

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

Document Number:	OPD-SYM004A	
Document Title:	Guidelines for Establishing an Alternate Processing Site	
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 Policy for Establishing Alternate Processing Sites for Commonwealth Agencies	
Revision History Date:	Description:	
12/20/2010	ITP Refresh	

Guidelines for Establishing an Alternate Processing Site

Agencies are to create an alternate site as though the IT function of a facility were being relocated under normal conditions. The practices and procedures outlined in this document provide a framework for establishing a computer room, server farm, communications room or any other facility that houses IT equipment and devices.

In general, the overall approach for setting up an alternate site is the following:

- Acquire space to serve as the alternate site that is a safe distance from the inaccessible facility.
- Acquire equipment that is compatible with existing network and infrastructure configuration.
- Establish network connectivity from the alternate site to the business locations - providing the ability for email and sharing of files.
- Restore the site in the event of a catastrophe, emergency, or similar-type disruptive incident in accordance with the agency's Continuity of Government (CoG) and Continuity of Operations (COOP) plan.

Depending on the agency's recovery time objectives (RTOs) (described in Paragraph A., Recovery Time Objectives), the first three steps listed above often are completed to varying degrees BEFORE a situation occurs that necessitates an alternate site.

Mandatory key areas that are to be addressed in any alternate processing site strategy include:

- Recovery Time Objectives
- Specified Roles and Responsibilities
- Facility Definition Guidelines
- Alternate Site Options
- Alternate Site Preparation

A. Recovery Time Objectives

Agencies are to update and maintain the Mission-Critical Applications Survey (HCIS Survey) to ascertain the business or human safety impact caused by a failure of an agency IT processing resource. The specific alternate site strategy selected by the agency is directly related to these RTO ratings.

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

HCIS Survey guidelines for rating the business or human safety impact caused by a failure of a resource are:

- **H = Highly Critical (1-3 Days):** Highly critical applications are defined as essential for the agency to remain operational. Suspension of these applications beyond a period of one to three days could cause the agency to be in violation of laws, contracts, or regulations. Suspension of these applications may also cause disruption of critical services needed by the citizenry and other agencies. The result could damage the reputation and image of the agency or the Commonwealth.
- **C = Critical (4-14 Days):** Critical applications are defined as necessary to avoid a significant impact to the agency's ability to operate and maintain control. Suspension of these applications beyond a period of four to fourteen (4-14) days could cause a significant operational problem.
- **I = Important (15-30 Days):** Important applications are defined as necessary to support non-critical management decisions. Suspension of these applications beyond a period of fifteen to thirty (15-30) days is to have a minimal impact to an agency's operations.
- **S = Suspend (30 or more Days):** Suspended applications are defined as non-critical and, if suspended for thirty (30) or more days, would have little or no impact on the agency's ability to operate. Typically, these applications pertain to static information and historical data.

B. Specified Roles and Responsibilities

To successfully establish an alternate processing site and relocate to the site should the need arise requires the cooperation of multiple teams. Each team addresses a unique aspect of an alternate site. Agencies are to establish and appropriately staff the teams listed below. Each team is to designate a team leader and at least one alternate.

- **CoG coordinator** is responsible for the overall coordination of all aspects of the CoG/COOP plan implementation. The coordinator notifies the Declaration Team chairman about the alert, and upon confirmation, the coordinator is responsible for activating the necessary Recovery Activation Teams. After initial activation of the plan, the recovery coordinator becomes a member of the Declaration Team and is assisted by other members of that team with managing all activities necessary to establish the alternate working environment.
- **Alternate Site Leasing Team** is activated upon the need to relocate part or all of a facility after a disaster. This team is designed to work with Department of General Services (DGS) to procure adequate facilities to accommodate the department's IT equipment in times of emergency.
- **Declaration Team** is responsible for receiving input from the recovery coordinator(s) and the Recovery Management Team and is responsible for deciding whether to declare a disaster and for activating the recovery plan through the recovery coordinator.
- **Fire/Safety Team** is responsible for ensuring that an adequate fire/safety plan is available for all relocated employees and for conducting tests of the plan as soon as feasible after the disaster.
- **IT Coordinator** is responsible for oversight and coordination of all IT Teams including Network Support Team, Operations Support Team, and Server Recovery Team. The IT coordinator also works closely with the agency CoG/COOP coordinator.
- **Logistical Delivery Team** is activated upon the need to relocate and is responsible for transport and delivery of all supplies and fixed assets to the relocated facility.

