# Information Technology Policy
## *Business Intelligence Reporting Policy*

**Number**
ITP-INF011

**Effective Date**
March 23, 2009

**Category**
Information

**Supersedes**
None

**Contact**
RA-ITCentral@pa.gov

**Scheduled Review**
December 2023

## 1. Purpose

This Information Technology Policy (ITP) establishes enterprise-wide standards and policies for Business Intelligence (BI) Reporting. Establishing standards will provide guidance to agencies as they plan for new application development projects or make investments in existing applications.

## 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 this ITP that are applicable to the products and services provided to the Commonwealth.

## 3. Background

BI reports deliver information that meet fundamental business requirements and are a common element of nearly all application implementations. BI reporting tools provide web-based viewing of reports, scheduling and automated distribution of reports, and security of both reports and the data within the reports. This ensures that consumers are able to view applicable reports.

*STD-INF011A, Reporting Product Standards* provides guidance to agencies on the current standards and the status of reporting solutions that are being used or being considered for use.

*GEN-INF011B, Reporting Product Availability* provides information on the availability and licensing of current reporting product standards.

## 4. Definitions

**Business Intelligence (BI) Report:** The process of utilizing BI software to collect, visualize, and analyze business or technical data for the purpose of finding relevant and actionable insights into operational or business trends.

**Information Silo:** An Information Silo is an information management system that is unable to freely communicate with other information management systems. Communication within an Information Silo is always vertical, making it difficult or impossible for the system to work with unrelated systems. Information Silos occur when different individuals or groups generate or record new data, but don't integrate or aggregate that information for other parts of the business to view or use in a strategic way. Additionally, it occurs from the tool sprawl and the poor or no integration of business applications and processes.

## 5. Policy

Agencies requiring reporting solutions shall standardize on the current architecture products identified in *STD-INF011A, Business Intelligence Reporting Product Standards*.

In the implementation of a reporting solution, application performance and operational database server utilization shall be analyzed for current and anticipated future levels to determine if the reporting solution requires a dedicated data store.

Agencies shall not intentionally create Information Silos. Agencies shall coordinate with the Commonwealth Data Officer to incorporate reporting data stores for enterprise-class applications into a broader BI framework. See *STD-INF010, Business Intelligence Policy*.

Agencies shall coordinate with the Office of Administration, Office for Information Technology (OA/OIT) to analyze security requirements for all reporting solution implementations.

Agencies shall coordinate with OA/OIT to ensure report users can only view reports they are entitled to view.

Agencies shall ensure only the data required for their business process is collected and retained per the agency record retention plan.

Agencies shall review and update their records retention plan with every implementation of BI Reporting in accordance with *Management Directive 210.5 Amended, The Commonwealth of Pennsylvania State Records Management Program*.

Agencies shall ensure the appropriate level of security controls are applied to all BI Reporting implementations.

Agencies shall coordinate with OA/OIT to ensure all users of BI reports are authenticated and authorized in accordance with all laws, statutes, executive orders, management directives, and policy.

Agencies may not implement a BI Reporting instance requiring authentication that does not leverage enterprise access management solutions.

## 6. Responsibilities

### 6.1 Agencies shall:

- Standardize on the current architecture products.
- Analyze application performance and database server utilization to determine if a dedicated data store is required.
- Ensure they are not creating Information Silos.
- Coordinate with the Commonwealth Data Officer to incorporate reporting data stores for enterprise-class applications.
- Coordinate with OA/OIT to ensure all report users can only view reports they are entitled.
- Review and update their records retention plan with every implementation of BI Reporting.
- Ensure the appropriate level of security controls are applied to all BI Reporting implementations and coordinate with OA/OIT to analyze security requirements.
- Coordinate with OA/OIT to ensure all users of BI reports are authenticated and authorized in accordance with all laws, statutes, executive orders, management directives, and policy.

### 6.2 Office of Administration, Office for Information Technology shall:

Coordinate with agencies implementing BI Reporting solutions to:

- Incorporate reporting data stores for enterprise-class applications into a broader BI framework.
- Analyze security requirements for all reporting solution implementations.
- Ensure report users can only view reports they are entitled to view
- Ensure all users of BI reports are authenticated and authorized in accordance with all laws, statutes, executive orders, management directives, and policy.

### 6.3 Third-party vendors, licensors, contractors, or suppliers shall:

Comply with the requirements of this ITP that are applicable to the products and services provided to the Commonwealth.

## 7. 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 210.5 Amended, The Commonwealth of Pennsylvania State Records Management Program*
- *ITP-ACC001, Information Technology Digital Accessibility Policy*
- *STD-INF010, Business Intelligence Policy*

- *STD-INF011A, Reporting Product Standards*
- *GEN-INF011B, Reporting Product Availability*
- *ITP-SEC007, Minimum Standards for IDs, Passwords, Sessions and Multi-Factor AuthenticationITP-SEC039 Keystone Login and Identity Proofing*
- *ITP-SEC040, IT Service Organization Management and Cloud Requirements*

## 8. Authority

*Executive Order 2016-06, Enterprise Information Technology Governance*

## 9. 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.

## 10. 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 | 03/23/2009 | Base Document | N/A |
| Revision | 11/18/2010 | ITP Refresh | N/A |
| Revision | 06/17/2021 | ITP Refresh<br>• Added to ITP template<br>• Added third-party vendors to Scope and Responsibilities Sections<br>• Added Definitions Section<br>• Updated Policy, Related ITPs and Exemption Sections | N/A |
| Revision | 12/02/2022 | • ITP Refresh<br>• Moved statement regarding the using current architecture products from Background to Policy Section<br>• Updated responsibilities<br>• Updated references | Revised IT Policy Redline <12/02/2022> |