pennsylvania
OFFICE OF ADMINISTRATION

Information Technology Policy

Enterprise Data and Information Management Policy

Number ITP-INF000	**Effective Date** July 11, 2016
Category Information	**Supersedes** All Prior Versions
Contact RA-ITCentral@pa.gov	**Scheduled Review** June 2023

1. Purpose

This Information Technology Policy (ITP) provides direction for effectively managing data and Information Life Cycles.

2. Scope

This ITP applies to all departments, offices, boards, commissions, and councils under the Governor's jurisdiction (hereinafter referred to as "agencies"). Agencies not under the Governor's jurisdiction are strongly encouraged to follow this ITP.

Third party vendors, licensors, contractors, or suppliers shall meet the policy requirements of this ITP that are applicable to the products and services provided to the Commonwealth.

3. Definitions

3.1 **Authentic Record:** A record that is what it purports to be; it was duly issued by an authorized person or Agency and has been preserved without any alteration that would impair its use as an Authentic Record.

3.2 **Dataset:** An organized collection of data.

3.3 **Data Exchange:** Data from a source system that is restructured for the target system for the purpose of accurately representing the source data. Data Exchanges rely on implementing data languages such as Extensible Markup Language (XML) and JavaScript Object Notation (JSON).

3.4 **Data Migration:** Utilizing a design for data extraction and data loading for the purpose of permanently relocating data from one system/application to another system/application.

3.5 **Information:** Any communication or representation of knowledge such as facts, data, or opinions in any medium or form, including textual, numerical, graphic, cartographic, narrative, or audiovisual forms.

3.6 **Information Asset:** Information relevant to the enterprise's business functions, including captured and tacit knowledge of employees, customers or business partners; data and Information stored in highly-structured databases; data and Information stored in textual form and in less-structured databases such as messages, e-mail, workflow content and spreadsheets; Information stored in digital and paper documents; purchased content; and public content from the internet or other sources.

3.7 **Information Life Cycle:** The stages through which Information passes, typically characterized as creation or collection, processing, dissemination, use, storage, and disposition.

3.8 **Master Data Management Plan:** An agency-specific document developed by the agency's data/information governance body that documents the governance operating model, data processes (collection, reporting, release), data roadmaps, data acquisition/integration methodologies, and other relevant procedures.

3.9 **Metadata:** Information that describes various facets of an Information Asset to improve its usability throughout its life cycle.

3.10 **Mosaic Effect:** An event in which Datasets that pose no disclosure threat by themselves can create a security risk or produce Personally Identifiable Information (PII) when combined with other Datasets.

3.11 **Record:** Information, regardless of physical form or characteristics, that documents a transaction or activity of an agency and that is created, received, or retained pursuant to law or in connection with a transaction, business or activity of the agency.

3.12 **Records System:** An information technology resource used to generate either an electronic or physical record that is based on business rules and processes.

4. Policy

Data and Information are valuable and strategic assets to the Commonwealth of Pennsylvania, its business partners, and the public. In order to ensure that agencies are taking full advantage of their information resources, it is imperative for agencies to manage data and Information as assets throughout its life cycle. Utilizing best practices for data and Information Life Cycles will increase operational efficiencies, reduce costs, improve services, support mission needs, and safeguard sensitive Information.

Agencies shall read and comply with the following sections of this ITP, which will provide the agencies with specific information, guidelines and best practices to help institutionalize the principles of effective information management at each stage of the Information Life Cycle:

4.1 Data and Information Life Cycle Best Practices

Agencies must consider, at each stage of the data and Information Life Cycle, the effects of decisions and actions on other stages of the life cycle. Reference ITP-INFRM001 *The Life Cycle of Records: General Policy Statement*. Agencies should design new information collection and creation efforts so that the information collected or created supports downstream interoperability between information systems, as appropriate, without the need for costly retrofitting. This includes consideration and consultation of key target audiences for the information when determining format, frequency of update, and other information management decisions. Specifically, agencies should incorporate the following components into future information collection and creation efforts:

4.1.1 Develop a data governance structure

Data governance must be aligned with the design and development tasks within the organization's system development life cycle. This permeates the lifetime of data management from the analysis and synthesis of data consumer requirements through conceptual modeling, logical and physical design, and subsequent implementation.

