pennsylvania
OFFICE OF ADMINISTRATION
INFORMATION TECHNOLOGY

Information Technology Policy

Information Technology Policy Governance

ITP Number ITP-BUS000	**Effective Date** April 29, 2016
Category Business	**Supersedes** None
Contact RA-ITCentral@pa.gov	**Scheduled Review** July 2022

1. Purpose

This Information Technology Policy (ITP) establishes the governance structure for all enterprise Information Technology Policies to ensure proper lifecycle controls and processes are in place and that the policies are managed in a transparent and inclusive manner.

2. Scope

This ITP applies to all departments, offices, 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.

3. Background

The management of Information Technology (IT) requires the development, control, and publication of a set of documents that convey purpose, direction, and required activities.

Executive Order 2016-06, *Enterprise Information Technology Governance*, gives the Office of Administration, Office for Information Technology (OA/OIT) general IT governance responsibilities over the planning, acquisition, and management of IT Resources; and responsibility for development and publication of related IT policy, standards, and guidelines governing IT investments by all agencies under the Governor's jurisdiction.

Management Directive 245.13 *Strategic Direction for Information Technology Investments*, identifies Information Technology Policies as the vehicle by which OA/OIT issues IT policies, standards, and guidelines.

4. Objective

To establish governance for the IT policy, including the development, control, and publication of the IT policy (lifecycle) as well as defining the roles and responsibilities for the governing bodies of the IT policy lifecycle.

5. Policy

The Office of Administration, Office for Information Technology Enterprise (OA/OIT Enterprise), is responsible for establishing and facilitating the following governance for IT Policies (ITPs).

1. IT Policy Governance Framework

- **a.** Agency IT Directors/Delivery Center CIOs
- **b.** Deputy Secretary of Information Technology (Commonwealth CIO)
- **c.** Domain Teams
- **d.** Enterprise Architecture Committee (EAC)
- **e.** Enterprise Technology Security Council (ETSC)
- **f.** OA Legal Office

g. Software Solutions Committee (SSC)

2. IT Policy Lifecycle Governance Model

a. Change Management
b. Release Management
c. Audit and Compliance Management
d. Records Management

Agencies may write their own policies that are more restrictive than the Enterprise IT policy but may not circumvent the controls or requirements described in the Enterprise IT policies.

5.1 IT Policy Governance Framework

The IT policy governance body framework establishes the formal structures, membership, decision rights, and roles and responsibilities that provide guidance, advice, information, and recommendations to the Commonwealth CIO. These bodies will be established and maintained by OA/OIT Enterprise for the purpose of conducting business relating to, but not limited to, IT Policies and other IT-related frameworks such as standards, guidelines, and best practices.

5.1.1. Domain Teams

The Domain Teams are comprised of the Domain Subject Matter Experts (Domain SMEs), the Domain Owner, the ETSC and the SSC.

- **Domain Team**

The Domain Team consists of the Domain Owner and Domain SMEs, which are assigned by the Domain Owners. Domain Owners are tasked to define roles, architecture, policy, and standards for enterprise IT services and solutions for agencies in their respective domains.

Domain	Domain Owner
Accessibility (ACC)	Accessibility Officer
Application (APP)	Enterprise Services
Business (BUS)	Technology Business Office Director
Information (INF)	Data Officer
Integration (INT)	Data Officer
Network (NET)	Enterprise CTO
Platform (PLT)	Enterprise CTO
Privacy (PRV)	EISO
Security (SEC)	EISO
Software (SFT)	Enterprise Services
System Management (SYS)	Enterprise CTO

The Domain Teams establish and maintain various IT components and services related to the elements of an enterprise architecture. The enterprise architecture models will be used in conjunction with defined business needs and priorities specified by the EAC to guide the domain teams' efforts.

- **Enterprise Technology Security Council (ETSC)**

The ETSC is comprised of designees from agencies and the Enterprise Information Security Officer (EISO) or designee. The ETSC is established by Management Directive 245.19 *Enterprise Technology Security Council* and is responsible for providing recommendations and evaluation of all IT policies within the SEC domain. In addition, the ETSC will provide security requirements, processes, procedures, and solutions to all IT policies as part of the enterprise security life cycle.

