Office of the Chief Information Officer Enterprise Policy

CIO-112: Security Planning Policy

Effective Date: 5/28/2019

Policy Statement

This policy establishes controls related to security planning. 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 enterprise agencies with IT systems in the Commonwealth's infrastructure shall develop and manage security plans for the IT systems under their control. These security plans may be single documents or a collection of various documents. COT and agencies shall adhere to the moderate-level access control standards outlined in the **NIST 800-53 Revision 4** Security Planning (PL) control family in accordance with CIO-091 Enterprise Information Security Program.

Agencies shall develop security plans, rules of behavior, and an information security architecture for Commonwealth systems in accordance with policies, procedures, and standards established by COT. For details on COT-approved access controls, refer to the Office of the Chief Information Security Officer's (CISO) Enterprise Security Controls and Security Best Practices.

Agencies may request exceptions to this policy by submitting a Security Exemption Request Form COT-F085 to the Commonwealth Service Desk via e-mail at CommonwealthServiceDesk@ky.gov. The CISO will consider requests on a case-by-case basis.

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. KRS 42.724 gives the Office of the CISO the responsibility to ensure the efficiency and effectiveness of IT security functions and responsibilities.

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
- CISO's Enterprise Security Controls and Security Best Practices
- Commonwealth Service Desk
- COT-F085 Security Exemption Request Form
- KRS 42.726
- NIST Special Publication 800-53 Rev 4 Control Families