Information Technology Policy
Commonwealth of Pennsylvania
Governor's Office of Administration / Office for Information Technology

ITP Number:	**ITP-SYM003**	
ITP Title:	**Off-Site Storage for Commonwealth Agencies**	
Issued by:	**Deputy Secretary for Information Technology**	
Date Issued: December 19, 2006		**Date Revised: December 20, 2010**
Domain:	**Systems Management**	
Discipline:	**Business Continuity**	
Technology Area:	**Off-Site Storage**	
Revision History Date:	**Description:**	
12/20/2010	**ITP Refresh**	

Abstract:
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.

General:
This ITP applies to all departments, boards, commissions and councils under the Governor's jurisdiction. Agencies not under the Governor's jurisdiction are encouraged to follow this policy to ensure that they develop and implement guidelines that facilitate enterprise-wide interoperability and standardization of off- site storage procedures.

Policy:
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 is to make arrangements 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.

Mission-Critical IT Resources Designated for Off-Site Storage (In 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.

Definitions of Terms:

Continuity of Government - An agency-specific plan which provides and documents a structured approach to ensure availability of resources, continuity of operations, and provisioning of services in times of emergency. The agency plan identifies mission-critical applications and services provided by the agency and minimal essential resources needed to provide for continuity and recovery of Commonwealth government operations in times of emergency.

Emergency - Any event that disrupts mission-critical applications and/or services beyond the point where an agency can restore such needs through routine recovery procedures.

Information Technology - Methods and techniques for creating, collecting, and producing information or for processing, transmitting, disseminating, storing, protecting, and disposing of electronic data, text, images, and voice through the use of contemporary electronic devices.

Mission-Critical Application - Any computer, desktop or network-based application which, if interrupted for a predetermined period of time, would cause hardship to a segment of the people of the Commonwealth, adversely affect public health and safety, seriously inhibit the primary function of an agency, or cause any legal liability on behalf of the Commonwealth, and is essential to restore or continue agency and/or state government operations in the event of a major or regional emergency.

Mission-Critical Resources - Computer or desktop hardware and network-based equipment and facilities, software, data, programs, documentation, vital records, essential applications and services including complex voice, data, video communications and other information essential to restore or continue agency and/or state government operations.

Off-Site Storage - The use of a separate facility at a remote site for storage of mission-critical resources (including a copy of the agency's continuity of government plan) is to facilitate business recovery of applications and/or services in the event of an emergency. Use of an off-site storage facility enables the agencies to satisfy their responsibilities for the protection and safeguarding of information technology-based resources under their jurisdiction in the event of an emergency and to be in compliance with the PEMA SEO Plan.

Commonwealth Emergency Operations Plan - A plan administered by PEMA to provide emergency operations policy, direction, and guidance to state agencies and to establish guidance for cooperative compacts with contiguous states during peace and wartime emergencies.

Vital Records - Records, regardless of archival value; which are essential to the functions of government during and after an emergency. Refer to Manual M210.8, Vital Records Disaster Planning.

Refresh Schedule:

All standards identified in this ITP are subject to periodic review and possible revision, or upon request by the Enterprise Architecture Standards Committee (EASC).

Exemption from This Policy:

In the event an agency chooses to seek an exemption, for reasons such as the need to comply with requirements for a federally mandated system, a request for waiver may be submitted via the Commonwealth of PA Procurement and Architectural Review (COPPAR) process. Requests are to be entered into the COPPAR Tool located at http://coppar.oa.pa.gov/. Agency CIO approval is required. Contact your agency CoP Planner for further details or assistance.

Questions:

Questions regarding this policy are to be directed to ra-itcentral@pa.gov.

References:

Manual 210.8 Vital Records Disaster Planning

Management Directive 210.8 Micrographics Procedures to be Used in Conjunction with Central Microfilm Management