pennsylvania
OFFICE OF ADMINISTRATION
INFORMATION TECHNOLOGY

Information Technology Policy

Policy and Procedures for Protecting Commonwealth Electronic Data

ITP Number ITP-SEC019	**Effective Date** November 16, 2007
Category Security	**Supersedes** --
Contact RA-ITCentral@pa.gov	**Scheduled Review** May 2019

1. Purpose

Addresses the policies and procedures for the identification of, and safe transmittal, transport, storage, and overall protection of commonwealth electronic data.

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.

These guidelines apply to environments supporting Commonwealth applications and data. Contractor staffs are responsible to understand and comply with this policy.

The policy is developed using the following guidelines:

- National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 Rev4 (Security and Privacy Controls for Federal Information Systems and Organizations).
- NIST SP 800-60 Rev1 (Guide for Mapping Types of Information and Information Systems to Security Categories).

3. Background

There are many forms of electronic records within the commonwealth which require special treatment and/or heightened protections. These types of electronic records, known as "C" classification records are defined below. Commonwealth employees and contractors must identify these electronic records and protect this information from improper disclosure.

"C" CATEGORY of CLOSED RECORDS

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.

Though 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 "category" within that designation, is a determination made by an agency head or designee. If another data designation or category is deemed necessary, justification shall be provided to OA for why a data element or group of data elements does not fit into the categories below.

4. Categories

"C" designated data elements shall be placed in one of the following **categories**:

A. **Sensitive Security Information**. This is a type of information that may fall under another category, but which is placed in this one because of the significant consequences of potential disclosure, and the high degree of protection necessary. 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, waste water, sewage and gas systems.

B. **Protected Information:** This is information that is subject to some degree of protection under any Pennsylvania or federal statute, 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 P.L. 474, No. 94.

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 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 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 the data that are not exempt or precluded from public disclosure under any Pennsylvania law or order (including the Right to Know itself), 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.

5. Policy

a. Enterprise Data Classification

i. Under no circumstances are "C" designated electronic records (sensitive security, protected, privileged, or prerequisite-required information) as defined above, to be stored in a non-approved storage facility or on a non-approved storage device. Approved storage facilities include:

- Commonwealth centralized facilities
- Agency data centers or
- Other storage facilities approved in writing by the agency Information Security

Officer (ISO) or equivalent.

ii. No "C" designated electronic records can leave a commonwealth facility without prior electronic approval from the agency ISO or equivalent. Additionally, all requests for information relating to "C" designated electronic records are to be made in writing to the agency ISO.

iii. Encryption standards are outlined in the following ITPs and are to be followed for any actions that specify encrypting data under the "C" classification.

ITP-SEC020 - *Encryption Standards for Data at Rest*
ITP-SEC031 - *Encryption Standards for Data in Transit*

iv. Encryption protection mechanisms are detailed in Section 6, Data Classification Tables.

v. Systems that store, process, transmit or otherwise handle the following categories of data: Sensitive Security, Protected, Privileged are <u>recommended</u> to be protected with a Database Firewall (DBFW) to protect database-related systems.

- Agencies designing modernized and new database-related systems should include DBFW configurations to meet DBFW best practices and future requirements.

vi. Systems that store, process, transmit or otherwise handle the following categories of data: Sensitive Security, Protected, or Privileged <u>must</u> be protected with a Web Application Firewall (WAF) to protect internet-accessible web sites/services.

vii. Systems that store, process, transmit or otherwise handle Prerequisite-Required <u>may</u> be protected with a Web Application Firewall (WAF) and/or Database Firewall (DBFW).

Agencies are recommended to evaluate the impact of third-party WAF/DBFW agents on their computing resources prior to deployment of agents.

b. Data Inventory

- Each Commonwealth agency shall produce a data inventory for internal use and shall provide an appropriate inventory to any Commonwealth data-holding contractor for all the servers in the contractor environment or under contractor control. (Refer to OPD-SEC019A – *Data Categorization and Inventory Operating Template*). OA/OIT/Enterprise Information Security Office (EISO) will assess Commonwealth agencies usage of OPD-SEC019A during the annual agency self-assessment (ITP-SEC023 – *Information Technology Security Assessment and Testing Policy*).

- The data inventory provides a list of Commonwealth applications and identifies data categories and sensitivity levels for the data present on each server (and desktops if applicable). A data inventory allows the Commonwealth and/or the contractor to identify protection mechanisms for each server.

- The data inventory shall aid the Commonwealth and contractors in the following:

  a. Identifying servers with data that have stringent regulatory requirements (such as commingling requirements of Federal Tax Information (FTI).

b. Increasing the speed of incident response procedures for breach notifications.

c. Saving costs through selective, strict protection of the highest sensitivity levels of data and not having to focus protection resources on lesser sensitivity levels.

d. Aiding in the identification of servers requiring special privileged user access.

