Office of Information Technology Policy

ISSUE DATE: February 12, 2009	PAGE 1 OF 2	POLICY NO: C-320

SUBJECT: Data Encryption Standards

APPROVAL AUTHORITY: OIT- Bureau of Enterprise Services, Chief Information Security Officer (CISO)

Authorization:

This policy is published under the general authority of the Security Domain Information Technology Bulletins published by the Office of Administration / Office of Information Technology (OA/OIT), in that it identifies key roles and responsibilities in support of Information Technology Bulletins (ITBs) relating to the encryption of critical data (reference OA **ITB-SEC020** Encryption Standards for Data at Rest & OA **ITB-SEC031** Encryption Standards for Data in Transit).

Purpose:

To create a standardize list of Labor & Industry (L&I) data that is to be encrypted in all application databases - for the Department.

The primary support and coordination of reported information security incidents will be completed by: Office of Information Technology (OIT) Bureau of Enterprise Services (BES) Chief Information Security Officer (CISO).

Background:

L&I data, especially data which pertains to the citizens of the Commonwealth of Pennsylvania, is a valuable asset that we are required to take every possible measure to protect. In order to add another pertinent layer to this protection strategy, all data that falls into the categories outlined in this policy will require some form of encryption to ensure it is protected while in transit and at rest in the applications that support our program areas.

Scope:

This policy applies to all databases for all L&I applications that may hold the information defined below, regardless if that data is part of an OIT-supported application or not.

Definitions:

Data Requiring Encryption:

- **Citizens and Employees**
  - Personal Identifiable Information (PII) as defined in Gramm-Leach-Bliley Act (GLBA)
    - e.g. Social Security Numbers (SSN), driver license number…
  - Financial Data
    - Credit/Debit card information
      - Strictly follows Payment Card Industry (PCI) guidelines
    - Bank Routing information
  - Health Insurance Portability and Accountability Act (HIPAA) data
    - All medical data directly associated with any individual
- **Business Partner Information**
  - Federal Employer Identification Number (FEIN)

        - Tax ID's and other uniquely identifiable business information reported to the Department
            - This information could be an individual's SSN in some instances
- **Common security elements**
    - Passwords, account (Personal Identification Numbers (PINS), security codes

This policy recognizes that other data may need to be treated as high risk due to the possible damage if disclosed or modified. The data owner (Program Areas) should make this determination on a case-by-case basis working with the L&I OIT CISO.

Responsibilities:

- **Department Agencies/Program Areas:** To correctly identify and classify critical data housed in their area of responsibilities databases that may require encryption.
- **OIT Bureau of Enterprise Architecture Database Administrator's & OIT Bureau of Business Application Development:** To provide the methods and ability to protect data deemed critical and/or as classified by the Departments Program Areas in compliance with this policy.

Policy Interpretation:

This policy is issued in light of other guidance issued by OA/OIT, as well as existing laws, policies, and agreements of the Commonwealth of Pennsylvania. Where possible, this policy should be construed in a manner consistent with such other guidance, laws, policies, and agreements.

Questions concerning the interpretation of this policy may be referred to the DLI CISO and designates. Please direct questions to: RA-LI-OIT-DLICISO@state.pa.us.

References:

L&I/OIT Related Policies:	**C-300** Computer and Information Security
OA/OIT ITB:	**ITB-SEC020** Encryption Standards for Data at Rest **ITB-SEC031** Encryption Standards for Data in Transit **ITB-PRV001** CoP Electronic Information Privacy Policy