COMMONWEALTH OF PENNSYLVANIA
DEPARTMENT OF PUBLIC WELFARE

INFORMATION TECHNOLOGY STANDARD

Name Of Standard: **Incident Reporting**	Number: **STD-ENSS027**
Domain: **Security**	Category:
Date Issued: **09/07/2012**	Issued By Direction Of:
Date Revised: **10/11/2013**	Shirley A. Monroe Shirley Monroe, Dir of Div of Tech Engineering

Abstract:

The purpose of this guideline is to describe the department's security incident reporting requirements to state and federal agencies.

Information is one of the department's most important assets and must be protected based on its value to the agency, including the value the department places on compliance with legal requirements and the protection of personal privacy. The value of information is often based on its confidentiality and integrity. The department is expected to meet state and federal regulations for establishing internal guidelines for incident reporting. Some of the key regulations include:

- Internal Revenue Service (IRS) Publication 1075
- Health Information Portability and Accountability Act (HIPAA) and associated Health Information Technology for Economic and Clinical Health (HITECH) Act
- Department of Health and Human Services (HHS) guidelines on the use the National Directory of New Hire (NDNH) and the Temporary Assistance for Needy Families (TANF) program
- Social Security Administration (SSA) – Computer Matching and Privacy Protection Act (CMPPA)
- Commonwealth of Pennsylvania Breach of Personal Information Notification Act

Internal incident reporting involves documenting and providing a detailed report to DPW management for the purposes of review future mitigation. External incident reporting involves notifying the appropriate Commonwealth and Federal authorities, as required by regulation, as well as notifying the general public where necessary.

General:

Incident Reporting – Internal Guidelines applies to the Department of Public Welfare, Pennsylvania Insurance Department (PID) and Department of Aging (collectively referred to as "Department"). The requirements outlined in this document are the guidelines for the department's CISO for reporting the incident to appropriate state and federal agencies.

Standard:

Internal Reporting

The CISO or his/her designee shall prepare an internal report for designated DPW management as soon as a potential security incident is identified or reported. The report should have the following details:

- Date and time of the incident
- Date and time the incident was discovered
- How the incident was discovered
- Description of the incident and the data involved. Include specific data elements if known, including whether the information was encrypted or protected by other means.
- Potential number of sensitive data records involved. If unknown, provide a range if possible.
- Location where the incident occurred
- Information technology involved (e.g. workstation, laptop, server, and mainframe)

The CISO shall involve the appropriate personnel (DPW Privacy Officer and system owners) to help identify the extent of the security and privacy impact. In addition, the CISO shall report to the Governor's Office of Information Technology (OIT) using the Commonwealth's incident reporting portal[2].

External Reporting

Where the security incident was discovered to have involved the breach of sensitive data records, the department's CISO and privacy officer shall make the final decision on external notification.

Information type definitions:

- Personally Identifiable Information (PII), including:

  o Name, such as full name, maiden name, mother's maiden name, or alias o Personal identification numbers, such as social security number (SSN), passport number, driver's license number, taxpayer identification number, or financial account or credit card number o Address information, such as street address or email address o Personal characteristics, including photographic image , fingerprints, handwriting, or other biometric data

- Protected Health Information (PHI), including demographic data, which relates to:

  o an individual's past, present or future physical or mental health or condition, o a provision of health care to an individual, or o past, present, or future payment for the provision of health care to the individual

- Federal Tax Information (FTI) refers to Federal Tax Returns and Return Information provided by IRS to DPW.

Where notification of Federal and Commonwealth authorities is deemed appropriate, the following agencies should be notified, depending on the type of sensitive data records involved in the breach:

Agency Name	What To Report	Contact Information	Reporting Timeframe
Department of Health and Human Services (HHS)	PII, PHI, FTI	Office of the Secretary OCRBreach@hhs.gov Office of Child Support Enforcement 215-861-4054	**500 records or more:** within 60 days **Less than 500 records:** no later than 60 days after the end of the calendar year in which the breach occurred
Internal Revenue	FTI	IRS Office of Safeguards SafeguardReports@IRS.gov	Immediate

