pennsylvania
OFFICE OF ADMINISTRATION
INFORMATION TECHNOLOGY

Information Technology Policy

Proper Use and Disclosure of Personally Identifiable Information (PII)

ITP Number	***Effective Date***
ITP-SEC025	March 19, 2010
Category	***Supersedes***
Recommended Policy	
Contact	***Scheduled Review***
RA-ITCentral@pa.gov	Annual

This Information Technology Policy (ITP) establishes guidelines for the proper electronic use and disclosure of Personally Identifiable Information.

1. Purpose

This policy provides guidelines for the exercise of agency discretion in creating policies and procedures on the proper electronic use and disclosure of Personally Identifiable Information (PII).

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. Policy

It is the intent of the Office of Administration/Office of Information Technology (OA/OIT) to take the necessary precautions to protect the identity of all of its constituents by minimizing or eliminating the electronic use of Personally Identifiable Information (PII) for identification purposes. All applications collecting PII must comply with applicable laws and be vetted through the CA^2 process.

For the purposes of this policy, the term "PII" is used by OA/OIT in the same way it is used by NIST and OMB (as referenced in NIST800-122: Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)), to mean "any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information." By way of further example, PII includes:

- Driver's license number or a State identification card number issued in lieu of a driver's license.
- Passport number.
- Identifying information that must be protected under any policy, law or other requirement

applicable to an agency.

Identifying PII

Agencies are responsible for identifying and classifying all PII generated, collected, stored, used, and disclosed by the agency or by a third party on the agency's behalf.

Collecting PII

Agencies must limit the generation, collection, storage, use and disclosure of PII to that which is necessary for business purposes only, and must further limit generation, collection, storage, use and disclosure of PII to the ***minimum*** PII necessary for the accomplishment of those business purposes.

Systems which are vendor or agency hosted shall use PII as data elements only and not as keys to databases. PII may be used for identification purposes or as identifiers only to address a business necessity, and only if allowed by applicable law and/or regulations/mandates.

Displaying PII

Systems which are vendor or agency hosted shall not display PII visually, whether on computer monitors, or on printed forms or other system output, unless required by any law or other requirement applicable to an agency, or business necessity.

PII Used in Test Environments

PII data used in staging, development, or test environments (as well as production environments) shall be secured properly in accordance with commonwealth ITP's and any law or other requirement applicable to an agency in order to prevent unauthorized use or disclosure. It is recommended that "simulated" PII data be used in test and development environments.

Unique Identifiers

Systems developed by an agency, third party or contracted provider or business partner that require a unique identifier shall not use PII as that identifier. All systems which must assign an identifying number for an individual must assign a unique identification number that is not the same as or cannot be traced back to users PII. Security must be applied, and care must be taken to ensure that access the electronic system and use of these unique identification numbers are restricted in accordance with any law or other requirement applicable to an agency.

Transferring PII

PII moved from one computer to another over an un-trusted network* must be transferred using encryption controls to protect data integrity and confidentiality. Agency legal review may be required, and is otherwise recommended, to ensure appropriate limits and processes are applied to any PII data transfer between commonwealth agencies, business partners, or external entities. See ITP-SEC019 - *Policy and Procedures for Protecting Commonwealth Electronic Data*

**This requirement does not apply when transferring PII between two hosts on the same secure/firewalled subnet.*

Maintaining PII

All agency entities maintaining files utilizing PII for any purpose shall ensure that access or use of such information is properly controlled, encrypted and restricted to prevent unauthorized use or disclosure, and that the retention period is minimized based upon business necessity.

Legacy Systems

Owners of legacy information systems that use PII as keys or indexes in their databases AND which are not specifically required to do so by any law, regulation, reporting requirement or other mandate must have an action plan and timeline for remediation.

Disclosure of PII

Data breaches involving PII must be reported via the requirements outlined in ITP-SEC024 - *IT Security Incident Reporting Policy*, regardless of other law or requirements that may be applicable to a particular breach. Breaches for the purpose of reporting under SEC024 include breaches of data in electronic or in paper form. Agencies or business partners are also required to follow, as appropriate, any mandates pertaining to breach found in any law or other requirement applicable to an agency.

4. Responsibilities

Agencies are to put in place processes for ensuring that all users of agency systems are aware of the procedures and the importance of reporting security incidents, threats, or malfunctions that may have an impact on the security of agency information.

5. References

- ITP-SEC005 - Commonwealth Application Certification and Accreditation
- ITP-SEC019 - Policy and Procedures for Protecting Commonwealth Electronic Data
- ITP-SEC020 - Encryption Standards for Data at Rest
- ITP-SEC024 - IT Security Incident Reporting Policy
    - ITP-SEC031 - Encryption Standards for Data in Transit
    - NIST800-122 - Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)
    - Breach of Personal Information Notification Act: 73 P.S. § 2301
    - HIPAA regulations: 45 CFR 160.101
    - Sarbanes Oxley: 15 USCS § 7201
    - Payment Card Industry Standards

6. Authority

- Executive Order 2011-05, Enterprise Information Technology Governance

7. Publication Version Control

It is the user's responsibility to ensure they have the latest version of this publication. Questions regarding this publication are to be directed to RA-itcentral@pa.gov.

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

Version	Date	Purpose of Revision
Original	3/19/2010	Base Policy
Revision	5/17/2011	Changed ITB # from 36 to 25
Revision	10/7/2011	Policy updated to reflect EASC comments
Revision	4/20/2012	Policy updated to reflect OA-Legal comments
	4/2/2014	ITP Reformat