CITY OF KEY WEST INDEMNIFICATION FORM

Contractor agrees to protect, defend, indemnify, save and hold harmless The City of Key West, all its Departments, Agencies, Boards, Commissions, officers, agents, servants and employees, including volunteers, from and against any and all claims, debts, demands, expense and liability arising out of injury or death to any person or the damage, loss of destruction of any property which may occur or in any way grow out of any act or omission of the Contractor, its agents, servants, and employees, or any and all costs, expense and/or attorney fees incurred by the City as a result of any claim, demands, and/or causes of action except of those claims, demands, and/or causes of action arising out of the negligence of The City of Key West, all its Departments, Agencies, Boards, Commissions, officers, agents, servants and employees. The Contractor agrees to investigate, handle, respond to, provide defense for and defend any such claims, demand, or suit at its sole expense and agrees to bear all other costs and expenses related thereto, even if it (claims, etc.) is groundless, false or fraudulent. The City of Key West does not waive any of its sovereign immunity rights, including but not limited to, those expressed in Section 768.28, Florida Statutes.

These indemnifications shall survive the term of this agreement. In the event that any action or proceeding is brought against the City of Key West by reason of such claim or demand, Contractor shall, upon written notice from the City of Key West, resist and defend such action or proceeding by counsel satisfactory to the City of Key West.

The indemnification provided above shall obligate Contractor to defend at its own expense to and through appellate, supplemental or bankruptcy proceeding, or to provide for such defense, at the City of Key West's option, any and all claims of liability and all suits and actions of every name and description covered above which may be brought against the City of Key West whether performed by Contractor, or persons employed or utilized by Contractor.

The Contractor's obligation under this provision shall not be limited in any way by the agreed upon Contract Price as shown in this agreement, or the Contractor's limit of or lack of sufficient insurance protection.

CONTRACTOR: Postal Center International, Inc. SEAL:

3406 S.W. 26 Ter.
Fort Lauderdale, FL. 33312
Address

Signature

Stephen Gussman
Print Name

Executive Vice President
Title

DATE: April 9th, 2012

UNIT PRICE BID SCHEDULE

Quantities may vary due to online billing and conversion of City's sewer billing to Florida Keys Aqueduct Authority.

Printing of Bills, Stuffing of Envelopes, and Processing of Information per month -		$951.707
Billing Stock		
8 ½" x 11" 20 pound stock	(12,100 quantity) per month-	$149.19
# 9 Envelopes	(12,100 quantity) per month-	$302.651
# 10 Envelopes	(12,100 quantity) per month-	$347.875
9" x 12" Insertion Envelopes	(70 quantity) per month-	$66.50
Postage (pass through)	(12,100 quantity) per month-	$4,525.40
Other (Please List Each Item)		Ø

TOTAL - $6,343.32

PCI POSTAL CENTER INTERNATIONAL

Disaster Recovery Plan

Tuesday, January 31, 2012

3406 SW 26 Terrace • Fort Lauderdale, FL 33312
(P) 954-321-5644 • (F) 954-797-8697 • www.surfpci.com

Table of Contents

Part I – Introduction and Overview

Part II – Plan Strategies

Part III – Disaster Response Actions

Part IV – Orientation and Plan Awareness

Part V – Facilities Restoration

Part I. Introduction and Overview

INTRODUCTION

Crisis management is PCI's first response to a business operations-altering event. Proper Management will help significantly ensure the employees, customers, partners and the general public continue to have confidence in the financial viability of the company.

This Disaster Recovery Plan focuses on the first component describing recoverability of the Postal Center International main computing facility at 3406 SW 26th Terrace, Ft Lauderdale, Florida 33312 and/or the facility at 10561 Satellite Blvd, Orlando, Florida 32837.

Overview

Section 1.01 Statement of Purpose

This document describes the facility disaster recovery plan for Postal Center International. It details how each organizational unit will carry out their responsibilities in the event of a disaster. It also describes the provisions and safeguards undertaken in such an emergency.

Management supports this cost effective and documented plan for reacting to a disaster that may disrupt the everyday computer operations at either of the two PCI entities. This document will serve as a resource to Management during and following a catastrophic event that negatively impacts the computer hardware, software, networks, and telecommunications system.