Agencies should establish a data governance structure that develops an agency Master Data Management Plan which captures the governance operating model, the data processes, roadmaps, and various data management methodologies. The governance structure responsibilities also include drafting policies, proposing policies at both agency and enterprise levels, and implementing and adopting these policies into the agency's business and technical environments.

The Master Data Management Plan should address the following components:

A. **Data integration and sharing capabilities**. Increasing reliability, performance, and access to data sources as well as adopting a standard model for Data Exchanges (infrastructure, software, methodologies) ensures successful internal and external sharing of data, which will provide value to the enterprise by potentially reducing cost and other maintenance resources.

B. **Metadata management**. The modern digital enterprise information management must enable business-oriented Metadata management, including procedures, processes, and tools for:

1. Business term glossaries to capture frequently used business terms and their authoritative definition(s).
2. Data standards such as naming conventions, defined reference data sets, and standards for storage and exchange. (Metadata standards and specifications must be reviewed for compliance with the common core Metadata standards, specifications, and formats developed within different communities (e.g., financial, health, geospatial, law enforcement)).
3. Data element definitions that reflect the connection to business terms and provide context-relevant definitions for use within business applications.
4. Data lineage that shows the relationships between data element concepts and their representation across different models and

applications.

5. Integration with data governance policies to support validation, compliance, and control.
6. Protection of the Metadata for a record from unauthorized deletion or alteration.
7. Procedures for retention or deleting in accordance with the record's retention schedule.
8. Migration and validation strategies for Metadata to ensure preservationand integrity during the transfer of Metadata and records.
9. Metadata associated with a record is to be categorized in at least one of the following:
   a. Identity - information identifying the record.
   b. Description - information determining the nature of the record.
   c. Use - information facilitating immediate and longer-term record use.
   d. Event plan - information used to manage the record, such as disposition information.
   e. Event history - information recording past events on the record and its Metadata
   f. Relation - information describing the relationship between the record and other records.

Records Systems should define Metadata to: 1) enable the identification and retrieval of records, 2) associate records with changing business rules, policies, and mandates, 3) associate records with agents, and their authorizations and rights with regards to the records, 4) associate records with their business activities, 5) track processes carried out on records, and 6) track relationships with other records. The Records System should provide the ability to filter and sort report data based on the values contained in anyfield or column.

Metadata should be utilized to detail information about a record and should capture the following:

1. the description of the content of the record;
2. the structure of the record (form, format, and relationships between record components);
3. the business context in which the record was created, including the author and date of creation;
4. relationships with other records and Metadata;
5. a unique identifier and other information needed to retrieve the record; and
6. the business actions and events involving the record throughout its existence.

Once the record has been captured, the associated Metadata must be fixed and kept as transactional evidence.

C. File formats. The file format in which organizational entities keep their data is a primary factor in providing the ability to properly integrate, share, and use data sets across organizational boundaries. To facilitate data integration and sharing, agencies should establish policies, standards, and procedures for file organization and formats to include/address the following elements:

1. File Version Control;
2. Directory Structure/File Naming Conventions;
3. File Naming Conventions for Specific Disciplines;
4. File Structure;

5. File change tracking and logs;
6. Use Same Structure for Backups;
7. Hardware and hardware obsolescence;
8. Short-term and long-term storage file formats; and
9. Structure for Backups & Recover.

4.1.2 Develop and maintain data inventory and classification procedures

Maintain a complete up-to-date inventory of all Data Exchanges between systems (with internal and external entities) and data systems used to store and process data. The data inventory should specify what data elements are collected, origin or source of the data elements, justification for their collection, explanation of the intended purposes for use, and the data elements classification by type and their sensitivity levels. Agencies must update their enterprise data inventory, accounting for Datasets used in the agency's information systems. If the inventory does not already exist, it can be built out over time, with the ultimate goal of including all agency Datasets, to the extent practicable. Refer to ITP-SEC019 *Policy and Procedures for Protecting Commonwealth Electronic Data* and OPD-SEC019A *Data Categorization and Inventory Operating Template* for data inventory guidance.

NOTE: Records can represent more than one business activity and therefore can be assigned to more than one record category.

4.1.3 Ensure data integrity and integration

Identify strategies for ensuring the accuracy and quality of data as well as preventing, detecting, and correcting errors and misuses of data. Establish data quality standards to ensure that the data is accurate, relevant, timely, and complete for the purposes it is intended to be used with an appropriate balance between privacy and security.

