COMMONWEALTH OF PENNSYLVANIA
DEPARTMENT OF PUBLIC WELFARE

INFORMATION TECHNOLOGY POLICY

Name Of Policy: **Incident Reporting & Response Policy**	Number: **POL-SEC004**
Domain: **Security**	Category:
Date Issued: **05/26/2011**	Issued By Direction Of:
Date Revised: **10/11/2013**	 Sandra Patterson, CIO Bureau of Information Systems

Table of Contents

Document History

Version	Date	Author	Status	Notes
1.0	05/26/2011	David Johnson	Draft	Initial Creation
1.0	05/31/2011	Tom Zarb	Baseline	Approved
1.1	10/11/2013	Pamela Skelton	Updation	Revised Content and formatted

1 Introduction

1.1 Purpose

This policy establishes requirements for the Department of Public Welfare's (DPW) capability to rapidly detect, contain, eradicate and recover from a broad range of information security incidents. DPW's incident response capability is a critical part of DPW's commitment to protecting citizen data and preventing disruption of government services. ITB-SEC024, IT Security Incident Reporting Policy, defines an incident as: "a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard computer security practices." An incident may result from any of the following: a failure of security controls; an attempted or actual compromise of information; and/or waste, fraud, abuse, loss, or damage of government information and/or property. An incident response capability is necessary for rapidly detecting incidents, minimizing loss, mitigating weaknesses, and restoring any disrupted services. This policy identifies the required security controls for incident response preparation; as well as incident monitoring, handling and reporting.

1.2 Scope

All DPW employees, contractors, vendors and business partners are responsible for understanding and complying with this policy.

1.3 Compliance

Violations of this policy may lead to revocation of system privileges and/or disciplinary action.

1.4 Exemptions

Requests for exemption to the policy should be submitted to the Chief Information Security Officer (CISO). Any exceptions granted will be issued a policy waiver for a defined period of time.

1.5 Policy Review and Update

This document, and its supporting standards and procedures, will be reviewed annually, and updated as needed.

2 Incident Response Plan

Preparation and planning, including ensuring that necessary plans, processes, and resources are in place; are critical to the effectiveness of DPW's incident response capability.

DPW Policy

a. DPW shall develop an Incident Response Plan, with supporting procedures, that:
   - provides a roadmap for implementing DPW's incident response capability;
   - describes the structure of the incident response capability;
   - provides a high-level approach for how the incident response capability fits into the overall organization;
   - defines reportable incidents;
   - provides metrics for measuring the incident response capability within the organization;
   - defines the resources and management support needed to effectively maintain and continually improve an incident response capability; and
   - Describes the roles and responsibilities of DPW's information security incident responders.

b. The incident response plan and supporting procedures shall be reviewed and approved by the CISO at least annually.

DPW Policy

a. The Incident Response Plan and supporting procedures shall be revised as needed, to address system/organizational changes or problems encountered during implementation, execution, or testing. Changes to the Incident Response Plan and supporting procedures shall be communicated to incident response personnel and other organizational elements as needed.

3 Incident Reporting

Timely reporting of incident information to proper authorities; as appropriate, both internal and external to DPW, is vital.

DPW Policy

a. The DPW staff, contactors, vendors and business partners will comply with DPW incident reporting requirements (IT Security Incident Reporting, POL-ENSS02), including:

- DPW staffs, contractors, Program Offices and Business Partners are to promptly complete an IT Incident Reporting Form and email it to ra-itsecurity@state.pa.us or fax it to 717-772-7163 within 1 hours of identification of the lost/stolen IT asset. In addition, DPW's CISO should be notified of all major thefts/losses, immediately via phone or email. This includes but is not limited to desktops, laptops, Blackberries, CD/DVD-ROM disks, USB memory sticks, etc. This policy also covers the loss of any data, such as confidential data being sent to the wrong person.
- Business partners and vendors shall immediately notify the respective program offices or the CISO on identification of an actual or suspected misuse of IT resources or security incident.

  DPW staff and contractors shall immediately notify their respective section chiefs or system owners upon identifying an actual or suspected misuse of IT resources or security incident. Section chiefs or system owners shall report computer security incidents to the CISO immediately upon identification of the incident occurrence.
- DPW shall report incidents using OPD-SEC024B, IT Security Incident Reporting Form. The completed form is to be submitted via e-mail to Pennsylvania-Computer Security Incident Response Team (PA-CSIRT) or online to the PA-CSIRT Web Portal.

b. DPW shall report incidents to the PA-CSIRT within 30 minutes of detection, via phone call or email.

4 Incident Handling

In order to protect information assets, DPW's security incident handling capability must provide the necessary steps for security incident detection and resolution.

DPW Policy

a. DPW shall implement an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery.

b. The CISO shall provide oversight for the incident response policies, procedures, investigations, and reporting of organizational incidents.

c. The CISO shall ensure that incident handling activities are coordinated with, and included in, contingency planning activities.

d. DPW shall employ automated mechanisms (e.g., an online incident management system or automated data collection, forensics, and analysis tools) to support the incident handling process.

e. Lessons learned from prior and ongoing incident handling activities shall be incorporated into the incident handling procedures.

5 Incident Monitoring

As part of DPW's incident response process, identified incidents are documented and tracked. Documentation of incidents is critical to provide a historical record of the actions taken to resolve an incident, as well as provide information essential to a potential or actual investigation.

DPW Policy

a. The DPW Incident Response Team shall maintain an Incident Log, to track and document information security incidents on an ongoing basis. The minimum information that shall be recorded is:
   - date and time the incident was reported, discovered or occurred;
   - who reported or discovered the incident;
   - how the incident was identified;
   - description of the incident;
   - incident-related tasks and who performed each, and the amount of time spent on each task;
   - person coordinating the incident response;
   - individuals contacted regarding the incident; and
   - Information system(s), application(s), program office(s), vendor(s), business partner(s) or network(s) impacted.

b. DPW shall ensure that relevant data from available information sources (e.g., application logs, host system logs, network logs) is included in incident documentation.

6 Incident Response Assistance

To increase the availability of incident response-related information and support, automated mechanisms are employed across the organization.

DPW Policy

a. As part of increasing understanding of current response capabilities and support, DPW shall provide a push and/or pull capability for users seeking to obtain incident response assistance through either a website to query assistance capability, or conversely have the ability to proactively send information to users.

b. The incident response assistance initiative and its supporting procedures shall be reviewed and approved by the CISO at least annually.

7 Appendix

7.1 Supporting DPW Policies

Document	Type
DPW IT Security Incident Reporting Policy (POL-ENSS02)	
ITB SEC021 - Security Information and Event Management Policy	CoPA
ITB-SEC024 - IT Security Incident Reporting Policy	CoPA
OPD-SEC024A: IT Security Incident Reporting Procedures	CoPA
OPD-SEC024B: IT Security Incident Reporting Form	CoPA
STD-SEC024C: Computer Incident Response Technology Standard	CoPA