Board Information Technology Policy

Policy and Procedures for Protecting PMRS Electronic Data

Board Policy 2023-02

Effective Date
November 16, 2007

Category
Security

Scheduled Review -
Annually

Any reference to the Commonwealth in this policy includes the Pennsylvania Municipal Retirement Board, the Pennsylvania Municipal Retirement System (PMRS) and PMRS' contractors and consultants

1. Purpose

This Information Technology Policy (ITP) addresses the policies and procedures for the safe transmittal, transport, storage, and overall protection of Commonwealth electronic data.

2. Scope

This ITP 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").

Third-party vendors, licensors, contractors, or suppliers shall meet the policy requirements of this ITP as outlined in the Responsibilities section.

3. Background

There are many forms of electronic records within the Commonwealth that require special treatment or heightened protections. These types of electronic records are known as closed or "C" Classification records.

Another form of electronic records is Public Records, also known as Open Records. For policy guidance on the handling of Public Records, refer to *Management Directive 205.36, Right-to-Know Law Compliance* and *Management Directive 210.5, The Commonwealth of Pennsylvania State Records Management Program*. A data classification table listing any protection requirements for Public Records can be found in Section 6A of this ITP (*Policy, Data Classification Tables*).

Commonwealth employees and contractors shall identify the Classification of

electronic records consistent with *ITP-INF015, Policy and Procedures for Identifying, Classifying, and Categorizing Commonwealth Electronic Data* and protect this information from improper disclosure based on the Classification of the records.

Categorization of data will follow the NIST SP 800-60 Rev 1 terminology, leveraging the security impact levels for data types and information systems. This activity determines the level of security controls to be implemented from NIST SP 800-53 Rev 5.

4. Definitions

Categorization: is the process of placing data into groups or types of data that are in some way similar to each other, based on characteristics of the data.

Classification: is the process of assigning labels to data according to a predetermined set of principles, which define that data class based on the treatment and use of the data.

For example, both apples and tomatoes are fruit (Categorization), but tomatoes are not typically added to fruit salad (Classification).

Commonwealth Enterprise Storage Solutions: are information technology services, applications, or programs either procured, obtained, created, or licensed by the Office of Administration for the storage or maintenance of records, data, or other information controlled, maintained, or possessed by the Commonwealth and its agencies. Commonwealth Enterprise Storage Solutions include, but are not limited to, the suite of applications provided as part of Microsoft 365 (Outlook 365, OneDrive, SharePoint, etc.) and the PACS environment (Pennsylvania Compute Services).

Public Records: also known as **Open Records,** are records from an agency that are: not exempt under Section 708 of the Right to Know Law; not exempt from being disclosed under any other Federal or State law or regulation, or judicial order or degree; and not protected by privilege.

Printed Media: is the physical copy made of a digital item either mechanically or electronically.

5. Policy

"C" Classification Records or Closed Records

The use of a "C" designation indicates that all or part of the record requires special treatment or heightened protections, including, but not limited to, non-disclosure to the public, non-disclosure to any person without a need to know, non-disclosure outside of certain workgroups, non-disclosure without certain prerequisites, etc. Agencies shall follow *ITP-INF015, Policy and Procedures for Identifying, Classifying, and Categorizing Commonwealth Electronic Data* for direction on classification.

Closed or "C" records shall be placed into one of the following Classifications:

- Sensitive Security Information
- Protected Information
- Privileged Information
- Prerequisite-Required Information

6. Procedures

- Agencies shall categorize and classify all data pursuant with *ITP-INF015, Policy and Procedures for Identifying, Classifying, and Categorizing Commonwealth Electronic Data*.

- "C" designated electronic records shall be stored in an approved storage solution. Approved storage solutions include:
  - Commonwealth Enterprise Storage Solutions;
  - Agency On Premise Data Centers;
  - Commonwealth Data Centers; or
  - Other storage facilities approved in writing by the Agency Information Security Officer (ISO) or equivalent.

- No "C" designated electronic records can leave an approved storage solution without prior electronic approval from the Agency ISO or equivalent. Additionally, all requests for information relating to "C" designated electronic records must be made in writing to the Agency ISO.

- Encryption standards are outlined in *ITP-SEC031, Encryption Standards* and shall be followed for any actions that specify encrypting data under the "C" Classification.