Periodic quality audits should be integrated into all cycles of data managements (e.g., collection, reporting, and release).

The key to providing and sharing data between systems is to determine packaging (files, transactions, data streams, etc.), content and formatting (values, formats, etc.) and package Metadata details (location, origin, availability, changes, etc.). This component also defines methods to allow data availability, such as support for internally and externally delivered content, production support and change control (errors, fixes, versions, etc.) and interface and access to allow data delivery. To improve data integration and sharing, these fundamental capabilities should be established:

A. **Data Accessibility.** A vital aspect of data integration is accessibility, and the information management framework must provide connectors to that wide variety of data sources, including file-based, tree-structured data sets, relational databases, and even streamed data sources.

B. **Data transformation, exchange, and delivery.** Establish controls, mechanisms, procedures, and integration frameworks for data sets to be accessed from their original sources, and efficiently move the data from source to target destinations in an effective and secure manor. There must be a capability to transform the data from its original format into one that is suited to the target, with a means of verifying that the data sets are appropriately packaged and delivered securely. Controls and tests should be performed that data was transformed accurately and completely (e.g. before and after snapshots of record counts/dollar amounts, control totals).

C. Data Retention Policy. Per MD 210.5 The Commonwealth of Pennsylvania State Records Management Program, all Commonwealth employees are to manage records under their care and control. Each agency has a records coordinator to assist in getting paper, electronic and mixed media records scheduled in their agency specific records retention and disposition schedule. Agencies must control any proposed deletion of records pursuant to existing Agency Specific and Commonwealth General Records Retention and Disposition Schedules.

D. Ownership and Privacy. Agencies shall ensure that due care and diligence is exercised to make sure that they have considered the implications of sharing data, in terms of copyright, intellectual property ownership, and ethical requirements such as privacy and confidentiality.

4.1.4 Data Quality Management

A record is considered reliable if it ensures a full and accurate representation of the transactions or activities. A record is considered to have integrity if it is complete and unaltered. A record must be able to provide adequate and proper documentation of agency business for as long as the information is needed.

Institute best practices for data quality management to ensure reliability and integrity. In addition, data quality management practices are to be used to improve the precision of identifying data flaws and errors as well as simplify the analysis and remediation of root causes of data flaws. Leveraging data quality tools and techniques to support the ability to standardize and potentially correct data when possible, flag issues when they are identified, notify the appropriate data steward, and facilitate the communication of potential data issues to the source data providers. These objectives can be met within a formal framework for data quality management that incorporates techniques for:

1. Data parsing and standardization: Scanning data values with the intentof transforming non-standard representations into standard formats.
2. Data correction and cleansing: Applying data quality rules to correct recognized data errors as a way of cleansing the data and eliminating inconsistencies.
3. Data quality rules management: Centrally manage data quality requirements and rules for validation and verification of compliance with data expectations.
4. Data quality measurement and reporting: Provide a framework for invoking services to validate data against data rules and report anomalies and data flaws.
5. Standardized data integration validation: Continual validation of

existing data integration processes and embedded verification of newly developed data integration processes.

6. Data quality assessment: Source data assessments (e.g., real time, generated, or compiled) and evaluation of data issues to identify potential data quality rules using data profiling and other statistical tools.

7. Incident management: Standardized approaches to data quality incident management (reporting, analysis/evaluation, prioritization, remediation, tracking).

4.1.5 Data Storage and Retrieval

Agencies should identify the useful life of their data and establish policies, procedures, and governance frameworks for the proper storage and retrieval of their data whether it be short term or long-term preservation of their data. Agency data owners and stewards should consult with records coordinators, business owners, legal, privacy officer, security, and other stakeholders to determine the useful life, retention schedule, access frequency, security, and appropriate storage, retrieval, backup, and recovery requirements of their data. Key elements that should be considered in this area are:

1. Useful Life of Data and Information.
2. Criticality and sensitivity of data and information.
3. Records Management and Retention Schedules.
4. Hardware and hardware obsolescence.
5. Backup Medium, Systems, and Schedules.
6. Backup integrity/validation checks.
7. Continuity of Government and Disaster Recovery.
8. Security controls and safeguards
9. Storage Facilities (e.g., Geographical Locations, Cloud, or On-Premise).
10. Contractual Terms & Conditions for third party providers.
11. Appropriate environmental conditions to increase the lifespan of media

