Information Technology Policy

Policy and Procedures for Identifying, Classifying, and Categorizing Commonwealth Electronic Data

Number
ITP-INF015

Effective Date
08/18/2022

Category
Information

Supersedes
None

Contact
RA-ITCentral@pa.gov

Scheduled Review
August 2023

1. Purpose

This Information Technology Policy (ITP) addresses the policies and procedures for the identification, classification, and categorization of Commonwealth electronic data.

2. Scope

This ITP applies to all offices, departments, boards, commissions, councils, or other entities that generate, access, store, or modify Commonwealth Data..

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

3. Background

Commonwealth employees and contractors shall identify the Classification of electronic records and protect information from improper disclosure based on the Classification of the records.

4. Definitions

Agency Data Steward: a functional role that:

- Facilitates the efficient sharing of agency/business area data assets.
- Coordinates the collection of data for optimized Commonwealth collaboration.
- Understands the data policies and privacy involved with data use by:
  - Acting as point of contact/expert for agency/program area data related decisions
  - Facilitates collaboration between other agencies and for Commonwealth enterprise data sharing initiatives

- Facilitates agency data governance and participates in enterprise level data governance meetings
- Assists with validating data quality
- Ensures data definitions and metadata are maintained
- Works with IT to design and organize data
- Consults with Agency Office of Chief Counsel to ensure appropriate data legal reviews

5. Classification

"C" CLASSIFICATION RECORDS or CLOSED RECORDS

The use of a "C" designation indicates that all or part of the record requires special treatment and/or heightened protections, including, but not limited to, as appropriate, 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.

Although a "C" designation usually equates to a "non-public record" designation under the Right-to-Know Law (65 P.S. Section 67.101, et seq.), the two designations are not the same. A record's treatment under the Right-to-Know Law must be determined in consultation with an agency's legal and Right-to-Know Law staff at the time of the Right-to-Know Law request.

Failure to classify records as "C" does not give rise to any presumption, implication, or indication that records are open or accessible to the public.

Only the originating agency may remove the "C" designation.

A "C" designation, and the more granular "class" within that designation, is a determination made by an agency head or designee. If another data designation or class is deemed necessary; justification shall be provided to OA for why a data element or group of data elements does not fit into the classes below.

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

A. Sensitive Security Information: This type of information may fall under another class, but it is placed in this one because of the significant consequences of potential disclosure, and the high degree of protection it requires. It is information maintained by an agency:

1. In connection with homeland security, national defense, military, law enforcement or other public safety activity the disclosure of which would be reasonably likely to jeopardize public safety or preparedness. Homeland Security information includes, but is not limited to, records designed to prevent, detect, respond to, and recover from acts of terrorism, major disasters and other emergencies, whether natural or manmade; emergency preparedness and response, including volunteer medical, police, emergency management and fire personnel; intelligence activities; critical infrastructure protection; border security; ground, aviation and maritime transportation security; bio-defense; detection of nuclear and radiological materials; and research on next-generation security technologies; or the disclosure of which creates a reasonable likelihood of endangering the life or safety of a natural person or threatening public safety or the physical security of a building, resource, infrastructure facility or

information storage system, including:

i. documents or data relating to computer hardware, source files, software and system networks that could jeopardize computer security by exposing a vulnerability in preventing, protecting against, mitigating or responding to a terrorist act;

ii. lists of critical infrastructure, key resources and significant special events, which are deemed critical due to their nature, and which result from risk analysis, threat assessments, consequences assessments; vulnerability assessments; anti-terrorism protective measures and plans; counter-terrorism measures and plans; security and response needs assessments; and

iii. building plans or infrastructure records that expose or create vulnerability through disclosure of the location, configuration, or security of critical systems, including public utility critical systems, such as information technology, communication, electrical, structural, fire suppression, ventilation, water, wastewater, sewage, and gas systems.

