I. PURPOSE

This policy establishes controls related to Supply Chain Risk Management. 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 other enterprise agencies with IT systems in the Commonwealth's infrastructure adhere to established controls for supply chain risk management. The agencies shall adhere to, at a minimum, the moderate-level control standards outlined in the NIST Special Publication 800-53 Rev 5 Supply Chain Risk Management (SR) 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 (ENT-201) found at the bottom of the main COT Enterprise IT Policies webpage.

Agencies may request exceptions to this policy by submitting a security exemption request through ServiceNow. 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.

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.