Office of the Chief Information Officer Enterprise Policy

CIO-121: Security Awareness and Training Policy

Effective Date: 10/31/2019

Policy Statement

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

Definitions

Awareness: Being informed of security policies and associated controls and guidelines.
Compliance: Adherence to the minimum guidelines outlined in this policy.
Training: Informing users of specific rules and guidelines to remain compliant with security policies.

Policy

The Commonwealth Office of Technology (COT) and other enterprise agencies with IT systems in the Commonwealth's infrastructure shall ensure proper security awareness and training. They shall adhere to, at a minimum, the moderate-level control standards outlined in the NIST Special Publication 800-53 Rev 4 Security Awareness and Training (AT) 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.

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 must adhere to this policy. This includes employees, contractors, consultants, temporaries, volunteers, and other workers within state government.

Responsibility for Compliance

Each agency must 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. Organizations may modify this policy to fulfill their responsibilities, but must obtain approval through an exception request. Staff should refer to their internal policy, which may have additional information or clarification.

Maintenance and Review

COT’s Office of IT Architecture & Governance and Office of the CISO share responsibility for maintaining this policy and shall review it at least every two years.

References

- CIO-091 Enterprise Information Security Program
- ENT-201 Enterprise Security Controls and Best Practices
- KRS 42.726
- NIST Special Publication 800-16, *Information Technology Security Training Requirements: a Role- and Performance-Based Model*
- NIST Special Publication 800-50, *Building an Information Technology Security Awareness and Training Program*
- NIST Special Publication 800-53 Rev 4, *Security and Privacy Controls for Federal Information Systems and Organizations*
- NIST Special Publication 800-100, *Information Security Handbook: A Guide for Managers*