Definition: A disaster is "an occurrence inflicting widespread destruction and/or distress." For the purposes of this document; the facilities, computing resources, or major components thereof, would be deemed unavailable for operations.

The following are the major purposes of this document:

(a) To plan for ongoing operations in the event of a disaster.
(b) To detail and describe the level of contingency preparations for management review.
(c) To prioritize and outline the recovery of pre-defined critical components, systems, and applications.
(d) To develop an organizational preparedness so that disruption and chaos are minimized.
(e) To anticipate vulnerabilities regarding the security and protection of the facilities.

Section 1.02 Scopes of the Plan

The scope of this plan is limited to the services and responsibilities of PCI's - Director of IT group (PCI-IT@surfpci.com) and cover these major resources:

(a) Computing facilities
(b) Computer hardware and systems software
(c) Enterprise network electronics, transport, and ISP access
(d) Telecommunications services
(e) Databases, electronic media and files
(f) Computer programs
(g) Computer execution and operation's procedures
(h) Documentation

The disaster recovery plan provides only for the continuation of certain essential technology services and information processing activities during the period of time required for recovering from a disaster.

Section 1.03 Procedures for Assessing Degree of Crisis

The PCI Management team will confer with the Crisis Assessment Team about the imminent crisis in an effort to classify the magnitude of the crisis as defined within this plan. The Crisis Assessment Team will be comprised of the following members (in descending chain of command order):

(a) The Executive Vice President
(b) The Director of IT
(c) The Network Administrator
(d) The Data Services Manager
(e) The Operations Manager's

This group shall survey the scope of damage and advise the Executive Vice President (or the available designee) about rendering a disaster classification. The pending decision may initiate the disaster recovery response action plan detailed in this document.

Crisis Designations

The following are crisis classifications that the Crisis Assessment Team may designate:

Category 3 - A major disruption in service affecting a subset of users or systems deemed to be non-critical for alternate site recovery.
The determination is that the disaster recovery plan provisions should not be implemented because the presenting problem(s) were determined to fall within existing operational resolution capabilities. Within this classification routine management and user communication channels would be utilized.

Category 2 – A major disruption to one or more entities, Recovery of services at prime location is more than 24 hours. Restoration at alternate site will consume more time than repairing at primary location.
Such damage as occasioned by water, smoke, fire, vandalism, terrorism, lightning, or any other causes that bring about an estimated period of technology services disruption deemed to be more than 24 hours in duration.

Under this classification the disaster response action plan, described elsewhere in this document, should be initiated only when there exist coincident critical processing turnaround needs. Such needs will be defined by the Director of IT and will be based on knowledge of processing schedules and the status of work in progress.

The recovery actions shall be directed primarily to reactivating processing within the facility.

Category 1 - A total system(s) outage affecting multiple entities, systems, and customers, Anticipated recovery at prime location(s) is impossible or expected to exceed 24 hours. Recovery at alternate site is more rapid than at primary location(s).
Such damage as occasioned by water, smoke, fire, vandalism, terrorism, lightning, or an estimate of a protracted period of equipment downtime that renders a major portion of the facility unusable for more than 24 hours.

Under this condition the disaster response action plan, stated in this document, shall be initiated.

Section 1.04 Chain of Command/Decision Making

The Executive Vice President, or designee, is in charge of evaluating and declaring the disaster classification. In the Executive Vice President absence, the Director of IT shall be responsible for these actions. Working together with the Executive Management of PCI, the final approval for execution of this recovery plan will be established and communicated to the necessary employees and the customer community. The Executive Management contacts are as follows:

Executive Vice President, Postal Center International
President, Postal Center International

Once notified, the Crisis Response Team will conduct further internal communications and will apprise the Executive Management of the plan's execution and its ongoing status.

Section 1.05 Telephone Tree/Crisis Management Immediate Contact Roster

In an effort to conduct rapid and simultaneous notifications, a calling tree approach will be used. Details regarding personnel and contact information will be maintained in the Disaster Recovery Plan Documentation with key contacts included.

