MANAGEMENT DIRECTIVE

245.11
Number

COMMONWEALTH OF PENNSYLVANIA
GOVERNOR'S OFFICE

Subject:

Development of Information Technology – Enterprise Continuity/Recovery Plans

By Direction Of:	Date:
Thomas G. Paese, Secretary of Administration	May 20, 1996

The Office of Administration/Information Technology (OA/IT) and all agencies under the Governor's jurisdiction are required to participate in the OA/IT-Enterprise Continuity/Recovery Planning Initiative, including developing and maintaining Information Technology – Enterprise Continuity/Recovery Plans by using an automated methodology.

1. PURPOSE. To establish policy and procedures for developing and maintaining OA/IT-Enterprise Continuity/Recovery Plans so that mission-critical services and applications can be maintained or restored in the event of an emergency.

2. SCOPE. To be implemented by OA/IT and all agencies under the Governor's jurisdiction. All other state entities employing Information Technology services and applications are encouraged to follow these procedures.

3. OBJECTIVES.

a. Define responsibilities for the protection and safeguarding of Information Technology based resources.

b. Establish a foundation and executive management framework for participation in the OA/IT-Enterprise Continuity/Recovery Planning Initiative, including developing and maintaining Commonwealth level and agency specific Emergency Continuity/Recovery Plans (hereinafter referred to as OA/IT-EC/RPlans).

c. Incorporate OA/IT-EC/RPlans as input to the Pennsylvania Emergency Management Agency (PEMA) "Commonwealth of Pennsylvania Emergency Operations Plan" (hereinafter referred to as the PEMA Emergency Operations Plan).

d. Provide positive identification for authorized emergency response personnel responding to an emergency at their own agencies and/or within the Commonwealth with a personal RED Emergency Response Card (RED Card) that is issued to ensure access to an agency facility; and/or alternate staging/recovery site, if necessary and to facilitate travel to the designated site in the instance of an emergency.

e. Ensure that mission critical IT based resources necessary for continuous operation of an agency are backed-up at an alternate site.

f. Provide preplanned responsive action to minimize the effects of a disruption to mission critical services and applications and to prevent an unplanned or unscheduled shutdown of state data centers.

g. Develop methods and procedures for OA/IT-EC/RPlanning.

h. Formulate standards directed towards improving timely recovery of IT based resources.

4. POLICY.

a. Agencies are required by *4 Pa. Code, Section 3.21* of the provision of the *Pennsylvania Emergency Management Service Act of 1978 P.L. 1332,* to develop plans to ensure continuity of assigned emergency/recovery management responsibilities and services.

b. Agencies are required to develop OA/IT-EC/RPlans according to the guidelines in this directive. Accordingly, the plans developed shall be in accordance with and in support of agency requirements for Information Technology in the PEMA Emergency Operations Plan.

5. DEFINITIONS.

a. Agency. Department, board, commission, or council under the Governor's jurisdiction.

b. Agency Emergency Continuity/Recovery Plan. An agency specific plan that provides and documents a structured approach to ensure availability of resources 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 State Government operations in times of emergency.

c. Automated Methodology. Software licensed to the Commonwealth through OA/IT that provides an uniform approach to the development of OA/IT-EC/RPlans (see Enclosure 1).

d. Certification. A document issued by OA/IT certifying that an agency has satisfied the requirements of this directive.

e. Emergency. 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.

(1) Emergency includes:

(a) ecological events (storms, earthquakes, floods, etc.); and,

(b) accidents (fire, power loss, voice data or video network communications loss, employe error, etc.).

(2) Emergency does not include:

(a) short duration interruptions or failures of hardware, software, network based facilities, or utilities that can be overcome through routine recovery procedures before the loss of services become critical; and

(b) planned cessation of the use of all or part of an application system.

f. Emergency Response Card (RED Card). An access card issued by an agency Security Administrator in concert with the Central Management Information Center (CMIC) to provide positive identification for authorized personnel responding to an emergency at their own agencies and/or within the Commonwealth. A personal RED Card is issued to authorized management and staff to ensure access to an agency facility and/or alternate staging/recovery site (should that be necessary) and to facilitate travel to the designated site during an emergency (see Enclosure 2).

g. Enterprise Continuity/Recovery Plan. Commonwealth-level plan developed by OA/IT provides and documents a structured approach to ensure availability of resources in times of emergency. The Commonwealth Plan identifies mission critical applications and services and the minimal essential resources needed to provide for the continuity and recovery of State Government operations in times of emergency.

h. Information Technology (IT). All 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. For purposes of Commonwealth business, the term Information Technology includes but is not limited to:

(1) Electronic Data Processing (EDP).