- **Software Solutions Committee (SSC)**

The SSC is comprised of Delivery Center CIOs or designees and the Bureau of Enterprise Solutions Director. The SSC is responsible for providing recommendations and evaluation of all IT policies within the APP and SFT domains to review the viability of software and application services that impact agencies.

5.1.2 Review Governance Bodies

The Review Governance Bodies are comprised of the EAC and the Agency IT Directors/Delivery Center CIOs.

- **Enterprise Architecture Committee (EAC)**

The EAC is comprised of the Chief Innovation Architect, Enterprise CTO, EISO, Enterprise Chief Architect, Chief Operating Officer, DC CTOs, DC ISOs, OA Legal Office, Office of Chief Counsel and Bureau of Enterprise Solutions Director. They are tasked to promote the advancement of enterprise architecture frameworks and methodologies; and evaluate and advise the Commonwealth CIO and relevant governing bodies on IT policy, enterprise-wide technologies, and capabilities to enhance investments, solution delivery, and cross boundary integration and interoperability.

  - OA Legal Office is a contributing member providing consultation and ensures compliance with all applicable laws and regulations.
  - Office of Chief Counsel is a contributing member providing consultation for INF, PRV and SEC policy Domains to ensure compliance with all applicable laws and regulations as it pertains to privacy.

The EAC provides a holistic technical perspective, including identification of future technical needs and opportunities, to help guide the development, evolution, and implementation of agency and Commonwealth-wide solutions. The EAC provides guidance on enterprise architecture frameworks that enable business and technology alignment to help the Commonwealth remain agile and efficient in the delivery of business solutions.

- **Agency IT Directors/Delivery Center CIOs**

The Agency IT Directors/Delivery Center CIOs are represented by the Commonwealth Agency IT Directors and Delivery Center Chief Information Officers or designees. The IT Directors/CIOs are responsible for reviewing all IT policy drafts, gathering internal feedback within their respective agencies, providing appropriate feedback, and providing the necessary communication within their respective agencies on all IT policy developments, including the publication of IT policies. IT Directors/CIOs are to be

proactive in ensuring their agency is complying with all ITPs and Management Directives (MD) and, if required, to utilize the enterprise IT Policy Waiver Process as described in ITP-BUS004 *IT Policy Waiver Review Process*. IT Directors/CIOs are to utilize ITPs to effectively mitigate IT risks to the Commonwealth and are encouraged to promote and advocate for robust and effective IT policies.

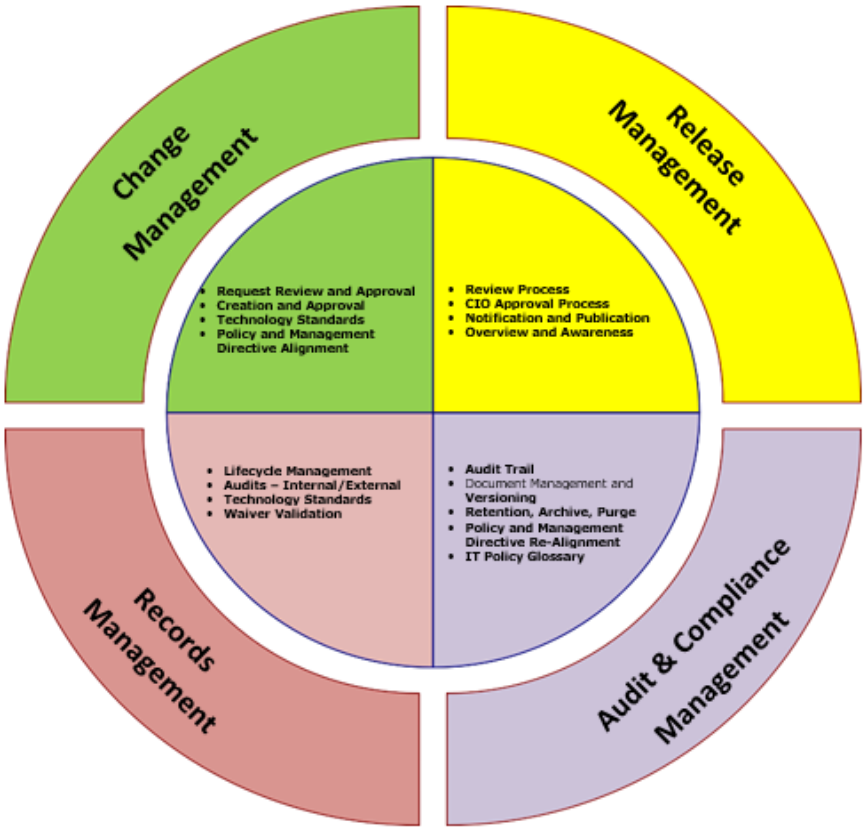
- **Deputy Secretary of Information Technology (Commonwealth CIO)**