If any PCI employee becomes aware of an existing emergency situation, or a potential crisis/disaster, they will immediately notify their direct Supervisor. If not available, the Site Manager should be directed to contact the Executive Vice President.

(a) **Crisis Management Team Notification**
Immediately upon the declaration of a disaster defined within this Plan, the Executive Vice President, or designee, shall notify the Management Team of the crisis.

(b) **Notifications within PCI**
In the event of a disaster declaration, the Director of IT, acting as the Executive Vice President's Disaster Operations Designee, shall immediately notify the remaining Management Team, OPS Direct Reports. Thereafter, each department manager shall notify their immediate personnel. These, in turn, will contact and notify the personnel within their departments, if the chain of command extends further.

More importantly, the Crisis Recovery Team, as outlined in the Disaster Recovery Plan Strategies procedures, will be contacted to commence execution of the recovery process. These notifications will be made, top down, by supervisory personnel. Supervisory personnel are expected to know how to reach any employee at work, home, or vacation (if such contact is feasible) by telephone, cellular phone, or email. During such notifications the staff shall be advised of their subsequent reporting locations and, if known, any specific immediate work assignments. The PCI Hotline will apprise all employees of next steps.

Section 1.06 Procedures for Communicating with External Authorities

The Executive Vice President (or designee) is designated with the responsibility for communicating with external public safety and security agencies such as police, fire, and other public safety officials.

All external notifications and communications with sponsoring agencies, financial institutions, insurance institutions, governmental entities, and media outlets shall be conducted by the Executive Vice President or a spokesperson designated by the Executive Vice President. The Executive Vice President shall have the sole franchise to speak about the disaster or its implications with all media external authorities.

Section 1.07 Procedures for Communicating Internally

(a) **Telephone-based communications**: Using telephone trees and distributed calling responsibilities, PCI staff will be notified once a disaster is declared.

(b) **Hotline Communications for disseminating ongoing status information**: If the PCI Hotline is operative this shall be used as the official method for communicating ongoing status information. This is a prerecorded message outlining time of recording, event status, and time of next update.

(c) **Voice Mail**: Emergency announcements can be disseminated internally using overall existing voice mail announcement capabilities. This would entail delivering a recorded and stored message to all voice mail users who will receive the message upon their next use of the voice mail systems. The voice mail distribution capability falls under the auspices of Telecommunications Services and represents an efficient and economical means to deliver an official message rapidly to a broad internal audience.

(d) **Mail-based communications**: Depending on the of the senior administration it may be desirable to broadcast official information concerning the disaster to the PCI community. If electronic mail facilities continue to be functional, emergency announcements can be sent through this medium.

If PCI electronic mail capabilities are not adequately available for this requirement, third party Internet Service Provider (ISP) email facilities will be used to attempt contact with Internet subscribers. It is recognized that not all individuals possess ISP accounts, but for those who do, this is a viable communication method. Instant Messenger is also available via the Internet for communications.

Alternatively, paper-based office mailings can be launched either individually addressed using address labels or by bulk mail delivery to departments. FAX is also an acceptable means to distribute this correspondence.

Section 1.08 Criteria for Determining the Success of the Plan

This review and rehearsal process will ensure the following success factors:

(a) Keeping the Disaster Recovery Plan up to date can be demonstrated by the stipulated process of annual reviews, plan revisions, and by the summary document the Executive President receives about this annual process and assessment.

(b) The success of applications testing is also demonstrable through the documentation and outputs that are created through this activity.

(c) The ongoing discussions about crisis management and disaster recovery planning are contributing to the success of the current plan. The key parameters of the plan are known, understood, and accepted. The crisis management discussions have been taking place at increasingly higher management levels, and as such are being properly focused on the overall planning requirements together with the cost benefit implications of various protection levels.

Section 1.09 Built-in Plan Review Procedures and Schedule

Reviewing the Plan: To assure the plans continued accuracy and viability. The Executive Vice President shall review the Disaster Recovery Plan periodically. Maintenance of the plan and overall coordination of plan activities (such as rehearsals and department activities) will be performed by the Crisis Response Team.

