pennsylvania
OFFICE OF ADMINISTRATION
INFORMATION TECHNOLOGY

Information Technology Policy

Commonwealth of PA Electronic Information Privacy Policy

ITP Number ITP-PRV001	**Effective Date** August 07, 2006
Category Privacy	**Supersedes** None
Contact RA-ITCentral@pa.gov	**Scheduled Review** March 2019

1. Purpose

Establishes guidance on the management of privacy of Commonwealth electronic information.

2. Scope

This Information Technology Policy (ITP) applies to all departments, boards, commissions and councils under the Governor's jurisdiction. Agencies not under the Governor's jurisdiction are strongly encouraged to follow this ITP.

3. Background

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.

To address the privacy and protection of information, federal and state governments have developed the following legislative mandates (not a full listing):

Health
Health Insurance Portability and Accountability Act (HIPAA) of 1996
Centers for Medicare & Medicaid Services (CMS) Minimum Acceptable Risk Standards for Exchanges (MARS-E)
Confidentiality of HIV-Related Information Act, 35 P.S. §§ 7601 et. seq.
Disease Prevention and Control Law of 1955, 35 P.S. §§ 521.1 et. seq.

Financial
Sarbanes-Oxley Act of 2002
Gramm-Leach-Bliley Act
Internal Revenue Service (IRS) Publication 1075 Safeguards Privacy and Audit Requirements

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
Commonwealth of Pennsylvania Breach of Personal Information Notification Act (73 P.S. §

2301 et seq.)
Family Educational Rights and Privacy Act (FERPA)

Visitors accessing Commonwealth websites are to be provided with a policy that encompasses a collection of information online so these users can make informed choices about interacting with the Commonwealth electronically. The Commonwealth is to ensure that agencies enforce and meet all federal and state legislative mandates related to information privacy for each system interacting with electronic information.

4. Policy

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

- Commonwealth-Owned Websites - Outlines standards for commonwealth-owned websites and applications with respect to privacy considerations;
- Agency Electronic Information Confidentiality Agreement - Provides guidance for the creation and enforcement of agency electronic information confidentiality agreements;
- Creating/Maintaining Auditable Data - Provides guidance for categorization of data and user types for authentication and access logging for use in audits;
- Privacy Impact Assessment – Annual review of in-scope information technology (IT) systems.

Agencies are responsible for annually reporting compliance with this policy to the Office of Administration/Office for Information Technology Enterprise (OA/OIT Enterprise). 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.

Commonwealth-Owned Websites

All Commonwealth-owned websites and web-based applications will link to the privacy statement defined in the Pennsylvania Privacy Policy, located at: http://www.pa.gov/privacy-policy/. Refer to ITP-SFT002 *Commonwealth of PA Website Standards* for additional guidance on the management of agency-owned web sites. Agencies are responsible for ensuring agency websites 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 may include additional agency-specific information deemed appropriate by the agency electronic information privacy officer.

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; and
- Include a signature sheet, which includes name and date of signature.

All Commonwealth employees and business partners 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.

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

<u>Creating/Maintaining Auditable Data</u>

Agencies are to categorize both data and users permitted to access various categories of electronic information, based on the guidelines provided ITP-SEC019 *Policy and Procedures for Protecting Commonwealth Electronic Data*. Agencies are to determine and identify all electronic information access activities that are to be logged, based on the categorized electronic information and are to capture and maintain, at a minimum, the required log data as defined below.

Log Data Requirements

For any electronic information defined as Sensitive Security, Protected, or Privileged as defined in ITP-SEC019, 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 have the capability to capture log information for inquiry requests.

For electronic information defined as Prerequisite-Required as defined in ITP-SEC019, 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/contractor roles for accessing electronic information as part of the definition of the job;
- *Public* – citizen, business, non-commonwealth-related users;
- *Auditor* - individual with specific business need to access electronic information for purposes of performing audits;
- *Other Agency* - other Commonwealth 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.

At a minimum, 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.

<u>Privacy Impact Assessments (PIA)</u>

Agencies are to conduct a PIA when they begin to develop a new or significantly modified information technology system as well as conduct an annual privacy impact assessment on all information technology 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 Office of Administration upon request. The agency electronic information privacy officer is responsible for ensuring these provisions are met. Agencies are to use OPD-PRV001A *Privacy Impact Assessment Template* to document the assessment findings.

PIA Content

The PIA is to contain, at a minimum, the following information:

1. Analysis and description of the Sensitive Security, Protected, or Privileged 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 this policy; and
8. Detail laws, policies, directives, standards, and other privacy-related requirements that apply to data; and
9. Detail potential impact to organizations or individuals should a breach occur.

5. Responsibilities

Commonwealth agencies under the Governor's jurisdiction are to actively manage their websites, applications, and other electronic assets to ensure proper privacy protections are in place. This includes:

- Point all in-scope websites and applications to the to the privacy statement defined in the Pennsylvania Privacy Policy

- Obtaining and retaining all required confidentiality agreements

- Adhering the Log Data Requirements

- Conducting annual privacy impact assessments (PIA), using OPD-PRV001A *Privacy Impact Assessment Template* to document the assessment findings

6. Related ITPs/Other References

Commonwealth policies, including Executive Orders, Management Directives, and IT Policies are published on the Office of Administration's public portal: http://www.oa.pa.gov/Policies/Pages/default.aspx

- Management Directive 205.34 *Commonwealth of Pennsylvania Information Technology Acceptable Use Policy*
- Management Directive 210.5 – *The Commonwealth of Pennsylvania State Records Management Program*
- Pennsylvania Privacy Policy statement: http://www.pa.gov/privacy-policy/
- OPD-PRV001A *Privacy Impact Assessment Template*
- ITP-PRV002 – *Electronic Information Privacy Officer*
- ITP-SEC000 – *Information Security Policy*
- ITP-SEC015 – *Data Cleansing Policy*
- ITP-SEC019 – *Policies and Procedures for Protecting Commonwealth Electronic Data*
- ITP-SEC024 – *IT Security Incident Reporting Policy*
- ITP-SFT002 – *Commonwealth of PA Website Standards*
- NIST SP 800-122 – *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)*

7. Authority

Executive Order 2016-06, Enterprise Information Technology Governance

8. Publication Version Control

It is the user's responsibility to ensure they have the latest version of this publication, which appears on https://itcentral.pa.gov for Commonwealth personnel and on the Office of Administration public portal: http://www.oa.pa.gov/Policies/Pages/default.aspx. Questions regarding this publication are to be directed to RA-ITCentral@pa.gov.

9. 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.

This chart contains a history of this publication's revisions:

Version	Date	Purpose of Revision
Original	08/07/2006	Base Document
Revision	03/01/2017	ITP format revision (no policy revisions) Updated Privacy Policy URL Updated ITP references

Revision	03/23/2018	Annual Review Clarified language throughout Corrected HIPAA name in Background section Added additional regulation references Removed Privacy Domain Team references Revised the Log Data Requirements subsection Added OPD-PRV001A *Privacy Impact Assessment Template* Added reference to ITP-SFT002 Added Responsibilities section