The Commonwealth CIO is tasked with review and providing final approval or disapproval of the IT policy.

5.2 IT Policy Lifecycle Governance Model

The governance of IT policies is the role of OA/OIT Enterprise per Executive Order 2016-06 *Enterprise Information Technology Governance* and supplemented by Management Directive 245.13 *Strategic Direction for Information Technology Investments*. The governance model of IT policies includes the following management components:

- **Change Management**
  - Request Review and Approval Process
  - Policy Creation and Approval Process
  - Policy Technology Standards Process
  - Policy and Management Directive Alignment Process
- **Release Management**
  - EAC and Agency IT Directors/Delivery Center CIO Review Process
  - Commonwealth CIO Approval Process
  - Notification and Publication Process
  - Overview and Awareness Webinars Process
- **Audit and Compliance Management**
  - Lifecycle Management Process
  - Internal and External Audits Process
  - Waiver Validation Process
- **Records Management**
  - Audit Trail Process
  - Document management and version control
  - Retention, Archival, and Purge Process
  - Policy and Management Directive Realignment Process
  - IT Policy Glossary



5.2.1 Change Management

- **Request Review and Approval Process**

A service request through the Enterprise Service Request Platform is required to initiate all change requests for IT policies. This process allows for requesting the creation of a new IT policy, the revision of a currently published IT policy, or the rescission of a currently published IT policy. Refer to Section 6 for the Enterprise Service Request Platform information.

The initiation of a Change Management process through the service request process will be reviewed by the service owner, service provider, and designated coordinator of enterprise IT policies (IT Policy Coordinator). The IT Policy Coordinator will work with the requester, the Domain SMEs and Domain Owner to document the requirements for the request.

- **Policy Creation and Approval Process**

For requests for a new or revised IT policy, the IT Policy Coordinator will work with the Domain SMEs and Domain Owner to utilize the OPD-BUS000B *Information Technology Policy Framework* as needed prior to developing the draft IT policy. If OPD-BUS000B is not required, a draft IT policy based on the requirements identified in the service request is developed in coordination with the IT Policy Coordinator and Domain Owner.

For requests for rescission of IT policy, the IT Policy Coordinator will work with the Domain SMEs and Domain Owner to draft a justification summary based on OPD-BUS000B *Information Technology Policy Framework* submission using the following table

summary:

ITP	Description of ITP	Impetus for Rescinding	Agency Impact of Policy
ITP Name	*Summary of ITP*	*Impetus and justification for rescinding the ITP*	*All potential impacts on agencies if ITP is approved for rescission*

- **Policy Technology Standards Process**

IT policies can be utilized to standardize technologies to support the business and information technology program areas of the Commonwealth. These technology standards may be required to be utilized by agencies . The IT Policy containing a technology standard shall specify whether that product or technology is required to be utilized by stating so within the Technology Standards section of the IT Policy. The requirement language shall be stated at the beginning of the Technology Standards section with the following statement:

"The Current Technology Standard(s) listed in this Technology Standards table is required to be utilized by Governor's Jurisdiction agencies. If business needs cannot be met with the Current Technology Standard, an IT policy waiver is to be submitted. Deployment of a non-Current Technology Standard may not occur until approval of the IT policy waiver is obtained."

