IT Policy Governance

Effective Date:
April 07, 2025

Category:
Security

Scheduled Review:
April 2026

1. Authority

Executive Order 2016-06, Enterprise Information Technology Governance

2. Document Control

This policy replaces, in its entirety, IT Policy Governance Policy, dated February 24, 2025.

3. Purpose

This Information Technology Policy (ITP) establishes the governance structure and lifecycle for IT Policies. It also establishes the policy for exceptions to published ITPs.

4. Scope

This policy applies to all offices, departments, boards, commissions, and councils under the Governor's jurisdiction and any other entity connecting to the Commonwealth Network (hereinafter referred to as "agencies").

Third-party vendors, licensors, contractors, or suppliers shall meet the policy requirements of this policy as outlined herein.

5. Policy

For definitions of terms found within this document, refer to the *IT Policy Glossary*.

Executive Order 2016-06, Enterprise Information Technology Governance, gives the Office of Administration, Information Technology (OA/IT) general IT governance responsibilities over the planning, acquisition, and management of IT Resources; and responsibility for development and publication of related IT policy, standards, procedures, and guidelines.

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

Agencies may establish 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 Lifecycle

OA/IT is responsible for maintaining the entire life cycle of all published IT policies in accordance with this policy.

All IT policies and related documents shall be reviewed every year by the Subject Matter Experts (SMEs). The review shall occur within 12 months from the last IT policy publication date. It is the responsibility of the IT Policy Coordinator and SMEs to conduct the annual review of the IT policy. Reviews of individual policies may be performed more frequently if a need arises. All reviews are to be documented in the IT policy's revision table including reviews that result in no revisions to the policy.

5.2 IT Policy Governance Framework

5.2.1 Policy Review Committee

The Policy Review Committee (PRC) provides oversight and guidance regarding IT policy and standards in support of IT services within the Commonwealth. The Policy Review Committee establishes formal structures, membership, decision rights, roles, and responsibilities. This Committee is established and maintained by OA/IT for the purpose of conducting business related to IT policies.

5.2.2 Governance, Risk, and Compliance Team

The OA/IT Governance, Risk, and Compliance (GRC) Team is responsible for the governance of IT Policies and related documents. This includes the creation and revision of IT policies as well as ownership of the review and approval process.

5.2.3 Commonwealth Chief Information Security Officer (CISO)

The Commonwealth CISO will review and recommend approval or disapproval of all IT policies.

5.2.4 Commonwealth CIO

The Commonwealth CIO provides the final approval or disapproval of the IT policy.

5.3 IT Policy Exceptions

Adherence to ITPs is required in order to protect the Commonwealth's IT Resources and mitigate business and IT risks, however, there may be circumstances where an IT policy exception is needed for a specific period. In these instances, OA/IT has an IT Policy Exception process in place, which allows agencies to request an exception from the requirements of a specific ITP.

Agencies shall submit an IT Policy Exception request when they are not able to comply with

the requirements of an ITP or when deemed necessary by the Commonwealth CIO and/or other governing entities. Agencies requiring an IT Policy Exception shall review and adhere to the process detailed in *IT Policy Exception Procedure*.

6. Contact

Questions or comments may be directed via email to OA, IT Policy.

7. Exception from Policy

In the event an agency chooses to seek an exception from this policy, a request for a policy exception shall be submitted via the enterprise IT policy exception process. Refer to the above sections for guidance.

8. Revision History

This chart contains a history of this publication's revisions. Redline documents outline the revisions and are available to Commonwealth users only during the drafting process.

Version	Date	Purpose of Revision
Original	01/06/2025	Base Document
Revision	02/24/2025	Added document control section Misc. grammatical updates and clarifications Removed reference to the "scenarios table" in the Exception Procedure
Revision	04/07/2025	Replaced domain owners with SMEs Removed lifecycle management components Added section regarding policy review committee Removed references to *IT Policy Governance Procedure* (rescinded)