Additional reviews will be performed as follows:

(a) The Director of IT shall make an appraisal of the plan annually, and formally comment to the Executive Vice President about the plan's effectiveness status in writing.

(b) A copy of the annual Plan appraisal shall be forwarded to the Executive Management Team.

(c) Annually, the status of the Disaster Recovery Plan will be discussed with the Executive Management Team.

(d) Commentaries and findings about the Plan's periodic review of its provisions for the testing of specified applications at both facilities, and about the review of the off-site data storage program, shall be incorporated into the annual status reporting.

Section 1.10 Identification of the Person in Charge of the Plan

The Executive Vice President has designated the responsibility for maintaining this Disaster Recovery Plan document to the Director of IT. Maintenance of the plan includes adherence to the periodic review provisions defined within the plan, monitoring the periodic preparedness testing, and maintaining the ready state of the plan for potential deployment.

Part II. Plan Strategies

Section 2.01 Contingency Site

Postal Center International has contracted with MailMax Services for disaster recovery services including contracted hot site equipment. This contract guarantees availability of the contracted equipment and a data center in which to recover the PCI computing environment. The primary recovery facility is located in Waco, Texas. This agreement does not provide for recovery of all PCI computing platforms or business entities. It specifically outlines highly specialized computing resources to be recovered, generally housed in the Data Center at Fort Lauderdale facility, 3406 SW 26th Terrace, Ft Lauderdale, Florida 33312.

The overall approach to recovery leverages the geographic dispersal of the two (2) PCI facilities as well as an extensive network that interconnects these facilities. Computing resources more readily available through distributor channels or readily available within the PCI Environment, in the form of test equipment, will be used to recover production systems. This will be done within the computing facility if accessible. In the event the computing facility is damaged or otherwise inaccessible, the corporate front office of PCI will be used as a cold shell to recover equipment local to the PCI Environment. This reduces the amount of bandwidth required to sustain high traffic to the Ft. Lauderdale facility and is not obtrusive to other computing operations.

In order to begin to use the contingency site at MailMax for actual recovery, an official disaster declaration process must be followed. This declaration process mobilizes resources at MailMax to prepare for the arrival of magnetic media, configuration of contracted resources to be recovered to, and provisions additional resources needed to commence recovery in anticipation of the arrival of PCI Crisis Recovery Team.

Section 2.02 Backup Environments Network Equipment

There is no feasible way to provide a backup environment for the PCI premises based network equipment. However, much of the data communications equipment in use is manufactured by Cisco Systems and SonicWall and is covered under a maintenance agreement. PCI has dual internet connections for backup, provided by 2 different carriers (ISN and Sprint) also under maintenance agreements. Under the terms of this agreement, all of this equipment is eligible for next-day advanced replacement. Networking Services keeps on-site most of the common Cisco equipment. For wide-area

connectivity, PCI uses routers manufactured by Cisco. This equipment is also covered by a maintenance agreement with Cisco. All of this equipment is eligible for next day advanced replacement should a failure occur. Our wide-area network (WAN) allows us to operate our daily network operations from Fort Lauderdale or Orlando as well as backup all of our data between the two (2) campuses. Our web site and FTP services have a backup facility outside the state. This facility has backup internet connections as well as power generation and is managed 24/7.

Section 2.03 Application Testing Plan

Designated applications are periodically tested at the contingency site's computer facility in order to verify functional condition of the contingency procedures. The purpose of these tests is to ensure the processing viability of vital applications off-site, assuming that the present computing facilities are unavailable.

Periodic component and system level tests will be performed at each of the PCI facilities in Ft Lauderdale, FL, and Orlando, FL. These tests will validate specific recovery procedures for key applications and infrastructure components. It will also ensure the precise documentation of all recovery activities required in the event of a disaster declaration. These tests are conducted throughout the year exercising various facets of the recovery plan and applications. Key applications undergo a complete system test at least every 6-12 months.

Recovery exercises include the testing of on-line as well as batch workflows to determine the veracity of backup procedural controls; bulk *printing of hard copy output is usually suppressed during these off-site tests.*

Section 2.04 Applications Analysis

A detailed analysis of critical applications and key processing components has been performed to identify and prioritize recovery efforts. These applications are considered business critical and must be included in any recovery plan to sustain the operational/financial viability of the company.