- Current standards are technologies that are approved to be deployed and utilized by agencies on IT Resources for all technology-based initiatives and projects.
- Contain standards are technologies that are approved to *remain* on existing IT Resources, however, any technology modernization initiative or project involving Contain standards on IT Resources must deploy the Current standard as part of the initiative or project, regardless of if that Technology Standard is required to be consumed. This requirement helps mitigate the risk of legacy and unsupported technologies on IT Resources. An IT policy waiver for the specific IT Policy detailing the Technology Standard is required if an initiative or project cannot deploy the Current standard.
- Retire standards are technologies that are being phased out. Plans shall be developed for their replacement, especially if there is risk involved such as lack of vendor support. A retirement date has been set.
- Emerging/Research standards are emerging technologies that have the potential to become current standards. At the present time, they shall only be used in a pilot or test environment where they can be evaluated. Use of these technologies shall be restricted to a limited production mode and requires approval of a waiver request.

Domain Owners, as part of their annual review of IT Policies, shall ensure any Current and Contain standards are in alignment with Commonwealth strategy and applicable industry best practices. If a Current standard is identified to be re-categorized as a Contain standard, the Domain Owner shall initiate an IT Policy revision with the IT Policy Coordinator. If a Contain standard is identified to be removed as a technology standard, the Domain Owner shall initiate an IT Policy revision with the IT Policy Coordinator and provide an "Expected Migration due date" that can be inserted into the IT Policy revision. The Expected Migration due date allows agencies to develop appropriate strategic and project planning to migrate off the Contain standard and replace with the Current standard. If an agency cannot meet the Expected Migration due date, a policy waiver for the specific IT policy containing the Technology Standard is required.

The above guidance should be vetted through appropriate governing bodies as necessary and determined by the Domain Owner to reduce unintended consequences and negative impact to business processes. Further, impact assessment will occur through the normal IT Policy Review Governance processes.

Agencies may submit a proposed new Current standard through the EARC Intake process, refer to Section 6 for intake link. It is recommended that the agency Chief Technology Officer be responsible for working with the EARC on presenting and gaining approval of the EARC members to accept the proposed technology standard. If approved, the chair of the EARC will initiate an IT policy revision with the IT Policy Coordinator to include the new technology standard.

- **Policy and Management Directive Alignment Process**

The IT Policy Coordinator is responsible for maintaining alignment of IT Policies and Management Directives, as necessary. This process should include the Office of Administration, Office of Continuity and Records Information Management (OA/OCRIM) and the appropriate stakeholders in conducting annual reviews of the IT Policies and Management Directives and initiate the appropriate Change Management processes if gaps are identified.

5.2.2 Release Management

- **Review Process**

The IT Policy Coordinator will introduce, through email or an enterprise collaboration tool, the draft IT policy or rescission justification summary to the IT Policy Governance Bodies for review and feedback. The review period will be designated as “Routine” (20-business day review), “Expedited” (10-business day review), or Emergency (at the Commonwealth CIO’s discretion to publish). The review period will be identified in the service request of the subject IT policy and this information will be relayed to the review governance bodies by the IT Policy Coordinator. Once consensus is received from all IT Policy Governance Bodies on the draft IT policy or rescission justification, the IT Policy Coordinator will send the final IT policy or rescission justification to the Commonwealth CIO for review and approval to publish.

Enterprise Architecture Committee (EAC) Responsibilities

The EAC is tasked with providing enterprise architecture perspectives during the review period of IT policies. This includes considerations on, but not limited to, IT technical feasibility, technical requirements, and other related technical issues that are required for the successful implementation of the IT policies. The EAC provides recommended language for policy clarification and adheres to the usage of IT standards (enterprise, national, international). The EAC is also responsible for notifying the appropriate stakeholders within their respective agencies that may be impacted by the policy and to gather and disseminate stakeholder concerns to the IT Policy Coordinator during the review period. If a response is not received by an EAC member within the designated review period, the IT Policy Coordinator will assume acceptance of the policy Change Management.