B. Protected Information: This is information that is subject to some degree of protection under any Pennsylvania or federal statute, law, order, or regulation. The degree of protection necessary will vary based on the law or order in question, and the potential consequences of disclosure. This information includes, but is not limited to:

1. Data elements as defined in the Breach of Personal Information Notification Act, Act of December 22, 2005, P.L. 474, No. 94, as amended, 73 P.S. §§ 2301-2329.

2. Information received from a federal or Commonwealth entity bound by specific regulations, including, but not limited to the following sources:

i. Social Security Administration (SSA).

ii. Internal Revenue Service (IRS).

iii. Centers for Medicare and Medicaid Services (CMS).

iv. Criminal Justice Agencies in accordance with the Criminal History Record Information Act (CHRIA).

v. Educational Institutions subject to the Family Education Rights and Privacy Act (FERPA).

vi. Entities subject to the Payment Card Industry (PCI) data security standards.

vii. Health care entities subject to the Health Insurance Portability and Accountability Act (HIPAA) or other data privacy or security law in the health care industry (including internal entities).

3. Third Party Data: Information associated with and specific to the Commonwealth's regulated entities, vendors, suppliers, business partners, contractors, and other third-party entities, including the trade secrets of third parties. The degree of protection necessary will vary based on the law or order in question, and the potential consequences of disclosure.

4. Geographic Data: Information associated with addresses, locational information, or elements from a Geographic Information System (GIS).

5. Contract Data: Information associated with contract, award, and bidding activities related to procurement of supplies or services, at appropriate stages of procurement.

C. Privileged Information: This is information that is protected by a recognized privilege or doctrine, such as attorney-client privilege, the attorney work product doctrine, executive privilege, or deliberative process privilege.

D. Prerequisite-Required Information: This includes data that is not exempt or precluded from public disclosure under any Pennsylvania law or order (including the Right-to-Know Law), but that require certain protections to ensure that the prerequisites to disclosure are met. The degree of protection necessary will vary based on the record in question, and the potential consequences of disclosure. For example, this includes records that may be disclosed only after a form is signed, etc.

6. Sensitivity Levels

The use of Sensitivity Levels provides further designation to indicate that all or part of the record requires special treatment and/or heightened protections, including, but not limited to, as appropriate, 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.

- Confidential - Data elements that are privileged under the Right-to-Know Act. Closed Record; Sensitive Secure.
- Restricted - Data elements that are not privileged under the Right-to-Know Act, but are highly sensitive and should not be released as they may cause harm to an individual. Closed Record; Protected.
- Internal - Data elements that are not privileged under the Right-to-Know Act, but release would not require notification or cause individuals drastic harm. Closed Record; Privileged or Closed Record; Prerequisite.
- Public - Data elements that are made readily available to the public through websites or other modes of publication.

7. Policy

7.1 Data Categorization and Classification

Agencies shall categorize and classify all data.

- Data Categorization shall follow the NIST SP 800-60 Rev 1 Guide for Mapping Types of Information and Information Systems to

Security Categories Volumes 1 and 2.
- Data classified as Public Records shall adhere to Management Directives 205.36 and 210.5.
- "C" designated data shall be placed in one of the following classes: Sensitive Security, Protected, Privileged, Prerequisite-Required.

Agencies shall apply appropriate protections for data as outlined in ITP-SEC019 *Policy and Procedures for Protecting Commonwealth Electronic Data.*

7.2 Data Inventory

Office of Administration, Office for Information Technology (OA/OIT) shall utilize catalog technology to automate inventory collection activities on behalf of agencies for inclusion in an enterprise-level view of data structures and elements managed by OA/OIT in conjunction with Agency Data Stewards. OA/OIT shall use operating procedures as defined in OPD-INF015B – *Data Catalog Connectivity for Data Categorization and Inventory* (Authorized Commonwealth Access Only), and OPD-INF015C – *Data Catalog Scanning for Data Categorization and Inventory* (Authorized Commonwealth Access Only).

