

Policy Title and #	<b>CIO-101: Information Technology (IT) Change Management</b>				
Effective Date:	<b>06/22/2016</b>	Revision Date:	<b>11/16/2020</b>	Review Date:	<b>12/10/2020</b>

**POLICY STATEMENT:**

This policy establishes controls related to Information Technology (IT) Change Management. The policy provides guidance in decision-making and practices that optimize resources, mitigate risk, and maximize return on investment.

**POLICY:**

With recognition that all agencies within the Commonwealth rely upon IT systems to perform critical business functions, agencies shall establish controls for the effective management of changes to IT systems. This includes, but is not limited to: IT hardware, operating systems, middleware, custom developed and commercial off-the-shelf (COTS) software applications, telecommunications equipment and call management systems, data center electrical and HVAC systems, and cloud or “as-a-service” solutions utilizing the Commonwealth’s shared IT infrastructure. A change is defined as the addition, modification, or removal of anything that could have a direct or indirect effect on IT services.

Key objectives of IT change management include:

- Ensuring business and IT stakeholders are aware of proposed changes and their risks prior to changes being made;
- Authorizing changes at a level appropriate for the degree of risk;
- Preventing service disruptions or re-work caused by poorly planned changes;
- Promoting repeated success by recording change results.

Each agency, including COT, shall establish change management processes that follow industry best practices and observe moderate controls for Configuration Management as outlined in NIST Special Publication 800-53 (Rev 4), to ensure all changes are properly recorded, tested, assessed, authorized, and scheduled prior to implementation. Agencies utilizing COT-supported infrastructure must use an IT Change Management process that aligns with COT’s process for the same.

The terms of this policy shall apply to production IT systems, and to non-production systems that are deemed mission-critical, as determined by the Business Owner.

**AUTHORITY:**

KRS 42.726 authorizes the Commonwealth Office of Technology (COT) to develop policies and compliance processes to support and promote the effective applications of information technology within the executive branch of state government.

**APPLICABILITY:**

All executive branch agencies, and non-executive branch agencies using COT-managed infrastructure or services, shall adhere to this policy. This includes employees, contractors, consultants, temporaries, volunteers, and other workers within state government.

**RESPONSIBILITY FOR COMPLIANCE:**

Each agency shall ensure that staff within their organizational authority are made aware of and comply with this policy. The agency is responsible for enforcing it. Unauthorized and/or neglectful actions regarding this policy may result in disciplinary action up to and including dismissal. COT may require additional service charges for remediation efforts due to non-compliance with this policy.

**MAINTENANCE:**

COT's Office of IT Architecture and Governance is responsible for maintaining this policy. Organizations may modify this policy to fulfill their responsibilities, but shall obtain approval through an exception request. Organization staff should refer to their internal policy, which may have additional information or clarification.

**REVIEW CYCLE:**

COT will review this policy at least every two years.

**REFERENCES:**

Helpful references can be found on the Enterprise IT Policies webpage.