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

Document Number:	**OPD-SYM004B**	
Document Title:	**Agencies Serviced by the Data PowerHouse Contract**	
Issued by:	**Deputy Secretary for Information Technology**	
Date Issued: June 21, 2007		**Date Revised: December 20, 2010**
Domain:	**Systems Management**	
Discipline:	**Business Continuity**	
Technology Area:	**Alternate Site**	
Referenced by:	**ITP-SYM004 Establishing Alternate Processing Site for Commonwealth Agencies.**	
Revision History Date:	**Description:**	
12/20/2010	**ITP Refresh**	

Introduction/Executive Summary:

In August 1999 the Unisys Corporation (vendor) and the Commonwealth of Pennsylvania (Commonwealth) entered into an agreement to outsource the operation and maintenance of mainframe and midrange computers for 18 Commonwealth agencies. Under the terms and conditions of this outsourcing contract as referenced in Contract Exhibit 1.02 (29), the outsourcing vendor works with Office of Administration/Office for Information Technology/Data PowerHouse (OA/OIT/DPH) Commonwealth project manager, and the respective agencies to provide the following services relevant to disruptive incidents and business continuity/recovery for the data center:

- Develop and maintain a comprehensive disaster recovery (DR) plan to document responsibilities, procedures, and tasks.
- Pickup and delivery of agency identified back up tapes to the off-site storage facility.
- Restore, for highly critical applications, the operating environment and required software at SunGard Recovery Services within three (3) days following a disruptive incident/disaster.
- Restore the operational environment and provide support at a pre-selected DR site biannually to enable testing of highly critical applications.

Recommend back up, off-site, and restoration procedures that will enable agencies to meet application currency requirements.

Main Document Content:

General Strategy

Advance Preparation

All agencies are to work with the vendor to ensure that adequate mainframe and midrange application backups are performed and the off-site rotation of these backups is sufficient to allow

Predefined supplemental document type codes are listed below:
APP = Appendix **BPD** = Best Practice Document **GEN** = General Information Document
OPD = Operations Document **RFD** = Existing Supporting Document Referenced by this ITP **WHP** = White Paper

restoration of the system if the DPH Data Center becomes inoperable and inaccessible for an indeterminate period of time.

For purposes of Continuity of Government/Continuity of Operations planning, applications supported by mainframe, midrange and open systems at the DPH Data Center fall into two categories: highly critical and non-highly critical. In order to maximize utilization of the DR Service Centers capacity, highly critical applications are to be restored first at the DR site (based on predetermined capacity requirements per agency). The remainder of the non-highly critical applications is to be restored at the agency's request, providing DR testing has been previously performed successfully.

The following criteria are used to determine highly critical applications:

- Supports public health and safety
- Provides subsistence to citizens or employees
- Results in a permanent business loss to the Commonwealth if the application is not available for an extended period of time

Agencies are required to develop and test a DR plan for highly critical applications as listed in Contract Exhibit 1.02 (29) of the outsourcing agreement. DPH will work with the agencies to ensure that agency backup, off-site, and restoration activities are in synchronization with the vendor’s plan.

DPH will assist the agencies in the preparation of their DR plans (DR plan, specific to DPH Data Center operations) and also will schedule disaster recovery tests for the agencies at the DR site. DPH will also assist the agencies through the following actions:

- Provides a sample format for completion of critical pieces of an agency’s DR plan (separate from agency-specific Continuity of Government/Continuity of Operations plan)
- Reviews agency DR plan and disaster recovery test results
- Works with the vendor and agency to resolve problems uncovered during disaster recovery testing
- Determines and refines capacity requirements at the DR site

Facility Restoration (DPH Data Center)

In the event of an emergency, disaster or disruptive incident affecting the DPH Data Center, the vendor is to work with the Commonwealth in providing the alternate site. (beyond using the DR site). The vendor is to be responsible for equipping the site with the necessary hardware and communication capability using commercially reasonable efforts to reinstitute Critical Services as promptly as possible.

During the term of the contract, the vendor (Unisys) would replace any data processing equipment lost in a disaster. For other expenses associated with restoration, although not part of the current contract, Unisys and IBM would be available to provide resources for the Facility Restoration effort, participating as requested by the Commonwealth. Agencies are to make provisions for additional costs that may be incurred.

The roles and responsibilities for restoration of this facility are defined in the enterprise DR plan for the DPH Data Center.