The inventory shall be housed in a central repository, with data assets/sources mapped to adopted enterprise data standards. This asset/source mapping shall support gap analysis and identification of areas requiring new enterprise data standards. This repository will be for internal use, shared with Agency Data Steward(s) and shall provide an appropriate inventory to any Commonwealth data-holding contractor for all the servers and/or application solutions in the contractor environment or under contractor control.

In situations where OA/OIT has not completed inventory collection of an agency data asset/source, the agency shall produce a data inventory themselves for inclusion in the enterprise-level inventory of data structures and elements managed by OA/OIT. Refer to OPD-INF015A – *Data Categorization and Inventory Operating Template*. OA/OIT/Enterprise Information Security Office (EISO) will assess Commonwealth agencies usage of OPD-INF015A and/or the OA/OIT data catalog during the annual agency self-assessment (ITP-SEC023 – *Information Technology Security Assessment and Testing Policy*).

The inventory provides a list of Commonwealth applications and identifies data classes and sensitivity levels for the data present on each server (and desktops, if applicable) and/or in any application solution. An inventory allows the Commonwealth and/or the contractor to identify protection mechanisms for each server and/or application solution.

Completing the inventory will aid the Commonwealth and contractors in the following:

- Identifying servers and/or application solutions with data that have stringent regulatory requirements (such as commingling requirements of Federal Tax Information (FTI) or other regulatory requirements).
- Increasing the speed of incident response procedures for potential breach notifications in accordance with the law.
- Cost saving through selective, strict protection of the highest sensitivity levels of data and not applying strict protections on lesser sensitivity levels.
- Aiding in the identification of servers requiring special privileged user access.

Agencies using the OPD-SEC015A template shall document an inventory of all data assets/sources as well as identify the categories and classes of data and their respective sensitivity levels for each respective data asset/source, at least annually.

Agencies using the OA/OIT data catalog technology shall allow OA/OIT to securely connect the data catalog to data assets/sources to document data inventory of the data assets/sources as well as identify the categories and classes of data and their respective sensitivity levels for each respective data asset/source. Connection of the data catalog technology to an agency data asset/source will be non-persistent and only used during the time an inventory scan is actually executed by the data catalog technology.

Agencies and/or OA/OIT shall perform, at a minimum, an annual update of the data inventory using either the OPD-SEC015A template or the OA/OIT catalog technology. Agencies shall also perform updates of data inventory at the following security events including, but not limited to:

- Upon the commencement of the use/holding of the data.
- Upon the initiation of the agency migration into contractor facilities or into facilities under contractor control.
- New data elements introduced to the server or application solution.
- Repurposing of the server or application solution.
- Major upgrades to the IT system, application, or databases.
- Changes in regulations or policies regarding data elements present.
- Any significant change that affects or introduces "C" classified data.

8. Responsibilities

8.1 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:

- Process and classify "C" designated electronic records as outlined in the above policy.
- Allow OA/OIT to perform a data inventory via data catalog technology or perform a data element inventory that shall be provided for inclusion in the enterprise-level inventory of data structures and elements managed by OA/OIT.
- Identify and classify all closed or "C" records generated, collected, stored, used, and disclosed by the agency or third party on the agency's behalf.

8.4 Agency Data Stewards Shall:

- Manage data assets on behalf of others and in the best interests of an agency and/or business area.
- Represent the interests of all stakeholders and take an enterprise perspective to ensure enterprise data is of high quality and can be used effectively.
- Help agencies and/or business areas establish control over data assets, including methods, technologies, and processes for the correct management of data.

- Manage the security, privacy, integrity, usability, integration, compliance, and availability an agency's and/or business area's internal and external data flows.

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-SEC000 – *Information Security Policy*
- 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)*
  - 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
- OPD-INF015A – *Data Categorization and Inventory Operating Template*
- OPD-INF015B – *Data Catalog Connectivity for Data Categorization and Inventory* (Authorized Commonwealth Access Only)
- OPD-INF015C – *Data Catalog Scanning for Data Categorization and Inventory* (Authorized Commonwealth Access Only)

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	08/18/2022	Base Document	Revised IT Policy Redline <08/18/2022>