Office of the Chief Information Officer Enterprise Policy

CIO-101: Enterprise IT Change Management Policy

Effective Date: 6/22/2016
Last Revised: 11/16/2020
Last Reviewed: 11/16/2020

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. Organizations may modify this policy to fulfill their responsibilities, but shall obtain approval through an exception request. Staff should refer to their internal policy, which may have additional information or clarification. 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 Contracts and Privacy is responsible for administrative coordination to maintain this policy, including review of this policy by the appropriate organizations at least every two years.

References

KRS 42.726

NIST Special Publication 800-53 Rev 4, *Security and Privacy Controls for Federal Information Systems and Organizations*