

# **Information Technology Policy**

## ***Enterprise Data Loss Prevention (DLP) Compliance Standards***

<b>Number</b> ITP-SEC032	<b>Effective Date</b> April 29, 2011
<b>Category</b> Security	<b>Supersedes</b> None
<b>Contact</b> <a href="mailto:RA-ITCentral@pa.gov">RA-ITCentral@pa.gov</a>	<b>Scheduled Review</b> June 2023

### **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 (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. DLP services help the organization comply with standards and regulations. It helps protect sensitive information and prevents its 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.

Agency ISO and/or designee shall conduct investigations on incidents involving potential or confirmed compromises of Commonwealth Data. Any confirmed compromises shall be reported in accordance with ITP-SEC024 [IT Security Incident Reporting Policy](#).

Any DLP technology/solution must comply with the technical specifications and/or 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-SEC031 Encryption Standards](#)

## 4. Responsibilities

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

**4.2 Office of Administration, Office for Information Technology 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.

## 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-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](mailto: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 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	<a href="#">Revised IT Policy Redline &lt;06/21/2022&gt;</a>