Service (IRS)		Treasury Inspector General for Tax Administration 202-283-3001	
Social Security Administration (SSA)	PII	Refer to SSA's requirements below[1]. SSA Regional Contact Prasanna Kartha Data Exchange Contact 215-597-2354 Prasanna.Kartha@ssa.gov SSA Systems Security Contact Michael G. Johnson Acting Director 410-965-0266 Michael.G.Johnson@ssa.gov	Immediate
Centers for Medicare and Medicaid Services (CMS)	PII	CMS Action Desk by telephone at (410) 786-2580 or by e-mail notification at cms_it_services_desk@cms.hhs.gov	1 Hour
Commonwealth of Pennsylvania	PII,PHI, FTI	OA/OIT's Chief Information Security Officer (CISO) 1-877-552-7478 RA-CISO@state.pa.us Agency Office of General Counsel Governor's Office Scott Roy Deputy Chief of Staff	**Low Level Incident –** Impacted resource goes no farther than a user workstation. Criminal activity is not suspected. Maximum response time for the incident is the next business day. **Medium Level Incident –** Impacted resources include workstations, file and print servers and application data. Criminal activity is not suspected. Maximum response time for the incident is 4-8 hours. **High Level Incident –** Impacted resources include internet connectivity, public web servers, highly critical system servers, firewalls and customer data. Criminal activity is suspected. Maximum response time for the incident is 30 minutes.
Administration for Children and Families (ACF) Office of Child Support Enforcement	NDNH	Linda Boyer FPLS Information Systems Security Officer (ISSO) 202-401-5410 linda.boyer@acf.hhs.gov	Immediately upon discovery, but in no case later than one hour after discovery of the incident, the state agency shall report confirmed and suspected incidents, in either electronic or physical form,

(OCSE) Division of Federal Systems (DFS)			to the FPLS ISSO.

[1]SSA's Requirements

If DPW experiences or suspects a breach in the network or loss of PII or a security incident, which includes SSA-provided data, they must notify the United States Computer Emergency Readiness Team (US-CERT) within one hour of discovering the incident.

DPW must also notify the SSA Systems Security contact named in the agreement. If within 1 hour DPW is unable to make contact with that person, DPW must call SSA's National Network Service Center (NNSC) toll free at 877-697-4889 (select "Security and PII Reporting' from the options list).

DPW will provide updates as they become available to SSA contact, as appropriate. Refer to the worksheet provided in the agreement to facilitate gathering and organizing information about an incident.

Incident Response testing procedure

DPW shall perform an annual incident response tests using reviews, analyses and simulations similar to the Commonwealth of Pennsylvania (CoPA) Cyberstorm exercise which includes the following logical step:

- Cyberstorm is an annual exercise where all CoPA agencies, CTO and CISOs are involved and given a particular incident scenario
- The review board assess agencies preparedness and approach to resolve security incidents
- The review board advises on the agencies approach.

The incident response testing procedure are simulations exercises that shall be performed once every year involving the agency CISO, selected supervisors and executive management to assess incident response effectiveness and give a complete picture of reporting capabilities (e.g., results, trends, impacts).

In addition, simulations shall be enforced with realistic test/exercise scenarios and environments to effectively stress response capability and help developing automated mechanisms over time. Example:

Exercises typically involve several departments, teams or disciplines prompting interaction between teams in a realistic environment:

- Typical Incident response cases (unauthorized access, breach of sensitive PII data records and disaster recovery)

The results of incident response tests/exercises shall be always documented. For FTI data, the annual incident response testing procedure shall include exercise responding to unauthorized FTI access and reporting unauthorized FTI access to IRS and TIGTA. *(Refer to Pub 1075, Ref 9.9)*

<u>General Public Notification</u>

DPW CISO shall work with the OIT and DPW Press Office to notify the general public, including the impacted individuals and other press releases. (refer to the other policy encryption)

In addition to providing the incident details listed in the internal report, the external notification shall adhere to the following guidelines:

- Notice shall be given without unreasonable delay, but no later than 60 days after the breach is discovered.

• When providing notification via email, 256-bit AES encryption must be used and the pass-phrase shall be shared via a separate communication.

• Consumer reporting agencies shall be notified in breaches involving sensitive data records of more than 1000 individuals.

• Online submission to the Commonwealth OIT should be completed by the department CISO only. In the absence of CISO, the deputy CISO, Chief Technology Officer (CTO) or Chief Information Officer (CIO), in that order, shall submit the form.

Exemptions from this Standard:

Exemptions from this Standard: System owners unable to comply with this guideline must discuss any exemption request with the department's Chief Information Security Officer (CISO).

Refresh Schedule:

All standards and referenced documentation identified in this standard will be subject to review and possible revision annually or upon request by the DPW Information Technology Standards Team.

Standard Supplements:

None

References:

1. ITB-PRV001: Commonwealth of Pennsylvania Electronic Information Privacy Policy

2. ITB-SEC024: IT Security Incident Reporting Policy

3. 73 P.S. §§ 2301: Commonwealth of Pennsylvania Breach of Personal Information Notification Act

4. IRS Publication 1075, Ref 9.9: Tax Information Security Guidelines for Federal, State and Local Agencies and Entities

5. P.L. 111-5: Health Information Technology for Economic and Clinical Health (HITECH) Act

6. Department of HHS guidelines on the use of the NDNH

7. NIST 800-122: Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)

Standard Revision Log:

Change Date	Version	Change Description	Author and Organization
09/07/2012	1.0	Incident Reporting	Clifton Van Scyoc
10/11/2013	1.1	Updation	Pamela Skelton