A detailed list of the applications follows for each of the PCI entities. This list is reviewed and updated periodically to ensure completeness. Executive Management may subsequently alter these priorities depending on timing requirements or special circumstances prevailing at the time of a disaster.

Ft Lauderdale

- Payroll system
- Accounts Payable Check Processing
- Purchase Order Preparation
- General Accounting
- Financial Accounting
- Accounts Receivable
- Human Resources Applications
- All Daily Laser Print Client Applications
- All Production database utilities that house customer data

Orlando

- All Production database utilities that house customer data

Section 2.05 Local and Off-site Media and Backup Storage

System backups are maintained on cassette tape media for all systems for the purpose of operational and disaster recovery. Multiple versions of backups are maintained on a weekly basis (unless otherwise specified by application backup requirements). The most recent version of the backup is rotated to our Orlando facility, a local offsite vaulting service, and an out of state data storage facility. This ensures that recovery of any system is at most a week old. If warranted, more current backup provisions are outlined in the specific application Disaster Recovery Plan.

Each application system is responsible for providing its own routine operational backup and recovery means as part of its design and regular operation. Reliance on the application's on-going ability to furnish backup is the principal strategy for immediate data set recovery.

Section 2.06 Telecommunication Services

Local Telephone Service: ISN provides incoming and outgoing local telephone lines to the facility telephone system. In the event that the ISN serving wire center experiences a catastrophe, PCI will switch to Sprint cellular phone service and Sprint satellite internet service.

The main facility telephone number will be redirected to our alternate site or a designated offsite telephone until the alternate site is able to receive calls through the telephone system.

Long Distance Service: ISN outgoing long distance service will be available as soon as ISN establishes outgoing dial tone. All ISN 800 services will be redirected to an alternate location or telephone number.

Section 2.07 Organizational Responsibilities Identification

General - In light of existing emergency conditions, the following contingency actions may be required:

(a) **Systems Development**: Depending on the Director of IT, some or all systems development work may be deferred. This is to be able to provide maximum assistance to impaired operations and to restoration initiatives.

(b) **Processing Order**: Depending on the Director of IT, in concert with the Production Managers, various shortcuts in processing procedures may be undertaken; including within the applications that may be identified as priority applications.

(c) **Vacations**: Depending on the Executive Vice President, any scheduled vacations may be deferred, and any vacations already in progress can be cancelled. In the event individuals incur financial loss occasioned by required changes in vacation plans, if demonstrable - such loss shall be reimbursed.

(d) **Ongoing Operations**: It will be the continued responsibility of the Director of IT in concert with the Production Managers to provide ongoing data center operations support for all production processing.

Part III. Disaster Response Actions

The below actions can only be undertaken when a disaster classification of Category 1 exists: as defined in part I of this document. All communications shall explain and include reference to the defined nomenclature of the disaster classification.

Once the classification of a disaster is made, and it is determined that disaster conditions exist, the Disaster Assessment Plan is to be implemented immediately. This step is undertaken formally once the

management notifications under the Plan begin.

The "end disaster" conditions must also be communicated formally through such management notifications.

Section 3.01 Pre-Disaster Procedures

If PCI is under the potential threat of a disaster, as mentioned in Category 1 of this document, all computers, printers, copy machines, and warehouse equipment will be secured and protected with tarpaulins/plastic. All computers and servers will be powered down and unplugged. Equipment will be moved to the safest locations within the building – away from doors and windows, the most secure room, etc... If the threat is a hurricane, hurricane shutters will be mounted.

Fuel will be procured for use in two small portable generators, two mid-size portable generators and two John Deere Triton facilities generators, if the Executive Vice President deems the damage to be minimal enough that the facility could still be productive with this energy source.

Employees are provided with emergency contact information (home telephone, cell phone, PCI Hotline number, and email address, if applicable). Employees also provide their immediate supervisor with their personal contact information. Employees are instructed to contact their immediate supervisor for updates throughout the ordeal. As stated earlier in this document, a telephone tree system will be in use during a disaster to continually inform the employees of their work status.

