pennsylvania
OFFICE OF ADMINISTRATION
INFORMATION TECHNOLOGY

Information Technology Policy

Information Technology Policy Governance

ITP Number	**Effective Date**
ITP-BUS000	April 29, 2016
Category	**Supersedes**
Business	None
Contact	**Scheduled Review**
RA-ITCentral@pa.gov	October 2018

1. Purpose

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 Information Technology Policy (ITP) applies to all departments, boards, commissions and councils under the Governor's jurisdiction. 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 *Amended, 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 Bodies
    a. Agency IT Directors/Delivery Center CIOs
    b. Enterprise Architecture Committee (EAC)
    c. Domain Teams
    d. Enterprise Technology Security Council (ETSC)

2. IT Policy Lifecycle Governance Model
    a. Change Management
    b. Release Management
    c. Audit and Compliance Management
    d. Records Management

5.1 IT Policy Governance Bodies

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 Deputy Secretary for Information Technology (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.

There are two governance bodies. The Review Governance Bodies are made up of the Agency IT Directors/Delivery Center CIOs and the Enterprise Archtiecture Committee (EAC). The Architectural Governance Bodies are made up of the Domain Teams and the Enterprise Technology Security Council (ETSC).

Review Governance Bodies

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 designee). The IT Directors/CIOs are responsible for reviewing all IT policy drafts, gathering internal feedback within their respective agency/delivery center on drafts, providing appropriate feedback to those drafts, and providing the neccessary 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 IT Policies and Management Directives and, if required, to utilize the Commonwealth of PA Procurement and Architectural Review (COPPAR) process as described in ITP-BUS004. IT Directors/CIOs are to utilize IT policies to effectively mitigate IT risks to the Commonwealth and are encouraged to promote and advocate for robust and effective IT policies.

Enterprise Architecture Committee (EAC)

The Enterprise Architecture Committee (EAC) is 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.

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.

Architecture Governance Bodies

Domain Teams

The Domain Teams are tasked to define roles, architecture, policy, and standards for enterprise IT solutions for commonwealth agencies, boards, and commissions under the Governor's jurisdiction.

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.

There are three defined Domain Teams that cover all the domains of IT policies (with exception of the Security Domain). These teams may have cross-over coverage of ITP domains due to the integration and alignment of certain IT policies.

- Software Domain Team: Application (APP), Software (SFT) and Information (INF)
- Data and Information Domain Team: Information (INF), and Integration (INT)
- Platform and Infrastructure Domain Team: Network (NET), Platform (PLT), Services (SER), and Systems Management (SYS)

These Domain Teams also share joint responsibility for the IT policy Business (BUS), IT Procurement (PRO), Project Management (EPM), and Privacy (PRI) domains.

Enterprise Technology Security Council (ETSC)

The Enterprise Technology Security Council (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 Security (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.

5.2 IT Policy Lifecycle Governance Model

The governance of IT policies is the role of OA/OIT Enterprise per Executive Order 2016-06 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 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
  - Retention, Archival, and Purge Process
  - Policy and Management Directive Realignment Process

6.2.1 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 7 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 to document the requirements for the request. The service owner will give approval and if necessary, gather the approvals from the IT Policy Business Owner, IT

Policy Domain Owner, and the Commonwealth CIO (or designee) to proceed with the Change Management process of the IT policy.

Policy Creation and Approval Process

For requests for a new or revised IT policy, the IT Policy Coordinator will work with the IT Policy Business Owner and IT Policy Domain Owner to utilize the OPD-BUS000B *IT Policy Framework Document* 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, IT Policy Business Owner, and IT Policy Domain Owner.

For requests for rescission of IT policy, the IT Policy Coordinator will work with the IT Policy Business Owner and IT Policy Domain Owner to draft a justification summary based on the OPD-SEC008A 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 and Management Directive Alignment Process

OA/OIT Enterprise is responsible for maintaining the alignment of IT Policies and Management Directives by conducting annual reviews of the IT Policies and Management Directives and initiate the appropriate Change Management processes if gaps are identified.

6.2.2 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 two 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 approved 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 both review 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 Responsibilities

The Enterprise Architecture Committee (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 and delivery center 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.

Office of Administration, Office of Chief Counsel Responsibilities

Legal representatives within the Office of Administration, Office of Chief Counsel will review all revisions and rescissions after the two governing bodies have reviewed and submitted feedback to ensure compliance with all applicable laws and regulations. Any recommendations from this office will be shared with the IT Policy Coordinator who will address those recommendations appropropriately including re-submission into the governance review process if warranted.

Commonwealth CIO (Deputy Secretary for Information Technology) 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 notify, through email or an enterprise collaboration tool, the approval of publishing the IT policy or rescission 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 develop a communication for distribution to commonwealth IT employees notifying the publication of the IT policy within 30 business days of the IT policy publication date.

Overview and Awareness Webinars Process

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

The IT Policy Coordinator or IT Policy 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.

Policy Glossary

OA/OIT Enterprise will maintain a publically 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 may 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 7 of this policy for the link to the glossary.

New, revised, or rescinded terms and definitions associated with ITPs will go through the established IT policy governance review processes prior to being published to the glossary. Proposed terms and definitions without an associated ITP may be published to the policy glossary. For unassociated ITP terms and defintions to be published, an ITP request must be submitted, using ITP-BUS000 as the associated ITP. Refer to Section 7 for the Enterprise Service Request Platform information.

6.2.3 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 IT Policy Business Owner and IT Policy Domain Owner. Any deficiencies or gaps identified during this review process should trigger the Change Management process. It is the responsibility of the IT Policy Business Owner and IT Policy 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 COPPAR waivers (requests, approvals, disapprovals) of IT policies and the IT Policy Coordinator will work with the COPPAR coordinators to document the necessary reporting requirements.

Waiver Validation Process

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

6.2.4 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 IT policy framework documents
- Final approved versions of revised IT policies with tracked revisions
- All communications from review governance bodies pertaining to feedback of policy drafts, revisions, or rescission justifications
- All decision communications from Commonwealth CIO or designeed 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 include the Office of Administration, Office of Continuity and Records Information Management (OA/OCRIM) and an internal documented process is to be established between the IT Policy

Coordinator and a representative of OCRIM that will provide a streamlined and efficient method for alignment.

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 *Commonwealth of Pennyslvania Information Technology Acceptable Use Policy*
- Management Directive 210.5 *Commonwealth of Pennsylvania State Records Management Program*
- Management Directive 245.13 *Strategic Direction for Information Technology Investments*
- Management Directive 245.19 *Enterprise Technology Security Council*
- Enterprise Service Request Platform: https://copaprod.service-now.com/oaportal (CWOPA access only)
- OPD-BUS000B *IT Policy Framework Document*
- OPD-BUS000C *IT Policy Rescinded Notice*
- OPD-BUS000D *IT Policy Webinar Presentation Template*
- OPD-BUS000E *IT Policy Template*
- ITP-BUS004 *IT Policy Waiver Review Process*

7. Authority

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

8. Publication Version Control

It is the 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, for reasons such as the need to comply with requirements for a federally mandated system, a request for waiver may be submitted via the Commonwealth of PA Procurement and Architectural Review (COPPAR) process. Requests are to be entered into the COPPAR Tool located at http://coppar.oa.pa.gov/. Agency CIO approval is required.

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

Version	Date	Purpose of Revision
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