4.1.6 Implement Effective Internal Controls

Agencies must adhere to the internal control framework outlined in Management Directive 325.12 *Amended, Standards for Enterprise Risk Management in Commonwealth Agencies* in order to develop effective data management processes. This directive establishes policy, responsibilities, and procedures for implementing effective internal control systems within agencies. With this directive, the Commonwealth adopted the U.S. Government Accountability Office's Standards for Internal Control in the Federal Government (often referred to as Green Book).The Federal Internal Control Standards can be found at https://www.gao.gov/greenbook/overview.

4.2 Data Migration Procedures and Best Practices

Agencies should continuously review their records schedules to determine if changes to their use of technology affects the value of the records in question. Ensuring usability of records includes carrying out system upgrades of hardware and software while maintaining the functionality and integrity of the electronic records created in them. This includes ensuring that migration of records addresses non-active electronic records stored off-line.

Agencies must utilize OPD-INF000A *Migration Audit Checklist Template* to facilitate all Data Migration initiatives that follow under this policy's definition of Data Migration (see Definitions section). Agencies may add additional criteria to OPD-INF000A in order to satisfy business requirements, mandates, audits, or other legal requirements. The completed OPD-INFO000A must be retained, utilizing proper records management procedures to satisfy any audit requests.

NOTE: The *Migration Audit Checklist Template* may have items that do not apply to all Data Migration initiatives. Agencies should determine appropriateness of each checklist item as it relates to their Data Migration initiative on a case-by-case basis.

Original source data must be retained for a *minimum* of five (5) business days after a successful Data Migration and validated in live production environments. Evidence that data validation procedures were completed and results of, and support for, those validations should be maintained for a minimum of three (3) years for audit purposes.

Any deletion of original source data after the minimum five (5) business day retention period should be authorized and approved by the business owner of the data, which may be contingent on one or more of the following criteria:

1. Business owner concurrence of a successful Data Migration that has been completely validated in live production environments.
2. Compliance with business data/records retention schedule and/or policies.
3. Deployment strategies to run parallel systems (original and target systems) for extended time periods or business cycles.

NOTE: When migrating records, all metadata must be preserved and accompanied with the transfer.

Agencies should define methodologies, policies, procedures, tools, and governance frameworks to manage the Data Migrations (i.e. movement of data from an old or legacy system to a new system or information systems modernization) and replication that enable rapid bulk transfers of large data sets securely and accurately.

Establish mechanisms to monitor system logs, trigger updates to the target systems as changes happen at the source and record periodic extractions from source systems and loading into data warehouses or backup and recovery systems. When performing Data Migrations, Agencies should have a Data Migration plan that is recommended to include, but not limited to, the following elements:

A. Pre-migration Environment Analysis and Impact Assessment

1. Evaluate previous Data Migration initiatives to capture lessons learned, re-use of project artifacts.
2. Sponsors and key stakeholder involvement (e.g., business and IT communities, and others).
3. Evaluate the scope and complexity of the migration initiative.
4. Access the data types and volume to be migrated.
5. Analyze the migration approach, options, and activities to be performed.
6. Scope the data being migrated (remove non-value added, non-required, or historical data).
7. Examine the viability, risks, level of effort, resources, timeframe, constraints, security, dependencies, and impacts.
8. Migration initiative involvement with third-party entities and cross-organizational support.
9. Skills, competencies, and subject matter expertise needs and availability.
10. Software, hardware, licensing, tools, systems requirements, capabilities, and availability to support migration relative to both the source and target environments.
11. Legacy environment decommission requirements, strategy, and approach.
12. Affiliated contractual, policies, procurements, SLAs, and/or legal considerations.

B. Cost and funding availability associated with the Data Migration Design

Blueprint

1. Create a high-level source to target mapping to identify objects and relationships that will be linked and/or translated during the migration.
2. Create conceptual/logical/physical models to define the structures, attributes, configurations, and specifications of the source and target environments.
3. Design a detailed Data Migration mapping of source to target.
4. Data backup schedules (i.e., source and target environments).
5. Data restoration and recovery procedures.
6. Design for any interfaces that are required to extract, clean/scrub, and translate the data from your legacy systems or to load the data into the target systems.
7. Define an executable legacy systems decommission roadmap.
8. Design the test strategy and plan that outlines the following:

   - What will be tested and by whom?
   - Sequence, interdependencies, cycle, and duration of tests to be performed.
   - Test environment requirements, configurations, and preparations.
   - Test pass/fail criteria.
   - Test procedures, pre and post conditions for test scripts and environments.
   - Test schedule.
   - Test and validation checklists.

