pennsylvania
DEPARTMENT OF LABOR & INDUSTRY
OFFICE OF INFORMATION TECHNOLOGY

L&I, Office of Information Technology Procedure

Name:	Security Breach Procedure
Effective Date:	December 2016
Category:	Security
Version:	1.1

1. Scope:

This procedure applies to all Department of Labor & Industry employees and business partners.

2. Procedure:

The procedure is implemented by various IT staff under the direction of the L&I Chief Information Security Officer (CISO) under the authority of the Chief Information Officer (CIO), or Deputy Chief Information Officer (DCIO).

Step	Responsibility	Action
1.	Any L&I staff	**Make a Preliminary Assessment of the Incident** When and where did the security breach occur? What devices or paperwork were lost, stolen or breached? If devices were stolen, were they immediately reported to law enforcement? What potential data might be involved? a. An individual's name b. Social Security number c. Credit Card information d. Financial data e. Driver's license number f. State identification card number g. Health information h. Any other specific information that might identify an individual Can the data be used for fraudulent or other purposes? Is there other information at risk? How many individuals were affected by the security breach?
2.	CIO/DCIO/CISO	**Notify Appropriate People within the commonwealth** Make the following Executive Offices' contacts: • Governor's office • OA/OIT's Chief Information Security Officer (CISO) can be reached at 1-877-552-7478 or via e-mail to RA-CISO@pa.gov • Office of General Counsel (OCC) (Note: Deputy Chief of Staff, is the point of contact from the Governor's office.) Make the following internal contacts: • Deputy Secretary responsible for the business area • Deputy Secretary of Administration

		• Chief Information Officer (CIO) • Agency CISO • Communications and Press Office (CPO) • Agency OCC
3.	CIO/DCIO/CISO	**Further Evaluate the Scope of the Incident** • Does there appear to be evidence of suspicious behavior or negligence by an employee? • Was there criminal intent by an employee? If so, does the Office of Inspector General need to conduct interviews? • Has the agency completed the IT security incident form? • Does a backup of the system/data exist? • Is there a similar functioning device that can be analyzed to help determine the risk? • Does the agency's human resource department need to be involved? • If there was physical damage to a building, should the agency hire security guards? • Do the access codes for the building need to be updated? • Were users' ID and passwords disabled that might have been associated with the stolen or lost devices? • Should the agency's employees be briefed on the situation? • Has a key person within the agency been identified to monitor the progress and communicate the actions to the appropriate people identified in Step 2 of this checklist?
4.	CIO/DCIO/CPO	**Determine Need to Notify Public** • Do commonwealth employees need to be informed of the incident? • Should the public be notified of the incident? If so, consider the following: a. Develop talking points 1. Key Message 2. Next steps b. Press Release c. Press Conference d. Contact other states e. Any national associations that could assist in communicating the information to the public

		• If law enforcement was involved, did the agency consult with them to determine the timing of what and when details of the security breach could be released to the public? • Has an individual been designated as the contact person for releasing information? • Have the communication messages to employees, legislators, and the public regarding the security breach been coordinated? • When does the agency need to notify affected citizens?
5.	CIO/DCIO/CPO	**Communication to the Public** • How are affected individuals going to be notified of the potential identity theft? • Has a notification letter been prepared announcing the incident to the affected individuals? • Should a fact sheet be provided to the individuals and legislators with the following key elements? a. Outline the incident b. Explain the actions currently being taken by the agency c. Include the contact information (e.g., the toll free number and website) d. Any other pertinent information • Does a toll free number need to be established to address questions from the individuals? • Does a call center need to be established to handle the calls? • Should questions and answers be developed and shared with the individual? • Would a website be beneficial to share information with the individual on the incident and next steps? • What types of services need to be purchased for affected individuals in order to mitigate the data breach? a. Does a contract need to be setup with one of the credit bureaus to provide free credit monitoring for affected individuals? b. How often should the credit bureau track statistics and report any identity thefts to your agency? c. If a contract is established with one of the credit bureaus, how will the information be communicated to the individuals?

		d. Does a reminder letter on the credit services need to be sent to the citizens? e. When the credit bureau is unable to locate a credit file for an individual, should a notification be sent?
6.	CIO/DCIO/CISO	**Analyze Need to Address Data Security Weaknesses** • Did the agency have full disk encryption on the hardware devices? • Was the security software up-to-date? • Did the agency employ other local security measures outside of encryption (i.e., password protected files, multiple factor authentication, etc.)? • Did the agency have security procedures in place? If so, were the procedures followed? If not, do procedures need to be implemented? • Does the agency need to conduct a security assessment? • Should this type of sensitive data be stored in the current location? • Does the access to the data need to be restricted? • Was the data being saved to the network and not to the local hard drives? • If the data should be stored in that particular location, is there a way to truncate the information? • If the agency has field offices with similar security, should the alarms be tested? • Does the agency need to conduct a risk analysis and security threat assessment if items were stolen from the building?

3. References:

L&I, OIT Policy Definitions

SEC-008 – Security Incident Response Policy

Reporting Information Security Incidents

Security Incident Reporting for Social Security Administration

Security Incident Reporting for Internal Revenue Service

OA ITP-SEC024 IT Security Incident Reporting Policy

4. Version Control:

Version	Date	Purpose
1.0	08/2008	Base Document
1.1	12/2016	Reformatted, revised content