(a) digital, analog, and hybrid computers and associated peripheral and accessorial equipment;

(b) data, voice, and video transmission and network-based communications equipment;

(c) office automation, electronic printing and dissemination, and desktop publishing equipment and technology;

(d) software, generally referring to all of the computer programs, languages, systems/ operations, and applications used to make a computer perform a useful function for both users and practitioners; and

(e) IT based functions such as feasibility and application studies, system analysis and design projects, computer programming, data acquisition and reduction, computer-time rental, and maintenance services.

(2) Network/Telecommunications Resources. Services, technology, and equipment for and the transmission, emission, reception or relay of signs, signals, text, images, and sound or intelligence of any nature by wire, radio, optical, or other electromagnetic means.

i. IT Disaster. Declared by Lt. Governor or designee based on recommendation and consultation with Cabinet Officer or designee of agency(s) involved and OA/IT, e.g., PEMA, Transportation, and State Police during flooding conditions.

j. IT Emergency. Declared by Cabinet Officer, agency head or designee based on recommendation and consultation with agency(s) involved and OA/IT, e.g., PEMA, Transportation, and Health at the time of the fire at the Transportation and Safety Building.

k. Mission Critical Application. Any computer 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.

l. Mission Critical Resources. Hardware and network equipment and facilities, software, data, programs, documentation, and information essential to restore or continue agency and/or state government operations.

m. Off-Site Storage. Use of a separate facility at a remote site for storage of mission critical resources to facilitate continuity/recovery of applications and/or services in the event of an emergency, including a copy of the OA/IT-EC/RPlans. Use of such an off-site storage facility enables the agencies' to satisfy their responsibilities for the protection and safeguarding of IT based resources under their jurisdiction in the instance of an emergency and to be in compliance with the PEMA Emergency Operations Plan (see Enclosure 3).

n. Pennsylvania Emergency Management Agency, Commonwealth of Pennsylvania Emergency Operations Plan (PEMA/EOP). Administrered 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.

o. PEMA Declared Disaster. Declared by the Governor or designee based on recommendation by and consultation with PEMA; generally concerned with ecological events (storms, earthquakes, floods, etc.) that involve a geographical region, e.g., central Pennsylvania during the TMI crisis in 1974.

6. RESPONSIBILITIES.

a. OA/IT shall direct and oversee:

(1) Overall coordination and planning of the Commonwealth OA/IT-EC/RPlanning Initiative.

(2) Development and maintenance of the OA/IT-EC/RPlans and their components, including off-site storage and authorized staff RED Cards.

(3) Assistance to agencies who have IT facilities in locating an alternate or backup site to be used in the event of an emergency.

(4) Review, evaluation, and acceptance of agency specific continuity/recovery plans and changes thereto.

(5) Review and evaluation of agency specific continuity/recovery capability.

(6) Preparation and development of standards and guidelines on all phases of continuity/ recovery planning.

(7) Review by the Office of the Budget/ Bureau of Audits and Information Technology Committee/Subcommittee on Security and Control.

(8) Certification of agencies that have fulfilled the requirements of this directive.

b. Agencies shall:

(1) Assign one full-time equivalent (FTE) staff member to have overall responsibility for coordinating the development, review, and maintenance of the agency plan in accordance with this directive and the automated methodology.

(2) Assign an individual as Security Administrator to administer the Agency IT Security Policy.

(3) Include the Agency OA/IT-EC/ RPlanning Initiative in the "Governor's FY Budget"; also to be referenced in the "Multiyear Plan" in accordance with guidelines contained in *Manual M245.1, Guidelines for Preparation of Automated Technology Multiyear Planning Documents.*

(4) Provide OA/IT with a complete copy of the OA/IT-EC/RPlan on or before November 1st of each year. Thereafter, forward significant updates to the plan throughout the year as they develop.

(5) Ensure that the OA/IT-EC/RPlan is incorporated into the PEMA Emergency Operations Plan.

(6) Conduct periodic training, at least annually, of all personnel involved in or affected by implementation of the agency specific continuity/ recovery plan.

(7) Test the implementation capability of the agency specific OA/IT-EC/RPlan annually, after a significant change or more frequently, as required under simulated emergency conditions.

(8) Ensure that staff members responsible for mission critical applications and/or services are provided with a personal RED Card to provide positive identification when responding to an emergency at their own agencies and/or within the Commonwealth.

