CIO–112: Security Planning Policy		
EFFECTIVE DATE: 05/28/2019	**REVISED:** 09/01/2021 11/28/2023	**REVIEWED:** 09/01/2021 11/28/2023

I. PURPOSE

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.

II. 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 5, 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 request to the Commonwealth Service Desk via e-mail at CommonwealthServiceDesk@ky.gov. The CISO will consider requests on a case-by-case basis.

III. CORRECTIVE OR DISCIPLINARY ACTION

Each agency shall ensure that all relevant staff within their organizational authority are 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.

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

V.   REFERENCES

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