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

- **Mail Resources Team** is responsible for ensuring all incoming and outgoing mail is delivered on a timely basis. If relocation is necessary, the team is responsible for diverting incoming mail from the inaccessible facility and confirming that outgoing mail is inserted, folded, collated and otherwise properly posted on a timely basis.
- **Network Support Team** is responsible for maintaining user connectivity to the primary processing facility and the backup site(s). This team works with service providers to evaluate any network outage or degradation of service that would prevent Commonwealth users from accessing business applications. In addition to these primary support requirements, this team performs the necessary actions to maintain and establish network access to the backups to facilitate Commonwealth users during activation of a Commonwealth Agency Disaster Recovery plan.
- **Operations Support Team** is comprised of staff responsible for the day-to-day activities of the data center. These members are the initial support for any incident that may require immediate attention. This includes current shift operations, customer engineers, level 2 "help desk," and on-call support personnel.
- **Physical Security Team** is responsible for securing the damaged area as soon as possible after a disaster and preventing inadvertent loss of salvageable records by those unfamiliar with salvage techniques. This team is also responsible for the physical security and safety of employees and assets at the damaged and relocation site(s).
- **Procurement Team** is activated upon the need to replace expendable and fixed assets after a disaster. This team is designated to work with DGS for the procurement of all supplies and assets necessary for the daily operations of the department, from computers to desks and office supplies.
- **Records Management Team** is responsible for providing all hard copy and microfilm/fiche records on demand for the entire department during the recovery phase of a disaster. This team prioritizes requests according to the department's Vital Records Retention Program.
- **Restoration Team** evaluates the primary facility damage and reports to the Recovery Management Team on the extent of the outage. This team assists local authorities, as needed, with securing the area from possible theft and also assists the Hardware & Resource Management Team. It establishes contacts and procedures to quickly restore facility function and data processing capability at the original data center in the event of a limited disaster.
- **Secretarial Services Support Team** is responsible to provide both clerical and typing support to the department during the recovery phase of the disaster. During the emergency, this team may also be tasked with citizen telephone requests.
- **Server Recovery Team** is to have a plan to replace all servers in place and implement it upon notification that a disaster has occurred. The disaster may or may not involve relocation.
- **Support Services Team** ensures that all system files, user files, and databases are backed up and relocated offsite on a scheduled basis. This team maintains current operating system software and library files for the alternate back up site host(s). It defines files/databases to be obtained from off-site storage to meet the minimum processing requirements (critical applications) at the alternate site. The first order of business at the alternate site is to recover the defined applications and return the back up tapes to off-site storage. This team assists the Operations Support Team in bringing up the systems at the alternate site and at the restored (or new) site.

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

- **Technical Support Team** prepares the servers and works with the Support Services Team to recover the defined applications. The team is to interface with the agencies and Media Services Teams to determine adjustment of schedules based on the recovery point established by the recovery teams.
- **Telecommunication Team** is activated as soon as it is determined that there is a need for facility relocation or repair at the affected facility. This team is responsible for quickly reestablishing all voice and data line requirements for the department.
- **Transportation Team** is responsible for providing vehicles necessary for a department's movement of personnel and equipment after a disaster. This team is responsible for arranging trucks, busses and cars needed by a department during the recovery phase of the disaster.
- **Emergency Response (ER) Teams** include, but are not necessarily limited to, the teams described in this list. It is imperative that these teams are established as part of the agency-specific CoG/COOP plan. Data relevant to these team members is to be reviewed and exercised/tested at least twice annually to assure currency.
- **Recovery Management Team** evaluates the emergency event/impact and determines the actions to be taken. The team responds to the needs of the various ER Teams and implements procedures to manage recovery activities. This team interfaces with upper and user management to apprise them of the status of the recovery operations. The Recovery Management Team chairperson, along with the Recovery Management Team, has the responsibility for expeditiously eliminating obstacles which may hinder the respective ER Teams in the attainment of assigned objectives. The Recovery Management Team chairperson is responsible for ensuring the swift acquisition of resources necessary for all contingency objectives.

C. Facility Definition Guidelines

This section establishes guidelines for resource considerations and items to be restored that are to be used to create the specifications for the alternate processing site. Please refer to the following site for additional guidance and details: [COOP Component Alternate Site](#).

Review existing facility

- Locate all IT rooms or areas within the facility
- Inventory equipment located in each area

Develop Specifications for the Alternate Processing Site to include:

- Identification of data/telecommunications requirements for each area (see note below)
- Identification of environmental requirements for each area
- Identify the power requirements for each area
- Identify storage requirements for each area
- Identify personnel requirements for each area
- Specification of space requirements:
 - Calculate space requirements for each individual IT area
 - Calculate space requirements for each office area
 - Calculate space required for personnel

Note: In order to ensure highly critical applications are running within one to three (1-3) days, the facility is to already have a telecommunications infrastructure in place. The DGS inventory is to indicate which buildings contain the fiber/telecom infrastructure. In an emergency situation, agencies are directed to work with appropriate Office of Administration/Office for Information Technology (OA/OIT) staff (with respect to logistics) as well as DGS (regarding procurement/leasing matters) to facilitate

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

arrangement of telecom services as quickly and smoothly as possible.

