I. PURPOSE

This policy establishes the need for processes related to Information Technology (IT) Change Management. The policy provides guidance in decision-making and practices that optimize resources, mitigate risk, and maximize return on investment.

II. DEFINITION

"Change" – means the addition, modification, or removal of anything that could directly or indirectly effect an IT service.

III. POLICY

With recognition that all agencies within the Commonwealth rely upon IT systems to perform critical business functions, agencies shall establish processes for the effective management of changes to IT systems. This includes, but is not limited to: IT hardware, operating systems, middleware, custom developed and commercial off-the-shelf (COTS) software applications, telecommunications equipment and call management systems, data center electrical and HVAC systems, and any cloud or "as-a-service" solutions utilizing the Commonwealth's shared IT infrastructure

Key objectives of IT change management include:

- Ensuring business and IT stakeholders are aware of proposed changes and their risks prior to changes being made;
- Authorizing changes at a level appropriate for the degree of risk;
- Preventing service disruptions or re-work caused by poorly planned changes;
- Promoting repeated success by recording change results.

Each agency, including COT, shall establish IT change management processes that follow industry best practices and observe moderate controls for Configuration Management as outlined in NIST Special Publication 800-53 (Rev 5), to ensure all changes are properly recorded, assessed, authorized, and scheduled prior to implementation. Agencies utilizing COT-supported infrastructure must use an IT Change Management process that aligns with COT's process for the same.

The terms of this policy shall apply to production IT systems, and to any non-production systems that are deemed mission-critical, as determined by the Business Owner.

IV. 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.

V. APPLICABILITY:

All executive branch agencies, and non-executive branch agencies using COT-managed infrastructure, data center facilities, 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, which may have additional information or clarification.

VI. REFERENCES:

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