security

Scheduled Review:
June 30, 2026

Supersedes:
ITP-SEC024

1. Authority

Executive Order 2016-06, Enterprise Information Technology Governance

2. Purpose

This Information Technology Policy (ITP) establishes the policies, procedures, and standards related to reporting and managing Cyber Security Incidents.

3. Scope

This policy applies to all offices, departments, boards, commissions, and councils under the Governor's jurisdiction and any other entity connecting to the Commonwealth Network (hereinafter referred to as "agencies").

Third-party vendors, licensors, contractors, or suppliers shall meet the policy requirements of this policy as outlined herein.

4. Policy

For definitions found within this document, refer to the *IT Policy Glossary*.

The Pennsylvania *Breach of Personal Information Notification Act, as amended November 3, 2022, P.L. 2139, No. 151, 73 P.S. §§ 2301-2330,* requires notification to affected individuals in instances where it is determined unencrypted or unredacted personal information was or is reasonably believed to have been accessed or acquired by an unauthorized person. This security incident reporting and escalation policy enables the enterprise to respond effectively to security incidents, such as a personal information breach, by clearly detailing the roles and responsibilities of all the parties involved. It provides a precise path for reporting, escalating, auditing, and remediating security incidents. Proper reporting and management of Cyber Security Incidents is critical to secure and protect the Commonwealth of Pennsylvania's critical Information Technology (IT) business processes and assets from cyber-crime or cyber-terrorism.

The Office of Administration, Office for Information Technology, Enterprise Information Security Office (OA/IT/EISO) is responsible for coordinating and leading the cyber incident response when a cyber security incident involves: the enterprise, an agency, multiple agencies, and entities such as business partners who have access to Commonwealth's network and data repositories. In addition, OA/IT/EISO is responsible for the Commonwealth's cyber security readiness, threat analysis, and remediation efforts.

The following IT security incident scenario table provides the responsibilities for OA/IT/EISO, Agency Information Security Officers (ISO), and Agency Chief Information Officers (CIO).

Scenario	OA/IT/ EISO	Enterprise	DC/Agency ISO
Proactively identify potential cyber security threats and take precautions before they can cause potential harm to the Commonwealth's IT infrastructure.	X	X	
Proactively identify potential cyber security threats and take precautions before they can cause potential harm to the agency's IT infrastructure.		X	X
Set and alert the agencies of the current cyber security threat posture.	X		
Coordinate the recovery of Commonwealth network operations, telecommunications, and IT applications and databases.	X		
Provide assistance to agencies in remediation of issues caused by Cyber Security Incidents.	X		
Prepare and educate Commonwealth agencies, and employees as to the dangers of cyber security threats and how to reduce their risk exposure.	X	X	
Coordinate remediation efforts with local government representatives through the Pennsylvania Sharing and Advisory Committee (PA-ISAC) to exchange policy and operational information necessary to respond to and recover from Cyber Security Incidents	X		
Conduct cyber security Forensic Analysis in investigating and gathering of information related to cyber threats and attacks.	X		

Work with third-party security providers to ensure they respond to and address Cyber Security Incidents reported to them.	X	X	
Track the status of ongoing investigations and provide reports to agency CIOs, ISOs, and OA executive staff.	X		
Appoint an agency ISO and a secondary point of contact (POC) for Cyber Security Incident reporting and handling. Provide OA/IT/EISO those POCs information.			X
Collaborate with business unit management to declare an outage for affected systems.	X	X	X
Act as the primary POC for Cyber Security Incident response for the agency.		X	
Report incidents bi-directionally from OA/IT/EISO via the Commonwealth reporting system. Automated SIEM process should be used where available.	X	X	

4.1 Incident Response and Countermeasures

Following the immediate response to a security incident, different countermeasures may be taken, depending on the type and severity of the incident and the value of the affected assets. As part of an incident response, the Commonwealth CISO or agency ISOs may prescribe the necessary incident management steps, which may include, but are not necessarily limited to, disconnecting a system from the network, confiscating hardware for evidence, or providing information for investigative purposes and choosing one or more of the following actions:

- **Information gathering:** Depending on the nature of the security event, it may be necessary to examine the situation, enhance logging capabilities, copy documents, back up temporary files, and set up alarms or change threshold values.
- **Configuration changes:** In many cases, configuration changes, including the installation of software patches, reconfiguration of hardware devices or policy revisions will be necessary following a security incident.
- **Forensics:** In certain cases, it may be required to conduct digital forensics on the affected IT resources to identify root cause or prevent an infection from spreading across the network. In certain cases, where criminal activity is suspected or confirmed, law enforcement authorities may be notified. In any case, all available evidence collected via digital forensics must be made tamper-resistant and the chain of custody of all such

evidence must be maintained throughout the forensics investigative process.

Note: In the event, an affected asset or assets must be isolated and excluded from regular service to prevent further security incidents, business unit management will be engaged by the agency CIO or ISO to declare an outage and invoke their disaster recovery plan, or continuity of operations plan.

4.2 Information Sharing with External Partners

Information specific to a Cyber Security Incident, such as but not limited to Indicators of Compromise (IOCs), shall not be shared with any external partners until after remediation of the incident has taken place. Sharing of this information can cause further harm to the Commonwealth if the vulnerability has not been remediated.