- Using the OPD-SEC019A template, individuals with an intimate knowledge of data used by Commonwealth applications (legacy and open systems) are to identify the categories of data and their respective sensitivity levels. The Commonwealth agencies shall perform an annual update of the data inventory, but also at the following security events including, but not limited to:

a. Upon the commencement of the use/holding of the data.

b. Upon the initiation of the Commonwealth agency migration into contractor facilities or into facilities under contractor control.

c. New data elements introduced to the server.

d. Repurposing of the server.

e. Major upgrades to the IT system, application, or databases.

f. Changes in regulations or policies regarding data elements present.

g. Any significant change that affects or introduces C classified data

6. Data Classification Tables

These data classification tables pertain to electronic records with a “C” classification and details the requirements for the various levels of protection determined by the various forms of data and transmission methods pertaining to:

1. Sensitive Security Information
2. Protected Information
3. Privileged Information
4. Prerequisite-Required Information

SENSITIVE SECURITY

Action	**Requirement**
Storage on Fixed Media	Encrypted
Storage on Exchangeable Media	Encrypted
Copying	Permission of Owner Required
Faxing	Encrypted Link plus Password Protected Recipient Mailbox or Attended Receipt
Sending by Public Network	Encrypted
* Disposal	Shredding or Secure Disposal Boxes
Release to Third Parties	Owner Approval and Non-Disclosure Agreement
Electronic Media Labeling Required	External and Internal Labels
Hardcopy Labeling Required	Each Page if Loose Sheets Front and Back Covers, and Title Page if Bound
Internal and External Mail	Address to Specific Person but Label only on Inside

Packaging	Envelope
Granting Access Rights	Owner Only
Tracking Process by Log	Recipients, Copies Made, Locations, Addresses, Those who Viewed, and Destruction
Web Application Firewall	Required (for Web Applications/Services)
Database Firewall	Recommended (for Database systems)

PROTECTED

Action	**Requirement**
Storage on Fixed Media	Encrypted or Physical Access Control
Storage on Exchangeable Media	Encrypted
Copying	Permission of Owner Advised
Faxing	Password Protected Recipient Mailbox or Attended Receipt
Sending by Public Network	Encrypted
* Disposal	Shredding or Secure Disposal Boxes
Release to Third Parties	Owner Approval and Non-Disclosure Agreement
Electronic Media Labeling Required	External and Internal Labels
Hardcopy Labeling Required	Each Page if Loose Sheets Front and Back Covers, and Title Page if Bound
Internal and External Mail Packaging	Address to Specific Person but Label only on Inside Envelope
Granting Access Rights	Owner Only
Tracking Process by Log	Not Required
Web Application Firewall	Required (for Web Applications/Services)
Database Firewall	Recommended (for Database systems)

PRIVILEGED

Action	**Requirement**
Storage on Fixed Media	Encrypted
Storage on Exchangeable Media	Encrypted
Copying	Permission of Owner Required
Faxing	Encrypted Link plus Password Protected Recipient Mailbox or Attended Receipt
Sending by Public Network	Encrypted
* Disposal	Shredding or Secure Disposal Boxes
Release to Third Parties	Owner Approval and Non-Disclosure Agreement
Electronic Media Labeling Required	External and Internal Labels
Hardcopy Labeling Required	Each Page if Loose Sheets Front and Back Covers, and Title Page if Bound
Internal and External Mail Packaging	Address to Specific Person but Label only on Inside Envelope
Granting Access Rights	Owner Only
Tracking Process by Log	Recipients, Copies Made, Locations, Addresses, Those who Viewed, and Destruction
Web Application Firewall	Required (for Web Applications/Services)
Database Firewall	Recommended (for Database systems)

PREREQUISITE-REQUIRED

Action	**Requirement**

Storage on Fixed Media	Encryption Optional
Storage on Exchangeable Media	Encrypted
Copying	No Restrictions
Faxing	No Restrictions
Sending by Public Network	Encrypted Optional
* Disposal	Ordinary Trash Can
Release to Third Parties	Non-Disclosure Agreement
Electronic Media Labeling Required	No Label Required
Hardcopy Labeling Required	No Label Required
Internal and External Mail Packaging	Only One Envelope with No Markings
Granting Access Rights	Local Manager
Tracking Process by Log	Not Advised
Web Application Firewall	Optional (for Web Applications/Services)
Database Firewall	Optional (for Database systems)

*Disposal – does not signify or negate policy and practices of records retention as described in INFRM001 – *The Life Cycle of Records: General Policy Statement*.

7. Responsibilities

Agencies are required to perform the actions outlined in this policy.

8. Related ITPs/Other References

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 *Commonwealth of Pennsylvania Information Technology Acceptable Use Policy*
- OPD-SEC019A – *Data Categorization and Inventory Operating Template*
- Breach of Personal Information Notification Act
- ITP-INFRM001 – *The Life Cycle of Records: General Policy Statement*
- ITP-SEC000 – *Information Security Policy*
- ITP-SEC015 - *Data Cleansing*
- ITP-SEC020 - *Encryption Standards for Data at Rest*
- ITP-SEC023 – *Information Technology Security Assessment and Testing Policy*
- ITP-SEC025 - *Proper Use and Disclosure of Personally Identifiable Information (PII)*
- ITP-SEC031 - *Encryption Standards for Data in Transit*
- NIST SP 800-53 Rev4 - *Security and Privacy Controls for Federal Information Systems and Organizations*
- NIST SP 800-60 Rev1 - *Guide for Mapping Types of Information and Information Systems to Security Categories*

9. Authority

Executive Order 2016-06, Enterprise Information Technology Governance

10. Exemption from This Policy

In the event an agency chooses to seek an exemption, for reasons such as the need to comply with requirements for a federally mandated system, a request for waiver may be submitted via the Commonwealth of PA Procurement and Architectural Review (COPPAR) process. Requests are to be entered into the COPPAR Tool located at http://coppar.oa.pa.gov/. Agency CIO approval is required.

11. Publication Version Control

It is the 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.

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

Version	Date	Purpose of Revision
Original	11/16/2007	Base Policy
Revision	04/02/2014	ITP Reformat; Merged GEN-SEC019A into ITP
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
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