(9) Meet all minimum requirements outlined in Enclosure 3.

(10) Prepare an alternate or contingency-site plan in conjunction with OA/IT to ensure continuity of mission critical applications and/or services.

(11) Ensure that agency policy for the security of personal computers is developed in accordance with guidelines contained in *Manual M245.3, Guidelines for Personal Computers.*

(12) Backup and provide for off-site storage of mission critical resources in accordance with guidelines contained in *Manual M210.8, Vital Records Disaster Planning.*

c. OB/Comptroller Operations, Bureau of Audits, shall:

(1) Work with OA/IT and ITC/Subcommittee in developing standards and guidelines to ensure effective Enterprise Continuity/Recovery Planning.

(2) Assess OA/IT-EC/RPlanning as part of Comptroller Operations Annual Audit planning process.

7. PROCEDURES.

a. Agencies are required to prepare an OA/IT-EC/RPlan each year using the Automated Methodology software identified by OA/IT. The plan is to be forwarded to OA/IT on or before November 1st of each year.

b. Agencies having only PC or LAN based resources are to use "Chapter 8, User Plan" of the Automated Methodology for development of their plan.

c. Agencies are required to forward their plans to OA/IT on 3-1/2" or 5-1/4" diskettes, single or double density.

d. Agencies will be certified for OA/IT–EC/RPlanning by OA/IT when the agency:

(1) Submits an OA/IT-EC/RPlan that meets all of the requirements of this directive.

(2) Implements a regularly scheduled OA/IT-EC/RPlan Training Program.

(3) Performs regularly scheduled OA/IT-EC/RPlan test exercises according to guidelines established by the agency in compliance with the PEMA Emergency Operations Plan and approved by OA/IT.

(4) Meets the minimum requirements outlined in Enclosure 3.

(5) Establishes an alternate or backup site plan for processing mission critical applications in the event of an emergency.

(6) Has an Agency IT Security Policy in place and on file with OA/IT in accordance with guidelines established by OA/IT.

8. RESCISSION. *Management Directive 245.8, Development of Automated Technology Contingency/Disaster Recovery Plans.*

Enclosures:

1 – Automated Technology Methodology
2 – Emergency Response Cards Functional Profile
3 – Off-Site Storage

AUTOMATED TECHNOLOGY METHODOLOGY FUNCTIONAL PROFILE

To provide a structured and uniform approach to the development of an OA/IT-Enterprise Continuity/Recovery Plan (OA/IT-EC/RPlan) to ensure availability of IT based resources in times of emergency. The OA/IT-EC/RPlan identifies mission critical IT based applications and services and the minimal essential resources needed to provide for the continuity and recovery of those applications and services. Accordingly, the plans developed as a requirement of this directive will meet the agency requirements for Information Technology in the PEMA Emergency Operations Plan.

Menu-driven software using an IBM-PC, LAN based, or compatible equipment that is licensed to the Commonwealth through OA/IT is required.

Software Characteristics are to provide:

(1) Uniform guidelines and a structured approach to develop recovery plans and strategies to ensure availability of resources and to ensure continuity of assigned emergency management responsibilities and services in times of emergency.

(2) Templates to create a set of procedures and identify mission critical applications and services and minimal essential resources.

(3) Notification lists to ensure that all state level and agency emergency response personnel, user/client staff, vendor personnel, and other emergency response contacts are able to be reached in a timely fashion to initiate necessary response and recovery activities.

(4) On-screen tutorials and detail HELP messages to assist in developing and maintaining agency-specific OA/IT-EC/RPlan(s).

(5) Preplanned responsive action to minimize the effects of a disruption to mission critical services and applications and to prevent an unplanned or unscheduled shutdown in state data centers.

(6) Capability to enter agency specific data center and network communication resources, documentation, hardware/software, forms and supplies data and information into a database management system through the use of inventory work sheets.

(7) Access to maintenance instructions, report generation capabilities for applications, and backup resources for all data and information entered into the database management system.

EMERGENCY RESPONSE CARDS

The following procedures tie together the job-related need of an ACTIVE Employe for a RED Card with the mandatory requirement for a driver's license (or an ID card where an individual does not have a driver's license). Initiation of this procedure by an agency Security Administrator or appropriate authorizing manager eliminates the need for processing separate RED Card photos since a new photo is taken whenever a driver's license/ID card is issued and also eliminates the requirement to have the badges laminated. The RED Card is signed both by the employe and the Security Administrator. In the instance of an inquiry by an agency official, security and/or law enforcement officer, the driver's license/ID card photo and signature are used with the RED Card for positive identification.

