pennsylvania
OFFICE OF ADMINISTRATION
INFORMATION TECHNOLOGY

Information Technology Policy

IT Security Incident Reporting Policy

ITP Number	**Effective Date**
ITP-SEC024	August 2, 2012
Category	**Supersedes**
Security	None
Contact	**Scheduled Review**
RA-ITCentral@pa.gov	March 2018

1. Purpose

This Information Technology Policy (ITP) establishes standard policies, procedures and standards related to the reporting and managing cyber security incidents.

2. Scope

This Information Technology Policy (ITP) applies to all departments, boards, commissions and councils under the Governor's jurisdiction. Agencies not under the Governor's jurisdiction are strongly encouraged to follow this ITP.

3. Background

The Pennsylvania Data Breach Notification Act requires notification to affected individuals in instances where personal information has been compromised. A 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.

4. Definitions

Cyber Security Incident: Any occurrence involving the unauthorized or accidental modification, destruction, disclosure, loss, damage, misuse, or access to information technology resources such as systems, files, and databases.

Data Breach: An unauthorized access and acquisition of computerized data that materially compromises the security or confidentiality of a system or personal information maintained by the entity that causes or the entity reasonably believes has caused or will cause loss or injury to any resident of this Commonwealth.

Forensic Analysis: Evidence found in computers and digital storage media as part of a formal investigation using systematic and sound methods to examine digital media with the aim of identifying, preserving, recovering, analyzing and presenting facts and opinions about the digital information.

5. Objective

Provide agencies the guidance and direction to promptly investigate IT Security incidents involving the unauthorized or accidental modification, destruction, disclosure, loss, damage, misuse, or access to information technology resources such as systems, files, and databases.

6. Policy

Office of Administration, Office for Information Technology, Enterprise Information Security Office (OA/OIT/EISO) is responsible for coordinating and leading cyber incident response when an 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/OIT/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/OIT/EISO, agency information security officers (ISO), and agency Chief Information Officers (CIO).

Scenario	EISO	Agency ISO	Agency CIO
Proactively identify potential cyber security threats and take precautions before they can cause potential to harm the Commonwealth's IT infrastructure.	X	X	
Proactively identify potential cyber security threats and take precautions before they can cause potential to harm 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 helping remediate 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 (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	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 for cyber security incident reporting and handling. Provide OA/OIT/EISO those POCs information.			X
Collaborate with business unit management to declare an outage for affected systems.	X	X	X
Act as the primary point of contact for cyber security incident response for the agency.		X	
Report incidents bi-directionally from OA/OIT/EISO via the Commonwealth reporting system. Automated SIEM process should be used where available.	X	X	

Incident Response and Countermeasures

Following the immediate response to a security incident, different countermeasure 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 and/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 will choose one or more of the following responses:

- **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 and/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 some cases, an affected asset or assets must be isolated and excluded from regular service to prevent further security incidents. Business unit management may be engaged by the agency CIO or ISO to declare an outage and invoke their disaster recovery plan.

7. Procedures

In the event an incident has been suspected or confirmed, the agency ISO is to evaluate cyber security incidents according to the following IT Security Incident Reporting Procedures:

Security Incident Category 1 (Critical/High)	
Description / Criteria	1. The agency has determined there is/was an active attack on an agency system or network (e.g., denial of service or rapidly spreading malicious code) and/or; 2. The agency has determined that other organizations' systems are affected, such as business partners or outside organizations and/or; 3. The agency has determined that the data involved is in the category of Sensitive Security or Protected as defined in ITP-SEC019.
Alerting Requirement	The agency ISO or designate is responsible for reporting the incident to the 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; • 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://oa-archer.state.pa.us/.
Incident Reporting Requirements	Within **1 hour** of detection, the agency ISO or designate is responsible for submitting the incident information online at: https://oa-archer.state.pa.us/.

Incident Remediation / Closure	Critical incidents need to be remediated/closed within **5 business days** of being reported to OA/OIT/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 has determined that the data involved is in the category of Privileged as defined in ITP-SEC019 and/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 and/or; 3. The agency has been unable to resolve the incident and/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; • 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://oa-archer.state.pa.us/.
Incident Reporting Requirements	Within **4 hours** of detection, the agency ISO or designate is responsible for submitting the incident information online at: https://oa-archer.state.pa.us/.
Incident Remediation / Closure	Medium incidents need to be remediated/closed within **15 business days** of being reported to OA/OIT/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 has determined that the data involved is in the category of Prerequisite-Required as defined in ITP-SEC019 and/or is publicly available and/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; • 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://oa-archer.state.pa.us/.

Incident Reporting Requirements	Within **8 hours** of detection, the agency ISO or designate is responsible for submitting the incident information online at: https://oa-archer.state.pa.us/.
Incident Remediation / Closure	Low incidents need to be remediated/closed within **20 business days** of being reported to OA/OIT/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.

8. Responsibilities

Agencies are to adhere to the policy and procedures of this ITP and are to put in place processes for ensuring that all users of agency systems are aware of the procedures and the importance of reporting security incidents, threats, or malfunctions that may have an impact on the security of agency information.

9. Related ITPs/Other References

Commonwealth policies, including Executive Orders, Management Directives, and IT Policies are published on the Office of Administration's public portal:
http://www.oa.pa.gov/Policies/Pages/default.aspx

- Management Directive 205.34 – *Commonwealth of Pennsylvania Information Technology Acceptable Use Policy*
- ITP-SEC000 – *Information Security Policy*
- ITP-SEC016 – *Commonwealth of Pennsylvania Information Security Officer Policy*
- ITP-SEC019 – *Policy and Procedures for Protecting Commonwealth Electronic Data*
- ITP-SEC021 – *Security Information and Event Management Policy*
- ITP-SEC025 – *Proper Use and Disclosure of Personally Identifiable Information (PII)*
- ITP-SYM006 – *IT Resources Patching Policy*
- Security Breach Checklist - https://itcentral.pa.gov/Security/Pages/Services.aspx (Limited Access)

10. Authority

Executive Order 2016-06, Enterprise Information Technology Governance

11. Publication Version Control

It is the user's responsibility to ensure they have the latest version of this publication, which appears on https://itcentral.pa.gov. Questions regarding this publication are to be directed to RA-ITCentral@pa.gov.

12. Exemption from This Policy

In the event an agency chooses to seek an exemption, for reasons such as the need to comply with requirements for a federally mandated system, a request for waiver may be submitted via the Commonwealth of PA Procurement and Architectural Review (COPPAR) process. Requests are to be entered into the COPPAR Tool located at http://coppar.oa.pa.gov/. Agency CIO approval is required.

This chart contains a history of this publication's revisions:

Version	Date	Purpose of Revision
Original	08/02/2012	Base Document
Revision	05/01/2013	Consolidated OPD- SEC022A, OPD-SEC24B, STD-SEC024C into base policy
Revision	04/02/2014	ITP Reformat
Revision	03/09/2017	• Added/Revised Definitions • Clarified and moved EISO, Agency CIO and Agency ISO responsibilities into scenario table in Policy section • Removed Computer Incident Response Technology Standard section • Revised the data category types to align with ITP-SEC019 in the Procedures section • Added Security Breach Checklist reference
Revision	03/30/2017	• Updated category tables language for clarity