Information Technology Policy
Enterprise Data Loss Prevention (DLP) Compliance Standards

Number	**Effective Date**
ITP-SEC032	April 29, 2011
Category	**Supersedes**
Security	None
Contact	**Scheduled Review**
RA-ITCentral@pa.gov	September 2024

1. Purpose

This Information Technology Policy (ITP) establishes the enterprise standards and administrative and technical controls that must be met to deploy Data Loss Prevention (DLP) technologies or solutions. DLP solutions protect sensitive data from data breach and are designed to detect and act upon unauthorized use and transmission of confidential information.

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 as outlined in the Responsibilities section of this ITP.

3. Policy

DLP technologies may exist in several forms including host-based (server or endpoint) or network-based solutions. DLP services help the organization comply with standards and regulations. It helps protect sensitive information and prevents unintended disclosure.

DLP technologies do not negate the need for users to utilize caution and adhere to all applicable policies (such as, but not limited to *ITP-SEC019, Policy and Procedures for Protecting Commonwealth Electronic Data*) and regulations to protect PII and sensitive data from accidental compromise and misuse.

3.1 Technical Requirements for DLP Solutions

Any DLP technology/solution must comply with the technical specifications and requirements outlined in the following Commonwealth ITP's:

- *ITP-SEC017, CoPA Policy for Credit Card Use for e-Government (if applicable)*
- *ITP-SEC019, Policy and Procedures for Protecting Commonwealth Electronic Data*
- *ITP-SEC025, Proper Use and Disclosure of Personally Identifiable Information*
- *ITP-SEC031, Encryption Standards*

NOTE: This ITP establishes the enterprise baseline minimum requirement for DLP. Agencies may set additional policy requirements to meet their specific compliance criteria due to additional laws, statues, or regulations such as CJIS Security Policy, IRS Pub 1075, PCI, HIPAA, etc.

3.2 Reporting Incidents of Data Compromise

The Agency ISO or designee shall conduct investigations into incidents involving potential or confirmed compromises of Commonwealth Data. Any confirmed or suspected compromises shall be reported in accordance with ITP-SEC024 *IT Security Incident Reporting Policy*.

4. Responsibilities

4.1 Agencies shall:
Comply with the requirements as outlined in this ITP.

4.2 OA/OIT shall:
Comply with the requirements as outlined in this ITP.

4.3 Third-party vendors, licensors, contractors, or suppliers shall:
Implement a DLP technology/solution if hosting or transmitting Commonwealth data.

5. 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

- *ITP-SEC017, CoPA Policy for Credit Card Use for e-Government*

- *ITP-SEC019, Policy and Procedures for Protecting Commonwealth Electronic Data*

- *ITP-SEC024, IT Security Incident Reporting Policy*

- *ITP-SEC025, Proper Use and Disclosure of Personally Identifiable Information*
- *ITP-SEC031, Encryption Standards*

6.   Authority

Executive Order 2016-06, Enterprise Information Technology Governance

7.   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.

8. 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	4/29/2011	Base Policy	N/A
Revision	4/2/2014	ITP Reformat	N/A
Revision	4/28/2021	Policy Refresh	N/A
Revision	06/21/22	ITP Refresh Third party responsibilities updated	N/A
Revision	09/26/23	Scope updated based on connection to Commonwealth Network and adjustment made to note third party requirements in Responsibilities section. Sections 3.1 & 3.2 added to separate policy language. Clarified when third parties must implement a DLP solution.	Revised IT Policy Redline <09/26/2023>