Information Technology Policy
Commonwealth of Pennsylvania
Governor's Office of Administration/Office for Information Technology

ITP Number:	**ITP-PRV001**	
ITP Title:	**Commonwealth of Pennsylvania Electronic Information Privacy Policy**	
Issued by:	**Deputy Secretary for Information Technology**	
Date Issued: August 7, 2006		**Date Revised: November 18, 2010**
Domain:	**Privacy**	
Discipline:	**Privacy**	
Technology Area:	**Privacy**	
Revision History Date:	**Description:**	
11/18/2010	**ITP Refresh**	

Abstract:

The purpose of this Information Technology Policy (ITP) is to define the Commonwealth Electronic Information Privacy Policy. This ITP will also provide guidance for implementation of this policy at an agency level.

With increased concern surrounding information security and privacy, federal and state legislation regarding electronic information in a variety of business areas has emerged over the last several years. These include:

- Health
  Health Information Portability and Accountability Act (HIPAA) Of 1996
- Financial
  Sarbanes-Oxley Act of 2002
  Gramm-Leach-Bliley Act
- Identity
  Real ID Act of 2005
- Public Safety
  Pennsylvania Criminal History Record Information Act (CHRIA), 18 Pa. C.S.A Section 9101 et seq
- General
  Federal Privacy Act of 1974
  Pennsylvania House Resolution 351

Information privacy pertains to both paper and electronic information. Electronic information can be accessed from a multitude of technologies, including, but not limited to:

- Internet/Intranet/Extranet sites and applications;
- Internal client-server and mainframe applications; and
- Data storage devices.

As the Commonwealth continues to develop the Internet as a key communication vehicle, visitors accessing Commonwealth Web sites are to be provided with a policy that encompasses a collection of online information online so these users can make informed choices about interacting with the Commonwealth electronically.

Also, the Commonwealth is to ensure that agencies enforce and meet all federal and state legislative mandates related to information privacy and security for each system interacting with electronic information.

The Privacy Domain Team was engaged:

- to set electronic information privacy standards for the Commonwealth;
- to provide standards to ensure federal and state electronic information privacy directives are met; and
- to review forthcoming legislation with regard to its impact upon existing standards.

General:

This ITP applies to all departments, boards, commissions and councils under the governor's jurisdiction. Agencies not under the governor's jurisdiction are encouraged to follow this policy to ensure they develop and implement applications that facilitate enterprise-wide interoperability and standardization.

Policy:

This policy establishes the Commonwealth's electronic information privacy standards specific to the following areas:

- E-government Web Sites - Outlines standards for agency e-government Web sites and applications with respect to privacy considerations;
- Agency Electronic Information Confidentiality Agreement/Statement- Provides guidance for the creation and enforcement of agency electronic information confidentiality statements; and
- Creating/Maintaining Auditable Data - Provides guidance for categorization of data and user types for authentication and access logging for use in audits.

Agencies are responsible for annually reporting compliance with this policy to the office of Administration/Office for Information Technology (OA/OIT). If there are areas in which an agency is not compliant, the agency is to provide a planned course of action to bring the agency within compliance of this policy.

E-government Web Sites

All agencies will publish the *Commonwealth of Pennsylvania E-government Privacy Statement* for all Web-based applications.

All agency "home" pages and e-government applications will link to the privacy statement defined in the *Pennsylvania Privacy Policy*, located at: http://www.portal.state.pa.us/portal/server.pt?open=514&objID=377333&mode=2.

Agencies are responsible for ensuring agency Web sites and applications are in adherence with this privacy statement.

Agency Electronic Information Confidentiality Agreement

Each agency is to provide a confidentiality agreement defining the responsibilities of the agency's employees and business partners (e.g., contractors, vendors) in maintaining the privacy of that agency's electronic information. Per ITP-PRV002, *Electronic Information Privacy Officer*, the agency electronic information privacy officer, in conjunction with the agency human resources department, is responsible for the development and administration of this confidentiality agreement.

