

Information Technology Policy

Enterprise Data Loss Prevention (DLP) Compliance Standards

ITP Number ITP-SEC032	Effective Date April 29, 2011
Category Security	Supersedes
Contact RA-ITCentral@pa.gov	Scheduled Review April 2022

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.

The Commonwealth and its agencies are custodians to a vast amount of sensitive citizen data, including, but not limited to, social security numbers, medical information, driving records, employee records, and financial information. This data is stored on numerous servers and storage devices and is transported throughout Commonwealth and business partner networks. Confidential data that is not protected or released to unauthorized parties is a fundamental Information Security failure.

2. Scope

This ITP applies to all offices, departments, 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 the Commonwealth's ITPs that are applicable to the products and services provided to the commonwealth.

3. Policy

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

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

- 1) ITP-SEC019 - *Policy and Procedures for Protecting Commonwealth Electronic Data*
- 2) ITP-SEC031 - *Encryption Standards*
- 3) ITP-SEC017 - *CoPA Policy or Credit Card Use for e-Government Applications*

(if applicable)

4. Responsibilities

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

4.2 Third-party vendors, licensors, contractors, or suppliers providing a DLP technology/solution on behalf of Commonwealth entities shall comply with the requirements as outlined in this ITP.

5. References

- ITP-SEC019 - *Policy and Procedures for Protecting Commonwealth Electronic Data*
- ITP-SEC031 - *Encryption Standards*
- ITP-SEC017 - *CoPA Policy or Credit Card Use for e-Government Applications*

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 are to 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 is to be submitted via the enterprise IT policy waiver process. Refer to ITP-BUS004 *IT Waiver Review Process* for guidance.

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

Version	Date	Purpose of Revision	Redline Link
Original	4/29/2011	Base Policy	
Revision	4/2/2014	ITP Reformat	
Revision	4/28/2021	Policy Refresh	Revised IT Policy Redline <04/28/2021>