Office of the Chief Information Officer Enterprise Policy

CIO-119: Audit and Accountability Policy

Effective Date: 9/23/2019

Policy Statement

This policy establishes controls related to auditing and accountability. The policy provides guidance in decision-making and practices that optimize resources, mitigate risk, and maximize return on investment.

Policy

The Commonwealth Office of Technology (COT) and other enterprise agencies with IT systems in the Commonwealth's infrastructure shall adhere to established controls for auditing and accountability. The agencies shall adhere to, at a minimum, the moderate-level control standards outlined in the NIST 800-53 Revision 4 Audit and Accountability (AU) control family in accordance with CIO-091 Enterprise Information Security Program.

For details on COT-approved controls, refer to the Office of the Chief Information Security Officer's (CISO) ENT-201 Enterprise Security Controls and Best Practices.

Agencies may request exceptions to this policy by submitting a COT-F085 Security Exemption Request Form via e-mail to the Commonwealth Service Desk. The CISO will consider requests on a case-by-case basis. COT may pass any costs resulting from the exemptions or exceptions to this policy to those agencies.

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

- CIO-091 Information Security Program Policy
- Commonwealth Service Desk (502) 564-7576
- COT-085 Security Exemption Request Form
- ENT-201 Enterprise Security Controls and Best Practices
- KRS 42.726, *Roles, duties, and activities of COT*
- NIST Special Publication 800-53 Rev 4, *Security and Privacy Controls for Federal Information Systems and Organizations*