D. Alternate Site Options

All space options (real estate) typically are procured by DGS or through the established procurement process. Subscriber fees are paid for the availability, space, equipment, and services of facilities provided by independent suppliers. Primary options that generally are considered prior to initiating the process to acquire an alternate site include:

- **Hot Site:** computer-ready space held in reserve for an agency's use and generally provided by DGS (e.g., Willow Oak) or monthly subscriber fees paid for the availability, space, equipment, and services of fully operational facilities maintained by independent providers (e.g., SunGard).
- **Warm Site:** data center or office space partially equipped with hardware, communications interfaces, power sources, and environmental conditioning.
- **Cold Site:** physical space that is available for an agency's use with few amenities, generally provided by DGS. Such space may be an available Commonwealth facility or acquired as commercial space.
- **Mobile Recovery Center:** custom-designed, movable structures outfitted with computer and telecommunications equipment as well as environmental resources and amenities that are transported to and set up at the chosen location.

The types of sites required will vary based on the agency's RTO. For example, a *hot site* or *warm site* is to be justified for processes deemed "highly critical" or "critical." Alternatively, *cold sites* are to be justified for "critical" or "important" functions.

E. Alternate Site Preparation

As mentioned earlier, many activities to prepare a site are performed before an actual need arises. After the necessary facility definitions, RTOs, and responsible teams are in place, agencies are to perform as much advance alternate site preparation as necessary. This includes:

Specific Site Preparation – Includes site strategies for specific environments:

- Desktop Applications: Acquire a predetermined/preconfigured number of desktop and server computers for the alternate site.
- Distributed Applications: Lease IT equipment compatible with existing network configuration.

Advance Preparation: Incorporate CoG/COOP planning functions to include:

- Identification of budget sources that can be diverted to cover emergency-related expenses.
- Identification of resources in the agency's CoG/COOP plan that can be reallocated to establish an alternate site.
- Maintenance of the CoG/COOP plan as a scheduled application by keeping current vendor, service provider, and hardware/software inventory lists.
- Maintenance of the CoG/COOP plan and the Mission-Critical Applications Survey, *HCIS Survey*, for the development of new applications and the upgrading of existing applications.

Definitions of Terms

Alternate Processing Site – The recovery site designated to house the required equipment, resources, and staff expertise for uninterrupted operations when an agency's primary work site is inaccessible, or non-operational. In this IT Bulletin, recovery sites generally are classified as *Hot Site*, *Warm Site*, *Cold Site*, or Mobile Recovery Center.

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

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

Continuity of Government Plan (COG/COOP Plan) – An agency-specific plan that provides and documents a structured approach to ensure availability of resources, the continuation of operations, and the provisioning of services in times of emergency. The agency plan identifies mission-critical applications and services provided by the agency and the minimal essential resources needed to provide for continuity and recovery of state government operations in times of emergency.

Existing Facility – This is the agency's primary work site(s) that has been temporarily or permanently damaged. Such sites are to be recovered to ensure mission-critical IT-based applications and/or services can be restored and provided in accordance with specific RTOs defined previously to ensure continuity and recovery of Commonwealth operations in times of emergency.

HCIS Survey – Agency management is to use the current HCIS Survey that classifies applications in accordance with established RTO ratings to assist with assignment of appropriate criticality levels for applications designated as essential for continuing operations in event of an emergency or disaster (e.g., H-C-I-S: H=Highly-Critical, C=Critical, I=Important, and S=Suspend).

Health, Safety & Welfare Application (HSWA) – May be used by an executive authority to determine application selection and processing requirements based on potential direct impact on the health, safety, and welfare of the citizenry and other agencies in the event of a disaster.

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

Mission-Critical Applications (MCA) – Any computer or network-based application which, if interrupted for a predetermined period of time, would cause hardship to 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. Such an application is designated as essential to restore or continue agency and/or Commonwealth government operations in the event of a major or regional emergency. MCA criticality levels are specified in accordance with RTO classifications (HCIS Survey).

Mission-Critical Resources – Computer hardware and network equipment and facilities, software, data, programs, documentation, and information essential to restore or continue agency and/or Commonwealth government operations.

Off-Site Storage – Off-site storage is a separate facility at a remote site for storage of mission-critical resources (including a copy of an agency's continuity of government plan) in order to facilitate business recovery of applications and/or services in the event of an emergency. Use of an off-site storage facility enables agencies to satisfy their responsibilities for protecting and safeguarding IT-based resources under their jurisdiction in the event of an emergency, and to be in compliance with the Commonwealth Emergency Operations plan and ITP SYM003, *Off-Site Storage for Commonwealth Agencies*.

Commonwealth Emergency Operations Plan – A plan administered by Pennsylvania Emergency Management Agency to provide emergency operations policy, direction, and guidance to state agencies and to establish cooperation with contiguous states during peace and wartime emergencies.

Server Farm – Any area or facility that is environmentally suited to house servers and/or routers in support of an agency's IT network.

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