Agency IT Directors/Delivery Center CIO Responsibilities

The Agency IT Directors/Delivery Center CIOs are tasked with providing agency information technology perspectives during the review period of IT policies. This includes considerations on the impact the policies may have on both agency and enterprise-level IT resources. The IT Directors/CIOs provide recommended language for policy clarification and adheres to the usage of IT standards (enterprise, national, international). The IT Directors/CIOs are responsible for notifying all agency personnel within their respective agencies that may be impacted by the policy and to disseminate agency concerns to the IT Policy Coordinator during the review period. If a response is not received by an IT Director/CIO within the designated review period, the IT Policy Coordinator will assume acceptance of the policy Change Management.

Commonwealth CIO Approval Process

If the IT policy or rescission justification is disapproved for publication, the Commonwealth CIO will communicate the reasons for the disapproval to the IT Policy Coordinator. The IT Policy Coordinator will work with the appropriate IT policy stakeholders and governance bodies to remediate the reasons for disapproval and resubmit to the Commonwealth CIO for approval to publish.

If the IT policy or rescission justification is approved for publication, the Commonwealth CIO will communicate the approval to the IT Policy Coordinator. The IT Policy Coordinator will initiate the Notification and Publication Process.

- **Notification and Publication Process**

The IT Policy Coordinator will publish the revised IT policy to an enterprise collaboration tool(s). Notification will occur through email or an enterprise collaboration tool, the approval or rescission of the IT policy to all IT policy stakeholders. If applicable, the IT Policy Coordinator will archive the previous IT policy to a repository prior to publishing the approved IT policy, as detailed in the Records Management subsection of this policy. The IT policy or OPD-BUS000C *IT Policy Rescinded Notice* will be published using a standard format to one or more online repositories that is accessible to both Commonwealth and public IT policy stakeholders.

The IT Policy Coordinator will add IT policy and publication details to the ITP dashboard within five (5) days of IT policy publication. This detail will include updated IT policy, revisions made to the policy, impacted areas and actions required by the agency.

- **Overview and Awareness Webinars Process**

If applicable, the IT Policy Coordinator will work with the Domain Owner to develop an IT policy webinar using the OPD-BUS000D *IT Policy Webinar Presentation Template* for presentation. The webinar shall be held within sixty (60) business days of the IT policy publication date. The Commonwealth CIO or designee may request a webinar for any IT policy at any time. This process is typically only for new or significant revisions to IT policies. Rescinded policies are outside the scope of this process.

The IT Policy Coordinator or Domain Owner will work with the appropriate stakeholders to schedule a webinar date, and the mechanism for delivering the presentation, detailing the results of the presentation, and making all presentation materials available on a repository accessible to all Commonwealth employees.

5.2.3 Audit and Compliance Management

- **Life Cycle Management Process**

OA/OIT Enterprise is responsible for maintaining the entire life cycle of all published IT policies of which that lifecycle is detailed in this policy. All IT policies will be reviewed on an annual basis from the IT policy publication date by the Domain SMEs and the Domain Owner. Any deficiencies or gaps identified during this review process shall trigger the Change Management process. It is the responsibility of the IT Policy Coordinator and Domain Owner to coordinate the annual review of the IT policy. All annual reviews are to be documented in the IT policy's revision table including reviews that result in no revisions to the policy.

- **Internal and External Audits Process**

OA/OIT Enterprise or an authorized entity may at any time request an audit of IT policies from the IT Policy Coordinator. This audit is not limited to current IT policies and may include rescinded IT policies. The audit request should detail a business case and the reporting requirements for the audit. The audit's scope also covers IT policy waivers (requests, approvals, disapprovals) of IT policies and the IT Policy Coordinator will work with the IT policy waiver process coordinators to document the necessary reporting requirements.