The agency confidentiality agreement is to:

- identify the state and federal legislation that applies to the agency-specific business;
- identify relevant policies the agency is to meet (i.e., agency level);
- clarify that use of and access to electronic information is audited;
- address ongoing responsibility for an employee to maintain, upon departure from the agency, the privacy of electronic information the individual was privy to during employment with the agency, pursuant to Commonwealth policy (i.e., ITP-PTL007); and
- include a signature sheet, which includes name and date of signature.

All Commonwealth employees and business partners who are required to access the Internet via the Commonwealth Metropolitan Area Network (MAN) are to verify through signature that they have read and accepted the terms of the agreement. All signed signature sheets are to be maintained by each agency in the appropriate office (i.e., human resources, information technology, privacy officer).

Agencies are to maintain signature sheets for a period of time in compliance with Commonwealth document retention policies including, but not limited to, Management Directive 210.5, *Records Management*.

The agency confidentiality agreement may include additional agency-specific information deemed appropriate by the agency electronic information privacy officer.

Creating/Maintaining Auditable Data
Agencies are to categorize both data and users permitted to access various categories of electronic information, based on the guidelines provided below and the agency-specific business drivers. In addition, agencies are to determine and identify all electronic information access activities that are to be logged, based on the categorized electronic information. Agencies are to capture and maintain, at a minimum, the required log data as defined below.

Types of data
Electronic information is to be broken into the following categories:

- Statutorily Protected - electronic information defined by state or federal statute which has business-specific privacy definitions; and
- Unprotected - electronic information not specifically defined by state or federal statute as protected or public. Agencies can determine how this data may be used.

For any electronic information defined as "statutorily protected," as well as data that agencies opt to maintain log/audit information for, agencies are to maintain a log/history of all transactions resulting in inserts, updates, and deletes. Agencies are to also have the capability to capture log information for inquiry requests.

For electronic information not defined as "statutorily protected," the agencies' discretion prevails as to whether log information is maintained.

Types of users
Users are to be broken into the following categories:

- *Employee* - employee roles for accessing electronic information as part of the definition of the job (i.e., roles for determining user access to systems);
- *Public* - general public users;
- *Auditor* - individual with specific business need to access electronic information for purposes of performing audits;
- *Other Agency* - other CoPA agencies with a business need to access electronic information; and
- *Business Partner* - users defined as business partners based on agency specification.

Auditable logs
Based on the type of electronic information and user access, agencies are responsible for maintaining auditable logs for electronic information access as specified by their applicable state and federal legislation.

Audit/log information is to include:

- user identification;
- user level (type of user);
- date and time of activity;
- type of activity (insertion, update, deletion, read/request); and
- key value or identifier for record accessed.

Privacy Impact Assessments (PIA)
Agencies are to, at a minimum, conduct an annual privacy impact assessment on all systems and data to ensure that all data and user access is categorized appropriately. Results of this annual survey are to be available for review by the OA Privacy Officer upon request. The agency electronic information privacy officer is responsible for ensuring these provisions are met.

Agencies are to also conduct a PIA when they begin to develop a new or significantly modified IT system.

PIA Content
The annual and/or periodic PIA is to contain the following information:

1. Analysis and description of the statutorily protected electronic information that is collected by the agency;
2. Explanation of why this information is collected;
3. Description of how the agency utilizes this information, including those categories of users which have access to the data and why;
4. Description of with whom the information can be and is shared, including the types of categorized users;
5. Description of any notice or opportunities for consent that would be provided to individuals regarding what information is collected and how that information is shared;
6. Description of how this information is to be secured; and
7. Description of how access to this information is logged/archived in coordination with ITP-PRV001.

Refresh Schedule:
All standards identified in this ITP are subject to periodic review and possible revision, or upon request by the Enterprise Architecture Standards Committee (EASC).

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. Contact your agency CoP Planner for further details or assistance.

Questions:
Questions regarding this policy are to be directed to RA-ITCentral@pa.gov.

References:
Management Directive 210.5: Records Management
ITP-PLT007 Commonwealth of PA Data Cleansing Policy
ITP-PRV002 Electronic Information Privacy Officer