PCI will activate the Disaster Recovery Hotline (Satellite Phone). The hotline is available by dialing (954) 734-9560

Section 3.02 Post-Disaster Procedures

Category 3
Equipment Failure

1. PCI's large volume of mail processed daily warrants at least one back-up of every essential machine. Please see PCI equipment list under separate cover.

2. In addition to support provided by Manufacturer's technicians (on call 24 hours a day), PCI employs on-site certified technicians at all locations. PCI operational employees are trained and certified by Bowe Bell + Howell, Heidelberg, and Pitney Bowes, and Konica to repair and maintain the following on-site machinery:

a. Bowe Bell + Howell
    I. Three (3) Letter Mail Size - Multi-Line Optical Character Readers (MLOCR)
    II. One (1) Flat Mail Size - Multi-Line Optical Character Readers (MLOCR)
    III. Two (2) Intelligent Inserters (Accumulate, Fold, Insert)
    IV. Four (4) Non-Intelligent Inserters.
b. Heidelberg
    I. One (1) 9110 Digital Laser Printers
    II. Three (3) Konica Digital Laser Printers
    III. Mx7000 Digital Laser Printers
c. Pitney Bowes
    I. Thirteen (13) DM1000 Metering Systems
    II. AccuTrac Postage Accounting System

PCI maintains replacement parts on site for immediate and routine repairs. All parts are available from our manufacturers overnight. PCI has a maintenance contract with all manufacturers directly. PCI does not use manufacturer representatives or resellers.

Local Emergencies

In case of local electrical outages, PCI houses two small and two mid-size portable generators and two John Deere Triton facilities generators to provide emergency power to all essential equipment.

Category 2

If PCI's facility has to be temporarily evacuated (due to fire, explosion, etc.) or is inaccessible for an undetermined amount of time, the following must occur *within 3 hours* of crisis assessment:

1. Transfer affected facility to an alternate operational facility if telephone system is non-operational.
2. If the T1 line is down - Switch to secondary satellite internet connection.
3. The Director of IT will contact each Daily Laser Print client.
    a. Clients will be instructed to utilize the backup ftp site. IP address, User ID, and password have been previously provided. Backup ftp is located in Minnesota.
    b. Clients will be instructed to utilize alternate email addresses. Alternate email addresses are previously provided.
4. The Ft Lauderdale/Orlando facilities will take over normal print and fulfillment operations as they become operable.

Category 1

If it is determined that the roadways are safely passable, and the office is safely inhabitable, employees are instructed to return to work for assignments. If roadways or the office are unsafe, a limited number of key employees will meet at a place determined to be safe, to discuss which course of disaster action plan will be taken.

No Power

a) If there is no power, switch to the facility's generator power.
b) If phone lines are down – transfer affected facility number to an alternate operational facility.
c) If T1 line is down - Switch to secondary satellite internet connection.

No Facility Generator Power

Within 12 - 24 hours of crisis assessment:

(a) Switch to portable generator power for skeleton equipment (servers, critical computers) if facility is accessible but main facility generator is not functioning
(b) Transfer main number (954.321.5644/407.852.1700) to cell phone (954.931.0068).
(c) If T1 line is down - Switch to secondary satellite internet connection
(d) Director of IT will contact each Daily Laser Print client
    a. a. Clients will be instructed to utilize an alternate ftp site. IP address, User ID, and password are previously provided. Backup ftp is located in Minnesota.
    b. b. Clients will be instructed to utilize alternate email addresses. Alternate email addresses have been previously provided.
(e) Daily Customer Service Representative will stay in touch with Daily Mail pickup clients.
(f) Digital Customer Representative Manager will touch base with Project mail clients.
(g) There are over 30 couriers servicing Dade, Broward, Palm Beach and Orlando. If no communication has occurred with specific clients, the couriers will physically drive to client locations to determine client needs and status.
(h) If Miami is an acceptable Disaster Recovery site – contact Diginet Printing for temporary printing while an alternate Disaster Recovery location is secured.
(i) If an out of state solution is necessary, contact MailMax in Waco, Texas.