- **Waiver Validation Process**

The IT Policy Domain Owner, in consultation with IT policy waiver process coordinators, is responsible for regularly reviewing all IT policy waiver requests for IT policies within the Domain Owner's domain. Should a disproportionate number of waiver requests be associated with an IT policy, the Domain Owner should initiate an internal audit to validate the appropriateness of the waivers (both requests and approved waivers). The Domain Owner should consult with the appropriate IT policy waiver stakeholders (coordinators, SME reviewers, business/technical reviewers, and executive reviewers) in determining the rationale behind the disproportionate number of waiver requests. The Domain Owner should then consult with the IT Policy Coordinator to determine if the IT policy requires an initiation of a Change Management process.

5.2.4 Records Management

- **Audit Trail Process**

The IT Policy Coordinator is responsible for maintaining an accurate and accessible audit trail for all IT policy processes. An intranet repository is to be maintained for the storage of the following IT policy deliverables:

- Completed Request Fulfillments.
- Completed OPD-BUS000B *Information Technology Policy Framework* documents.
- Final approved versions of revised IT policies.
- A "redline" version of the IT policy that details all changes of a policy revision:
  - The redline version shall be referenced in the revised IT policy's "Revision Table" for Commonwealth personnel access only.
  - The redline version is not to be made available publicly.
- All communications from review governance bodies pertaining to feedback of policy drafts, revisions, or rescission justifications.
- All decision communications from Commonwealth CIO or designee pertaining to policy requests, frameworks, drafts, revisions, or rescission justification.
- Final publication IT policies that have been designated to be rescinded.

- **Retention, Archival, and Purge Process**

The IT Policy Coordinator is responsible for adhering to Management Directive 210.5 *Commonwealth of Pennsylvania State Records Management Program* for all records management of IT policies and other policy-related records.

- **Policy and Management Directive Realignment Process**

The IT Policy Coordinator is responsible for maintaining alignment of IT Policies and Management Directives, as necessary. This process should OA/OCRIM and the appropriate stakeholders in conducting annual reviews of the IT Policies and Management Directives and initiate the appropriate Change Management processes if gaps are identified.

- **IT Policy Glossary**

The IT Policy Coordinator will maintain a publicly accessible policy glossary in which all enterprise IT policies will reference. The glossary will display terms and definitions as well as reference the source of those definitions. Sources that are not IT policies shall come from trustworthy federal or industry-standard entities (e.g. NIST, U.S.C). All IT polices will reference the glossary in the Related ITPs/Other References section. Refer to Section 6 of this policy for the link to the glossary.

6. 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 *Commonwealth of Pennsylvania State Records Management Program*
- Management Directive 245.13 Amended *Strategic Direction for Information Technology Investments*

- Management Directive 245.19 Amended *Enterprise Technology Security Council*
- Enterprise Service Request Platform: https://copaprod.service-now.com/oaportal (CWOPA access only)
- EARC Intake: https://servicegateway.pa.gov/vcac/org/edc/ (CWOPA access only)
- OPD-BUS000B *Information Technology Policy Framework*
- OPD-BUS000C *Information Technology Policy Rescinded Notice*
- OPD-BUS000D *Information Technology Policies Educational Webinars Presentation Template*
- OPD-BUS000E *Information Technology Policy Template*
- ITP-ACC001 *Information Technology Digital Accessibility Policy*
- ITP-BUS004 *IT Policy Waiver Review Process*

7. Authority

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

8. 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.

9. Exemption from This Policy

In the event an agency chooses to seek an exemption from this 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:

Version	Date	Purpose of Revision	Redline Link
Original	04/29/2016	Base Document	
Revision	10/26/2017	Minor format and grammar updates for clarity Added Services (SER), Software (SFT) ITP domains Added Policy Glossary language and linked relevant terms Updated the Request to Review process; rescinded OPD-BUS000A Added language that all ITPs must document annual review	
Revision	07/23/2021	• Updated IT Policy Governing Bodies and Lifecycle Governance Model • Domain Table added • Added Policy Technology Standards Process • Updated Related ITPs and Exemption Sections	Revised IT Policy Redline <07/23/2021>