- Test results reviews and approvals.
- Retests.

9. Define a data quality management plan to include the following elements:

    - Outline the criteria to ensure and validate the integrity, accuracy, and security of the data before and after Data Migration.
    - Define processes and procedures for Data Migration records exception and error handling and resolution procedures.
    - Outline processes and procedures for identifying, categorizing, prioritizing, documenting, and tracking defects, root cause, and corresponding resolution status.
    - Establish on-going reviews of predefined task, inspection, testing, and validation checklists to guide, facilitate awareness, and determining Data Migration status, conditions, risks, issues, and outcomes.
    - Define business and systems operational readiness assessments with final acceptance criteria

C. Data Migration Planning, Execution, and Validation

Create a formal Data Migration plan with the following elements:

1. Data Migration playbook with check lists defining gateposts for “Go” and “No-Go” decision criteria.
2. Ownership, roles, responsibilities, and resources to perform the Data Migration tasks.
3. Integrated quality controls and assurance as defined in the quality plan.
4. Building, configuration, and testing of the source and target environments and associated tools to support Data Migration initiative.
5. Building, testing, and validating the effectiveness and accuracy of mechanisms and utilities used for data extractions, cleaning, conversions, translations, and loading between source and target systems.
6. Conducting pilots or test runs as required to refine/validate Data Migration design approach, mappings, testing approach, and estimated durations to complete Data Migration.
7. Evaluate and refinement of the Data Migration test plan.
8. Backup of original source data for recovery, restoration, and business continuity.
9. Retention schedule and storage of original source data and systems for validation, recovery, restoration, and business continuity.
10. Data owner approvals and authorizations for deletion/purging of original source data.
11. Source and target data sets comparisons (e.g., total number of data elements, size, record counts, dollar amounts, etc.).
12. Legacy environment decommissioning roadmap execution.

13. Executing and monitoring each of the Data Migration tasks in alignment with predefined playbook.
14. Communications Plan.
15. Risk and issues management plan.
16. Project schedule with key milestones and deliverables.
17. Conduct and assess business and systems operational readiness assessments in order to make recommendations and determinations for final approval and sign-off.
18. Post execution monitoring, impact assessments, and reporting for latent data anomalies and/or defects.
19. Data Migration project closeout and lessons learned.

4.3 Security of Data and Information

Establishing a comprehensive data security management plan with checks, controls, and systems is critical to prevent, identify and mitigate security risks, which will ensure the security of sensitive data (data that carry the risk for harm from an unauthorized or inadvertent disclosure) and PII. Agencies should regularly review their data security management plans and processes and initiate change management processes as needed to remain up to date as to the latest threats and ensure compliance with security policies and legislation.

Agencies should regularly monitor and evaluate their records controls including monitoring and reviewing access rights and permission rules for electronic records regularly; these access rights and permission rules should be updated on a regular basis. Any actions changing the level of access, altering the record, or changing the location of the record must be documented and tracked in an audit log.

As agencies consider security-related restrictions for handling data and information, focus should be centered on information confidentiality, integrity, and availability as part of the agency's overall risk management framework. In addition to all Commonwealth IT policies and management directives, agencies should reference and consider incorporating the National Institute of Standards and Technology (NIST) Federal Information Processing Standards Publication (FIPS-PUB) 199 *Standards for Security Categorization of Federal Information and Information Systems* and (FIPS-BUS) 200 *Minimum Security Requirements for Federal Information and Information Systems*. Agencies should also review the National Strategy for Information Sharing and Safeguarding and NIST guidance on Security and Privacy Controls for Federal Information Systems and Organizations.

Ensuring compliance with security IT policies can be accomplished by clearly specifying all activities related to handling data by data stewards as well as users; defining who can access what data, for what purpose, when, and how; and outlining guidance about the appropriate managerial and user data activities for handling records throughout all stages of the data life cycle, including acquiring, maintaining, using, and archiving or destroying both regular and secure data records with mechanisms for de-identifying PII data in order to protect individual privacy for information systems development and testing purposes.