(1) The Security Administrator shall review agency-wide requirements for staff RED Cards. There is an immediate need to REPLACE EXISTING RED Cards, preprinted with a 07/01/1996 EXPIRATION DATE.

(2) Upon completion of the review, a list of EMPLOYE NAMES WITH THE RELATED DEPARTMENT and/or BUREAU who are to receive RED Cards will be prepared and alphabetized. EMPLOYE NAME provided MUST BE EXACTLY as issued on the driver's license/ID card to ensure integrity and usefulness for positive identification. (In an emergency, there should be no confusion as to RED Card holder identity.)

(3) The completed, validated list of employes who are to receive RED Cards should be sent to the Central Management Information Center (CMIC), Enterprise Continuity/Recovery Planning.

(4) CMIC will provide necessary materials to produce agency requested RED Cards, i.e., Dutch Red Security Screen Card Stock and Vinyl Card Holders, as lists are received.

(a) The EMPLOYE, DEPARTMENT, and, BUREAU NAMES provided are printed on the front of the RED Card with space for the EMPLOYE'S SIGNATURE.

(b) Indicative, authorizing information is printed on the back of the RED Card with space for the SIGNATURE OF THE ISSUING OFFICER. (See the EMERGENCY RESPONSE CARD sample (next page).)

(5) CMIC will return the printed cards to the requesting agency Security Administrator for validation and EMPLOYE SIGNATURE.

(6) Accompanying the printed cards, CMIC also will provide the appropriate number of vinyl card holders for insertion of the signed RED Card and subsequent return to the employe. (Lamination is NOT required for this type card holder.)

(7) If, for any reason, cards must be changed or additional cards prepared, the Security Administrator should follow these procedures beginning at (2) above and submit the new or changed list to CMIC, EC/RPlanning.

(8) Upon presentation of the RED Card, the Security Administrator should request that the EMPLOYE keep it readily available at all times should there be an emergency.

COMMONWEALTH OF PENNSYLVANIA
EMERGENCY RESPONSE

NAME:
DEPT:
BUREAU:

Signature of Employee

Signature of Issuing Officer

FOR OFFICIAL USE ONLY: This individual is authorized to respond to Commonwealth emergency situations contingent upon health and safety conditions at the emergency facility.

COMMONWEALTH OF PENNSYLVANIA
EMERGENCY RESPONSE

NAME: **Vincent E. McNamara Jr.**
DEPT: L&I
BUREAU: BMIS Data Center

Signature of Employee

COMMONWEALTH OF PENNSYLVANIA
EMERGENCY RESPONSE

NAME: **Charles J. Fye**
DEPT: L&I
BUREAU: BMIS Data Center

Signature of Employee

COMMONWEALTH OF PENNSYLVANIA
EMERGENCY RESPONSE

NAME: **Charles A. Maguire 3rd**
DEPT: L&I
BUREAU: BMIS Data Center

Signature of Employee

COMMONWEALTH OF PENNSYLVANIA
EMERGENCY RESPONSE

NAME: **Christine L. Todd**
DEPT: L&I
BUREAU: BMIS Data Center

Signature of Employee

OFF-SITE STORAGE

To ensure that mission critical IT based resources necessary for continuous operation of an agency are backed-up at a separate, remote-site facility to facilitate 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 their jurisdiction and in the instance of an emergency, ensure that mission critical services and applications can be maintained or restored.

MISSION-CRITICAL RESOURCES	Off-Site Storage Contractor or Equivalent[1]	Back-Up Site[2]
• "Emergency Continuity/Recovery Plan"	X	X
• Inventory Records: Hardware, System/Application Software, Tape/Disk Libraries, Supplies, Schematics and Floor Plans	X	
• Master Files	X	
• Transaction Files	X	
• Database, Data Files	X	
• Operating Systems Software	X	
• Application Software	X	
• Libraries, Software	X	
• Source and Executable Programs	X	
• Security Software	X	
• ALL Documentation Required To Process Mission Critical Applications	X	X
• Systems, Programming, Operations, and Run Book Documentation	X	X
User Documentation	X	X
• Inventory of ALL Other Materials, Supplies, Documentation Needed for Processing at an Alternate Site	X	X
• Journals, Software		X
• Special Forms/Critical Supplies		X

———————————————————————

[1] Protected in an environment approved by OA/IT.

[2] Stored at alternate recovery site or a location external to primary site.