(j) Replication of data (Tape backups/CDs/dongles) is to be sent to alternate site, if other than Orlando.
(k) Schedule the transport of additional required Paper/Envelopes/Materials to backup site.
(l) Director of IT, Operations Manager/Supervisor, and other designees will travel to Disaster Recovery site and set up operations within 48 hours.
(m) Ft Lauderdale/Orlando facility will take over normal print and fulfillment operations as they become operable.
(n) Mail will be transported to the closest open and operating USPS location.

Note: Our Orlando facility currently houses our standard materials (paper and envelopes) backup. Orlando's server replicates all daily laser print customer systems.

Part IV. Orientation and Plan Awareness

To ensure effective operation of the disaster recovery plan, strategies, procedures, and actions described within this document, all parties involved with its implementation must be aware of the potential threats ensuing by a disaster and of their responsibilities under the plan. Both systems personnel, who will be actively engaged in recovery operations and functions, and the user community, which must adjust to emergency procedures, must be properly prepared, informed, and trained.

Section 4.01 PCI Personnel Orientation

One of the purposes of the disaster recovery plan is to increase awareness of all parties to the potential threats posed by a disaster, and to acquaint them with the company's strategies, expectations, procedures and actions required under such emergency conditions.

The goal of orienting the staff at PCI is more specifically geared to achieve a detailed understanding of the expectations by which they must operate when a disaster is declared. Toward this end the following actions are planned:

In order to complete a periodic review of the disaster plan document. This is carried out by:

(a) Holding periodic staff meeting presentations and reviews.

(b) Circulating a copy of the plan to individuals based on levels of responsibility as follows:

1) Executive Management within PCI
2) Managers and Supervisors within PCI

(c) During the design stage of new systems, Systems Analysts recommend how the application systems under development can be appropriately protected against a disaster. Recommendations should be geared to raising the users' awareness toward the potential risks and changed liabilities for the application area.

Section 4.02 Disaster Plan Testing

Tests of the disaster plan, or of one or more of its facets, will be conducted periodically and/or may be requested by management to insure that elements of the plan are feasible, compatible, and effective. An objective of this testing will be to minimize interference and interruption of the normal production operations. While most exercises are performed on a scheduled basis, an unannounced recovery may be conducted to validate preparedness for unanticipated outages.

The following tests are designed to be undertaken periodically and documented:

(a) Applications designated as critical by management shall be periodically tested in a backup

environment.

(b) A review of the plan's disaster announcement, communication and notification provisions should be periodically conducted to test this component of the plan. The review should deal with updating the names and contact details contained in the plan.

(c) Periodic tests shall be made of the timeliness and content of the off-site storage arrangements.

(d) Periodic tests shall be made of the contents of the off-site storage vault. The tests should validate that the required materials (recovery kits, manuals, tapes) are physically present.

Part V. Facilities Restoration

The objective of Facilities Restoration is to establish a viable/ongoing processing facility, upon completion of the use of computing operations from the contingency site. This may require an extended period of time depending on the crisis event experienced and the extent to which the original data center facility is unacceptable for ongoing operations.

Section 5.01 Restoration Designee

a) Primary restoration designee: The Director of IT shall coordinate all facilities and equipment restoration efforts.

b) Alternate restoration designee: The Network Administrator shall be the alternate restoration designee.

Section 5.02 Responsibilities

Conduct an assessment of damage to the facilities together with:

a) Hardware vendors' representatives for salvage, repair, or replacement
b) Software vendors' representatives for salvage, repair, or replacement
c) Client representatives for data transmissions or general communications issues
d) Telephone company representatives for any communications and connectivity issues
e) Operations staff for the cleanup and restoration of the facility

Develop a restoration plan, which includes realistic cost and time estimates, to be forwarded to the Operations Designee and to Executive Management.

This effort will be primarily based on Dell special hardware disaster recovery support plans. The replacement of systems software will need to receive special attention since it will be unlikely that an identical hardware replacement configuration can be implemented under emergency conditions. For this reason, it will be necessary to make immediate arrangements with Dell for their free of charge defined systems support. In addition, it may be necessary to purchase extra systems support from Dell or other sources. The Director of IT shall make these decisions and arrangements with concurrence of the Executive Vice President.