Privacy Policy

Effective Date:
January 06, 2025

Category:
Privacy

Scheduled Review:
January 2026

Supersedes:
ITP-PRV001, ITP-PRV002, OPD-PRV001A

1. Authority

Executive Order 2016-06, Enterprise Information Technology Governance

2. Purpose

This Information Technology Policy (ITP) sets forth designation and responsibilities of the Privacy Officer (PO).

3. Scope

This policy applies to all offices, departments, boards, commissions, and councils under the Governor's jurisdiction and any other entity connecting to the Commonwealth Network (hereinafter referred to as "agencies").

4. Policy

For definitions found within this document, refer to the *IT Policy Glossary*.

4.1 Privacy Officer Assignment

4.1.1 Privacy Officer (PO) Assignment

The Deputy Secretary of Administration for each agency shall identify and designate a Commonwealth employee who will serve as the Agency Privacy Officer (APO). The APO is to be a separate individual from the agency's Information Security Officer. Each agency Deputy Secretary for Administration shall notify the Chief Privacy Officer (CPO) in writing identifying the APO and acknowledging compliance with this policy. In the event of staff changes or reassignment of the APO role, the agency Deputy Secretary is to notify the CPO immediately.

4.1.2 Privacy Officer Minimum Responsibilities

With increased concern surrounding information security and privacy, federal and state legislation has emerged regarding information in a variety of business areas. These include, but are not limited to:

- Health
- Health Information Portability and Accountability Act of (HIPAA) 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 found in a multitude of platforms:

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

Visitors accessing Commonwealth websites are to be presented with a policy that encompasses a collection of online information 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.

The Chief Privacy Officer (CPO) is engaged:

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

The Agency Privacy Officer (APO) minimum responsibilities are, but not limited to:

- Enforcing the Privacy Policy requirements within the agency as defined herein.
- Setting and providing privacy standards to ensure all applicable

federal, state, and other mandates specific to privacy concerns pertaining to the agency areas are met and enforced, and to review forthcoming legislation with regard to its impact upon existing standards.

- Ensuring that all applicable federal, state, and other mandates specific to privacy concerns that pertain to the agency areas are met and enforced.
- Defining the categories of information and categories of users to be identified for the agency.
- Notifying the Chief Privacy Officer (CPO) of concerns regarding the agency's compliance with either this policy or other state/federal business-related privacy directives.
- Developing and providing, in conjunction with the agency human resources department, 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 information. 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 information is audited.
    - Address ongoing responsibility for an employee to maintain, upon departure from the agency, the privacy of information the individual had access to during employment with the agency, pursuant to Commonwealth policy.
    - Include a signature sheet, which contains name and date of signature.
    - Ensure all Commonwealth employees and business partners verify through signature that they have read and accepted the terms of the confidentiality agreement.
    - Ensure all signed confidentiality agreements are maintained by each agency for a period in compliance with Commonwealth document retention policies.

- Annually reporting compliance with this policy to the Chief Privacy Officer. 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 into compliance with this policy.

4.1.3 Agency and Enterprise Collaboration

The Privacy Officer shall have the capability and authority to raise concerns, issues, and report problems and cyber security incidents to their Enterprise counterpart (Enterprise Privacy Officer) as appropriate via the chain of command.

4.1.4 Enforcement and Escalation

Areas subject to enforcement:

- E-government Websites – Outlines standards for agency e-government Websites

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
- Creating/Maintaining Auditable Data – Provides guidance for categorization of data and user types for authentication and access logging for use in audits

If the APO determines that the agency is not in continuous compliance with the standards set forth in this policy, the APO may utilize the following escalation procedures. This list may include steps outside of the APO's normal chain of command.

The following procedures should be used for escalation of agency privacy compliance issues:

1. The APO determines that the agency is not in continuous compliance with any aspect of this policy.
2. The APO provides written notification of the issue to the agency chief information officer (CIO), chief privacy officer (CPO), and any other personnel deemed appropriate. If an immediate solution to the issue can be identified, then the issue is resolved.
3. If an immediate resolution cannot be reached, the APO will schedule a meeting with all pertinent parties within two weeks of notification about the issue.
4. If the APO is unable to schedule this meeting due to lack of response from pertinent parties, the APO will notify, in writing, the Chief Privacy Officer about the issue (see escalation procedures below).
5. In the scheduled meeting the group will determine a projected deadline and a remediation plan based upon the severity of the noncompliance.
6. The APO will monitor agency progress against the remediation plan and projected deadline.
7. If the remediation plan is successfully completed, the issue is resolved.
8. If the projected deadline is not achieved, at the APO's discretion, the APO will notify, in writing, the CPO about the issue (see escalation procedures below).
9. If the agency is making efforts toward the corrective action and a reasonable modified deadline is created, the APO is not required to notify the CPO unless otherwise directed by the CPO.
10. If notified by the APO of an issue, the CPO will monitor agency progress against the revised remediation plan and projected deadline(s).