4.3 Incident Response Process

All Agencies shall follow the incident response process outlined in the Incident Response Process Document, which can be found on IT Central https://itcentral.pa.gov/Security/Services/IRP.pdf (Commonwealth Access only), when responding to or determining whether a Cyber Security Incident exists.

In the event a cyber security incident has been suspected or confirmed, the agency ISO shall evaluate the cyber security incident according to the following IT Security Incident Reporting Process:

Security Incident Category 1 (Critical/High)

Description / Criteria	1. The agency or EISO has determined there is an active attack on an agency system or network (e.g., denial of service or rapidly spreading malicious code); or 2. The agency or EISO has determined that other organizations' systems are affected, such as business partners or outside organizations; or 3. The agency or EISO has determined that the data involved is in the category of Sensitive Security or Protected as defined in the *Data Classification Policy*.

Alerting Requirement	The agency ISO or designate is responsible for reporting the incident to the Pennsylvania Computer Security Incident Response Team (PA-CSIRT) within thirty (30) minutes of detection. The following information, at a minimum, is required when reporting the incident: • Agency name and business unit; • The point of contact name and phone number; and • Brief description of intrusion and damages (real or anticipated). Notification can take the form of a phone call to the PA-CSIRT Incident Response Hotline at 1-877-55CSIRT (1-877-552-7478) or online at: https://grc.pa.gov/RSAarcher/apps/ArcherApp/Home.aspx#home
Incident Reporting Requirements	Within **1 hour** of detection, the agency ISO or designate is responsible for submitting the incident information online at: https://grc.pa.gov/RSAarcher/apps/ArcherApp/Home.aspx#home
Incident Remediation / Closure	Critical incidents need to be remediated/closed within **5 business days** of being reported to OA/IT/EISO. Incidents that cannot be remediated/closed during this timeframe need to have **weekly status updates** entered into the incident tracking system until the incident can be closed.

Security Incident Category 2 (Medium)

Description / Criteria	1. The agency or EISO has determined that the data involved is in the category of Privileged as defined in the *Data Classification Policy*; or 2. The incident has an impact or potential impact of: • financial loss, • loss or compromise of data, • violation of legislation/regulation, • damage to the integrity or delivery of critical goods, services, or information; or 3. The agency has been unable to resolve the incident; or 4. The vulnerability that caused the incident has not been determined or mitigated.
Alerting Requirement	The agency ISO or designate will be responsible for reporting the incident to the PA-CSIRT within **1 hour** of detection. The following information, at a minimum, is required when reporting the incident: • Agency name and business unit; • The point of contact name and phone number; and • Brief description of intrusion and damages (real or anticipated). Notification can take the form of a phone call to the PA-CSIRT Incident Response Hotline at 1-877-55CSIRT (1-877-552-7478) or online at: https://grc.pa.gov/RSAarcher/apps/ArcherApp/Home.aspx#home
Incident Reporting Requirements	Within **4 hours** of detection, the agency ISO or designate is responsible for submitting the incident information online at: https://grc.pa.gov/RSAarcher/apps/ArcherApp/Home.aspx#home
Incident Remediation / Closure	Medium incidents need to be remediated/closed within **15 business days** of being reported to OA/IT/EISO. Incidents that cannot be remediated/closed during this timeframe need to have **biweekly status updates** entered into the incident tracking system until the incident can be closed.

Security Incident Category 3 (Low)

Description / Criteria	1. The agency or EISO has determined that the data involved is in the category of Prerequisite-Required as defined in the *Data Classification Policy* or is publicly available; or 2. The agency has contained or resolved the incident.
Alerting Requirement	The agency ISO or designate will be responsible for reporting the incident to the PA-CSIRT within **1 hour** of detection. The following information, at a minimum, is required when reporting the incident: • Agency name and business unit; • The point of contact name and phone number; and • Brief description of intrusion and damages (real or anticipated). Notification can take the form of a phone call to the PA-CSIRT Incident Response Hotline at 1-877-55CSIRT (1-877-552-7478) or online at: https://grc.pa.gov/RSAarcher/apps/ArcherApp/Home.aspx#home
Incident Reporting Requirements	Within **8 hours** of detection, the agency ISO or designate is responsible for submitting the incident information online at: https://grc.pa.gov/RSAarcher/apps/ArcherApp/Home.aspx#home
Incident Remediation / Closure	Low incidents need to be remediated/closed within **20 business days** of being reported to OA/IT/EISO. Incidents that cannot be remediated/closed during this timeframe need to have **monthly status updates** entered into the incident tracking system until the incident can be closed.

5. Contact

Questions or comments may be directed via email to OA, IT Policy.

6. Exception from Policy

In the event an agency chooses to seek an exception from this policy, a request for a policy exception shall be submitted via the IT policy exception process. Refer to *IT Policy Governance Policy* for guidance.

7. Revision History

This chart contains a history of this publication's revisions. Redline documents outline the revisions and are available to Commonwealth users only during the drafting process.

Version	Date	Purpose of Revision
Original	01/06/2025	Base Document