- Encryption protection mechanisms detailed below in the Data Classification Tables shall be followed.

- Systems that store, process, transmit, or otherwise handle the following categories of data: Sensitive Security, Protected, or Privileged must be protected with a Web Application Firewall (WAF) or Database Firewall (DBFW) as follows:
  - Web Application Firewalls must be utilized to protect Internet accessible web sites and services.
  - DBFW must be utilized to protect Database related systems.
  - Agencies designing modernized and new database-related systems shall include DBFW configurations to meet DBFW data owner requirements and future requirements to ensure the highest level of required security controls.
  - Agencies shall evaluate the impact of third-party WAF and DBFW agents on their computing resources prior to the deployment of the WAF and DBFW agents.

- Systems that store, process, transmit, or otherwise handle prerequisite-Required or Public Records may be protected with a WAF or DBFW as follows:
  - WFAs may be utilized to protect Internet accessible web sites and services.
  - DBFW may be utilized to protect database related systems.
  - Agencies designing modernized and new database-related systems shall include DBFW configurations to meet DBFW data owner requirements and future requirements to ensure the highest level of required security controls.
  - Agencies shall evaluate the impact of third-party WAF and DBFW agents on their computing resources prior to the deployment of the WAF and DBFW agents.

7. Data Classification Tables

The following data Classification tables pertain to electronic records and details the requirements for the various levels of protection determined by the various forms of data and transmission methods pertaining to:

- Sensitive Security Information
- Protected Information
- Privileged Information
- Prerequisite-Required Information
- Public Records

SENSITIVE SECURITY INFORMATION

Action	Requirement
Storage on Fixed Media	Encrypted
Storage on Exchangeable Media	Encrypted
Creation of Printed Media	Information owner should designate which data is allowed to be further duplicated or distributed.
Faxing	Transmitted over an encrypted link to password-protected mailbox or, if sent to a public or multi-user fax machine, received (printed) using Attended Receipt
Sending by Public Network	Encrypted
Sending over Agency Network	Encrypted (refer to *ITP-SEC031, Encryption Standards*)
Disposal	Electronic data or media on which it is stored shall be sanitized or destroyed per *ITP-SEC015, Data Cleansing Policy*, subject to any applicable records retention requirements
Release to Third Parties	Owner Approval and Non-Disclosure Agreement
Electronic Media Labeling Required	External and Internal Labels
Internal and External email	Addressed to Specific Person but Label only on Inside
Packaging	Security Envelope
Granting Access Rights	Data Owner Only
Tracking distribution and lifecycle of electronic data	Ensure that the actions of individual information system users can be uniquely traced to those users so they can be held accountable for their actions.
Web Application Firewall and/or Database Firewall	Required (for Web Applications/Services or Database systems)

PROTECTED INFORMATION

Action	Requirement
Storage on Fixed Media	Encrypted
Storage on Exchangeable Media	Encrypted
Creation of Printed Media	Information owner should designate which data is allowed to be further duplicated or distributed.
Faxing	Transmitted over an encrypted link to a password- protected mailbox or, if sent to a public or multi- user fax machine, received (printed) using Attended Receipt

Sending by Public Network	Encrypted
Sending over Agency Network	Encrypted (refer to *ITP-SEC031, Encryption Standards*)
Disposal	Electronic data or media on which it is stored shall be sanitized or destroyed per *ITP-SEC015, Data Cleansing Policy*, subject to any applicable records retention- requirements
Release to Third Parties	Owner Approval and Non-Disclosure Agreement
Electronic Media Labeling Required	External and Internal Labels
Internal and External email	Addressed to Specific Person but Label only on Inside
Granting Access Rights	Data Owner Only
Tracking distribution and lifecycle of electronic data	Ensure that the actions of individual information system users can be uniquely traced to those users so they can be held accountable for their actions.
Web Application Firewall and/or Database Firewall	Required (for Web Applications/Services or Database systems)