The CPO will notify in writing and schedule a meeting with the APO and agency CIO, in which the agency participates, as appropriate, upon escalation of an issue by an agency APO. This meeting will establish responsible parties, next steps, and deadlines.

The APO may escalate a privacy issue in the following situations:

1. The agency does not meet and/or enforce applicable federal, state, and other mandates specific to information privacy, provided the APO discusses the situation with Agency Legal Counsel prior to escalation;
2. The agency has not completed the reporting responsibilities to CPO regarding the agency's compliance with this policy;
3. The agency does not categorize information and users in accordance with this policy;
4. The agency does not distribute and maintain an agency information confidentiality agreement; or
5. The agency does not comply with this policy in any other areas identified by the APO.

Notification to the CPO must be in writing and should include the following:

1. A description of the non-compliance issue, including, as appropriate, the system(s), statutory obligations, etc.
2. A description of actions, if any, taken to date in an attempt to correct the issue.

4.2 Privacy Impact Assessments

Agencies are to conduct a Privacy Impact Assessment (PIA) when developing a new or significantly modified information technology system as well as to 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 Chief Privacy Officer upon request. The Agency Privacy Officer is responsible for ensuring the provisions of the Privacy Officer Policy are met. Agencies will use the Privacy Impact Assessment Template in the next section to document the assessment findings.

4.2.1 Privacy Impact Assessment Template

Detailed Analysis of Data Collection:
Analysis and description of the Sensitive Security, Protected, or Privileged information that is collected by the agency

Explanation:
Explanation of why this information is collected

Description of Data Usage:
Description of how the agency utilizes this information, including those categories of users which have access to the data and why

Description of Data Sharing:
Description of who the information can be and is shared, including the types of categorized users

Notification of Consent:
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

Data Security:
Description of how this information is to be secured

Access Logs and Archiving:
Description of how access to this information is logged/archived in accordance with this policy

Applicable Requirements Detail:
Detail laws, policies, directives, standards, and other privacy-related requirements that apply to data

Breach Impact:
Detail potential impact to organizations or individuals should a breach occur

4.2.2 Legislative Mandates

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)

4.2.3 Privacy Standards

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.

4.2.3.1 Commonwealth-Owned Websites

All Commonwealth-owned websites and web-based applications will link to the privacy statement defined in the Pennsylvania Privacy Policy. Refer to *Software Development Life Cycle (SDLC) Policy* for additional guidance on the management of agency-owned websites. Agencies are responsible for ensuring agency websites and applications are in adherence with this privacy statement.

4.2.4 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 in *Data Classification Policy*. 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.

4.2.4.1 Log Data Requirements

For any electronic information defined as Sensitive Security, Protected, or Privileged as defined in the *Data Classification Policy*, as well as additional data that agencies opt to maintain log/audit information, 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 the *Data Classification Policy*, the agency's discretion prevails as to whether log information is maintained.

4.2.4.2 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 users
- *Auditor* - individual with specific business need to access information for purposes of performing audits
- *Other Agency* - other Commonwealth agencies with a business need to

access information
- *Business Partner* - users defined as business partners based on agency specification

4.2.4.3 Auditable logs

Based on the type of information and user access, agencies are responsible for maintaining auditable logs for 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)
- key value or identifier for record accessed

5. Contact

Questions or comments may be directed via email to OA, IT Policy.

6. Exception from Policy

In the event an agency chooses to seek an exception from this policy, a request for a policy exception shall be submitted via the IT policy exception process. Refer to *IT Policy Governance Policy* for guidance.

7. Revision History

This chart contains a history of this publication's revisions. Redline documents outline the revisions and are available to Commonwealth users only during the drafting process.

Version	Date	Purpose of Revision
Original	01/06/2025	Base Document