Business Continuity Policy

Effective Date:
January 06, 2025

Category:
Systems Management

Scheduled Review:
June 30, 2025

Supersedes:
ITP-SYM003, ITP-SYM004

1. Authority

Executive Order 2016-06, Enterprise Information Technology Governance

2. Purpose

The purpose of this Information Technology Policy (ITP) is to establish a policy for the implementation of a Commonwealth Enterprise Continuity of Government Plan that ensures the storage of vital records in off-site facilities in the event of an emergency.

3. Scope

This policy applies to all offices, departments, boards, commissions, and councils under the Governor's jurisdiction and any other entity connecting to the Commonwealth Network (hereinafter referred to as "agencies").

Third-party vendors, licensors, contractors, or suppliers shall meet the policy requirements of this policy as outlined herein.

4. Policy

For definitions found within this document, refer to the *IT Policy Glossary*.

Commonwealth agencies are to develop and implement plans addressing basic alternative facility requirements for inclusion in their Continuity of Operations (COOP) plans. The facility requirements are based on essential functions identified in the agency continuity plan.

Agencies are to establish pertinent alternate sites following the guidelines contained in the *Business Continuity Standard,* ensuring that the mandatory key areas listed below are addressed:

- Recovery Time Objectives, RTO
- Specified Roles and Responsibilities
- Facility Definition Guidelines

RTOs and prioritization of critical applications must be consistent with

documentation in the agency continuity plan. Because the need to relocate may occur without warning, agencies should o make every effort to pre-position, maintain or provide for minimum essential equipment for continued operations of agency essential functions critical business functions at the alternate operating facilities for a minimum of (30) days.

Each agency-specific COOP plan is to contain provisions for conducting annual mission-critical restoration at an alternate processing site.

Agencies are to contact and involve the Office of OA Continuity of Government and, Department of General Services, Property Management in the following capacities:

- Determine the alternate processing sites that are available and provide the best fit for the agency.
- Undergo a review and schedule periodic reviews of agency alternate processing sites and associated plans and strategies at the discretion of the Office of Continuity of Government.

Agencies with systems serviced by the Commonwealth Pennsylvania Computer Services (PACS) are to comply with the PACS-specific alternate processing site guidance described in the *Business Continuity Standard.*

Agencies are required by *4 Pa. Code, Section 3.21 of the provisions of the Pennsylvania Emergency Management Service Act of 1978 Pamphlet Laws 1332*, to develop plans to ensure continuity of designated emergency/recovery management responsibilities and services. An important and essential part of any agency plan is the off-site storage of vital records identified as essential for an agency's continued operations in times of emergency.

The *Pennsylvania Emergency Management Agency State Emergency Operations Plan (PEMA SEO Plan), Emergency Support Function (ESF) Section No. 2*, directs Office of Administration (OA) to be the primary agency responsible for administrative oversight of all Commonwealth Telecommunications and Information Technology (IT) services. OA provides technical advice and assistance to other state agencies on immediate and long-term IT records recovery and records management.

The Office of Administration/Office for Information Technology (OA/OIT) is responsible for developing and disseminating policy and procedures governing Commonwealth agencies' off- site data center storage needs.

Each agency will arrange to store mission-critical resources at a remote storage site that is geographically separated from the Commonwealth Capitol complex in the event of a local disaster. The media are to be maintained in a secure, conditioned, and hazard-free environment located at least 50 miles from the Commonwealth Capitol. The media are to be accessible 24 hours a day, seven days a week, and be retrievable within four hours (for agencies within a 15-mile radius of the Commonwealth Capitol) as requested by authorized Commonwealth personnel.

Agencies are to provide for access control, intruder and environmental warning alarms, fire suppression, and water damage protection at any off-site location. *Management Directive 210.8, Micrographics Procedures to be used in Conjunction with Central Microfilm Management*, specifies additional guidelines concerning the storage of vital records to ensure that mission-critical IT-based resources necessary for continuous operation of an agency are backed up at a separate, remote site (facility). *MD 210.8* also specifies for continuity/recovery of applications and/or services in the event of an emergency. Use of such an off-site storage facility enables the agency to satisfy its responsibilities for the protection and safeguarding of IT-based resources under its jurisdiction and in the instance of an emergency.

The agency is ensured that mission-critical services and applications can be maintained or restored. The following is a list of suggested mission-critical resources which are to be designated for off-site storage. Please note that the list is not to be considered all-inclusive; each agency is to determine its own requirements based on its business functions and responsibilities.

4.1 Mission-Critical IT Resources Designated for Off-Site Storage

This applies to a protected environment approved by OA/OIT:

- Agency Continuity of Government Plan
- Vital Agency Records
- Inventory Records: Hardware, System/Application Software, Tape/Disk Libraries, Supplies, Schematics and Floor Plans
- Master Files
- Transaction Files
- Database and Data Files
- Operating System Software
- Application and 3rd-Party Software
- Software Library
- Source and Executive Programs
- Security Software
- Documentation Required to Process Mission-Critical Applications
- Systems, Programming, Operations, and Run-Book Documentation
- User and 3rd-Party Documentation
- Inventory of Other Materials, Supplies, Documentation Needed for Processing at an Alternate Site
- Journals, Software
- Special Forms/Critical Supplies

Off-site storage facilities are to, at a minimum:

- Maintain a normal office environment with temperature and humidity controls.
- Contain fire alarm protection.
- Contain safeguards in a controlled access area.
- Maintain a constant temperature of 62 to 68 degrees with a constant relative humidity of 35 percent to 45 percent for storage areas with computer magnetic tapes/cartridges containing permanent records.

These same environmental standards are recommended for the storage of all off-site

electronic records, regardless of the media.

5. Contact

Questions or comments may be directed via email to OA, IT Policy.

6. Exception from Policy

In the event an agency chooses to seek an exception from this policy, a request for a policy exception shall be submitted via the IT policy exception process. Refer to *IT Policy Governance Policy* for guidance.

7. Revision History

This chart contains a history of this publication's revisions. Redline documents outline the revisions and are available to Commonwealth users only during the drafting process.

Version	Date	Purpose of Revision
Original	01/06/2025	Base Document