PRIVILEGED INFORMATION

Action	**Requirement**
Storage on Fixed Media	Encrypted
Storage on Exchangeable Media	Encrypted
Creation of Printed Media	Information owner should designate which data is allowed to be further duplicated or distributed.
Faxing	Transmitted over an encrypted link to a password-protected mailbox or, if sent to a public or multi-user fax machine, received (printed) using Attended Receipt
Sending by Public Network	Encrypted
Sending over Agency Network	Encrypted (refer to *ITP-SEC031, Encryption Standards*)
Disposal	Electronic data or media on which it is stored shall be sanitized or destroyed per *ITP-SEC015, Data Cleansing Policy*, subject to any applicable records retention requirements
Release to Third Parties	Owner Approval and Non-Disclosure Agreement
Electronic Media Labeling Required	External and Internal Labels
Internal and External email	Addressed to Specific Person but Label only on Inside
Granting Access Rights	Data Owner Only
Tracking distribution and lifecycle of electronic data	Ensure that the actions of individual information system users can be uniquely traced to those users so they can be held accountable for their actions.
Web Application Firewall and/or Database Firewall	Required (for Web Applications/Services or Database systems)

PREREQUISITE-REQUIRED INFORMATION

Action	Requirement
Storage on Fixed Media	Encrypted
Storage on Exchangeable Media	Encrypted
Creation of Printed Media	Information owner should designate which data is allowed to be further duplicated or distributed.
Faxing	Transmitted over an encrypted link to a password-protected mailbox or, if sent to a public or multi-user fax machine, received (printed) using Attended Receipt
Sending by Public Network	Encrypted
Sending over Agency Network	Encrypted (refer to *ITP-SEC031, Encryption Standards*)
Disposal	Electronic data or media on which it is stored shall be sanitized or destroyed per *ITP-SEC015, Data Cleansing Policy*, subject to any applicable records retention requirements
Release to Third Parties	Non-Disclosure Agreement
Electronic Media Labeling Required	No Label Required
Internal and External email	Addressed to Specific Person but Label only on Inside
Granting Access Rights	Data Owner, Agency Legal
Tracking distribution and lifecycle of electronic data	Ensure that the actions of individual information system users can be uniquely traced to those users so they can be held accountable for their actions.
Web Application Firewall and/or Database Firewall	Recommended (for Web Applications/Services or Database systems)

PUBLIC RECORDS

Action	Requirement
Storage on Fixed Media	No restrictions
Storage on Exchangeable Media	No restrictions
Creation of Printed Media	No restrictions
Faxing	No restrictions
Sending by Public Network	No restrictions
Sending Over Agency Network	No restrictions
Disposal	No restrictions
Release to Third Parties	No restrictions
Electronic Media Labeling Required	No restrictions
Internal and External email	No restrictions
Granting Access Rights	Preapproval required for unrestricted access by Agency Legal and Business Owner
Tracking distribution and lifecycle of electronic data	Logging of initial recipients
Web Application Firewall or Database Firewall	Recommended

8. Responsibilities

8.3 Agencies Shall:
Comply with the requirements as outlined in this ITP.

8.2 Office of Administration, Office for Information Technology shall:
Comply with the requirements as outlined in this ITP.

8.3 Third-party vendors, licensors, contractors, or suppliers shall:

- Utilize a web application firewall (WAF) to protect data classified under this policy as Class "C", utilizing the standards set forth in *ITP-SEC004, Enterprise Web Application Firewall*.
- Encrypt "C" class data at rest to include, using encryption standards forth in *ITP-SEC031, Encryption Standards* and the National Institute of Standards and Technology (NIST) Cryptographic Module Validation Program.
    - For Criminal Justice Information, encryption must also meet CJIS policy requirements.
    - For systems receiving, processing, or storing Federal Tax Information (FTI), must meet IRS Publication 1075 requirements.