As a security best practice, Agencies should:

1. Ensure that once a record has been captured into a records system, all events and actions related to the record by person entities and non-person entities are documented on an on-going basis.
2. Collect or create only data or information necessary for the proper performance of agency functions and business requirements and which has practical utility;
3. Limit the collection or creation of data or information which identifies individuals to that which is legally authorized and necessary for the proper performance of agency functions and business requirements;
4. Limit the sharing of data or information that identifies individuals or contains proprietary information to that which is legally authorized, and impose appropriate conditions on use where a continuing obligation to ensure the confidentiality of the information exists;
5. Ensure that information is protected commensurate with the risk and magnitude of the harm that would result from the loss, misuse, or unauthorized access to or modification of such information; and
6. Take into account other publicly available information when determining whether particular information should be considered PII.

5. Responsibilities

5.1 Agencies are recommended to follow the best practices outlined in this policy and are required to:

- Adhere to Management Directive 325.12 *Amended, Standards for Enterprise Risk Management in Commonwealth Agencies*.
- Maintain a complete up-to-date inventory of all Data Exchanges between systems (with internal and external entities) and data systems used to store and process data.
- Follow and complete the OPD-INF000A *Migration Audit Checklist Template* and maintain the complete checklist following the appropriate records management procedures for all Data Migration initiatives.
- Retain Data Migration source data for a minimum five (5) business days after a successful Data Migration and validation in live production environments. Evidence that data validation procedures were completed and results of, and support for, those validations should be maintained for a minimum of three (3) years for audit purposes.

5.2 Third-party vendors, licensors, contractors, or suppliers shall comply with the requirements outlined in this ITP.

6. 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 210.5 The *Commonwealth of Pennsylvania State Records Management Program*
- Management Directive 325.12 Amended *Standards for Enterprise Risk Management in Commonwealth Agencies*
- Manual 210.1 The *Commonwealth of Pennsylvania Employee Records Management Manual*
- Manual 210.7 *State Records Management Manual*
- Manual 210.9 Amended - *The Commonwealth of Pennsylvania General Records Retention and Disposition Schedule*
- Executive Order 1992-01 *Records Management*
- Executive Order 2016-07 Amended - *Open Data, Data Management, and Data Governance*
- OPD-INF000A *Migration Audit Checklist Template*
- ITP-INFRM001 *The Life Cycle of Records: General Policy Statement*
- ITP-SFT008 *Enterprise Resource Planning (ERP) Management*
- ITP-SEC019 *Policy and Procedures for Protecting Commonwealth Electronic Data*
- OPD-SEC019A *Data Categorization and Inventory Operating Template*
- ITP-SEC024 *IT Security Incident Reporting Policy*
- ITP-SEC025 *Proper Use and Disclosure of Personally Identifiable Information (PII)*
- ITP-SEC031 *Encryption Standards*
- Federal Internal Control Standards
- National Institute of Standards and Technology (NIST) Federal Information Processing Standard Publication (FIPS-PUB) 199 - *Standards for Security Categorization of Federal Information and Information Systems*
- National Institute of Standards and Technology (NIST) Federal Information Processing Standard Publication (FIPS-BUS) 200 - *Minimum Security*

Requirements for Federal Information and Information Systems

- National Strategy for Information Sharing and Safeguarding
- NIST guidance on Security and Privacy Controls for Information Systems and Organizations
- National/Homeland Security and Privacy/Confidentiality Checklist and Guidance

7. Authority

Executive Order 2016-06 *Enterprise Information Technology Governance*

8. 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 are to be directed to RA-ITCentral@pa.gov.

9. 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 is to 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	07/11/2016	Base Document	N/A
Revision	12/17/2018	Revisions throughout for clarity Added language to align National Archives and Records Administration (NARA) on records and metadata management	N/A
Revision	12/22/2020	Definition section updated Added FIPS 200 Removed reference to COPPAR	N/A
Revision	05/27/2022	• ITP refresh • Utilizing accessible ITP Template • Added third parties to the scope • Added additional guidance/best practices related to the categorization of records, data security, and the capture and migration of metadata. • Updated and added links to references	Revised IT Policy Redline <05/27/2022>