9. Related ITPs/Other References

- Definitions of associated terms of this policy are published on the Office of Administration's public portal: http://www.oa.pa.gov/Policies/Pages/Glossary.aspx
- 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 Amended, Commonwealth of Pennsylvania Information Technology Acceptable Use Policy*
- *Management Directive 205.36, Right-to-Know Law Compliance*
- *Management Directive 210.5, The Commonwealth of Pennsylvania State Records Management Program*
- *Breach of Personal Information Notification Act, Act of December 22, 2005, P.L. 474, No. 94, as amended, 73 P.S. §§ 2301-2329*
- *IRS Publication 1075, Tax Information Security Guidelines for Federal, State, and Local Agencies*
- *ITP-INFRM001, The Life Cycle of Records: General Policy Statement*
- *ITP-INF015, Policy & Procedures for Identifying, Classifying, and Categorizing Commonwealth Electronic Data*
- *ITP-SEC000, Information Security Policy*
- *ITP-SEC004, Enterprise Web Application Firewall*
- *ITP-SEC015, Data Cleansing Policy*
- *ITP-SEC023, Information Technology Security Assessment and Testing Policy*

- *ITP-SEC025, Proper Use and Disclosure of Personally Identifiable Information (PII)*
- *ITP-SEC031, Encryption Standards*
- *NIST SP 800-53 Rev 5, Security and Privacy Controls for Federal Information Systems and Organizations*
- *NIST SP 800-60 Rev. 1, Guide for Mapping Types of Information and Information Systems to Security Categories*
- *Office of Open Records, Right-to-Know Law Statue*
- *CJIS Policy*

10. Authority

- *Executive Order 2016-06, Enterprise Information Technology Governance*
- *Executive Order 2019–04, "Citizen-First" Government and Promoting Customer Service Transformation*
- *Executive Order 2016-07 Amended, Open Data, Data Management, and Data Governance*

11. Publication Version Control

It is the Authorized 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 shall be directed to RA-ITCentral@pa.gov.

12. Exemption from this Policy

In the event an agency chooses to seek an exemption from the guidance within this ITP, a request for a policy waiver shall be submitted via the enterprise IT policy waiver process. Refer to *ITP-BUS004, IT Policy Waiver Review Process* for guidance.

This chart contains a history of this publication's revisions. Redline documents detail the revisions and are available to CWOPA users only.

Version	Date	Purpose of Revision	Redline Link
Original	11/16/2007	Base Policy	N/A
Revision	04/02/2014	ITP Reformat; Merged GEN-SEC019A into ITP	N/A
Revision	08/20/2015	Expanded Scope Section Revised Background Section Clarified Sensitive Security Information "C" data category Expanded Protected Information "C" data category language Added Privileged Information "C" data category (including within Reference Guide Section) Replaced Exempt Information, replaced with Prerequisite-Required Information "C" data category Expanded the Policy Section Added Data Inventory sub section Expanded Related ITPs/Other References Section Added OPD-SEC019A (Data Categorization and Inventory Operating Template) supporting document	N/A

Revision	05/25/2018	Added Web Application Firewall and Database Firewall language in Policy section Added Web Application Firewall and Database Firewall in Data Classification Tables Added Encryption requirement for Prerequisite-Required data	N/A
Revision	9/9/2020	Distinguished between categorization and classification Expanded related ITPs/Other references to include Management Directives for open records Added table for open records	N/A
Revision	12/17/2020	Included language under "C" designated electronic records to include storage solutions. Changed approval from Commonwealth Chief Information Security Officer to Agency Information Security Officer. Added Commonwealth Enterprise Storage Solution definition	N/A
Revision	05/06/2022	Updated Scope, Definitions, Responsibilities and Policy References. Added third party vendor language and links. Updated requirements for encryption, logging, and creation of printed media for classifications within the charts. Updated term Open Records to Public Records. Updated requirements in Public Records chart. Updated requirements in "C" class electronic records to ensure consistency. WAF and/or DBFW made requirement for Sensitive Security, Protected and Privileged. WAF and/or DBFW made recommended for Pre-requisite required.	N/A
Revision	09/21/2022	Policy was split between Protection and Identifying, Classifying and Categorizing (latter items moved to INF015). Section 5 Classification – moved language to IN015 left summary and reference to new ITP. Details on classification types moved to INF015. Renamed section to Policy, Section 6 renamed to Procedures – updated to removed details on categorizing and added reference to INF015. Moved Data Inventory to INF015. Updated 3rd party responsibilities to reflect updated ITP. Responsibilities related to identifying, classifying, and categorizing were moved to INF015. Updated references OPD-SEC019A was transitioned to INF015A.	Revised IT Policy Redline <09/21/2022>

Adopted by the Pennsylvania Municipal Retirement Board, March 16, 2023

Barry Sherman, Chair