DISASTER RECOVERY PLAN

FOR
Amerijet International, Inc

Prepared by:
Amerijet Information Technology Department
July, 2005

Table of Contents

1.0 Plan Introduction

Amerijet International recognizing their operational dependency on computer systems, including the Local Area Network (LAN), Database Servers, Internet, Intranet and e-Mail, and the potential loss of revenue and operational control that may occur in the event of a disaster; authorized the preparation, implementation and maintenance of a comprehensive disaster recover plan.

The intent of a Disaster Recovery Plan is to provide a written and tested plan directing the computer system recovery process in the event of an interruption in continuous service resulting from an unplanned and unexpected disaster.

The Disaster Recovery Plan preparation process includes several major steps as follows:

- Identify Systems and Applications currently in use.
- Analyze Business Impact of computer impact and determination of critical recovery time frames.
- Determine Recovery Strategy
- Document Recovery Team Organization
- Document Recovery Team Responsibilities
- Develop and Document Emergency Procedures
- Document Training & Maintenance Procedures.

These steps were conducted and this document represents the completed effort in the preparation of the Amerijet International Disaster Recovery Plan.

Acronyms and abbreviations used in this report:

UUNet	
ITN	International Transport Network, 7007 N.W 30th St Miami
MIA	Amerijet Warehouse, 72nd Street, Miami
CC	“Cargo City”, Building 716, Miami Airport
HQ	Headquarters, 2800 Andrews Ave, Ft. Lauderdale
FLL	1401 SW 39th St, Ft. Lauderdale Airport

JFK (New York), IAH (Houston), POS (Port of Spain) – Amerijet
Stations that have domain controllers

1.1 Mission and Objectives

The mission of the Disaster Recovery Plan is to establish defined responsibilities, actions and procedures to recover the Amerijet International computer, communication and network environment in the event of an unexpected and unscheduled interruption. The plan is structured to attain the following objectives:

- Recover the physical network within the Critical Time Frames established and accepted by the user community.
- Recover the applications within the Critical Time Frames established and accepted by the user community.
- Minimize the impact on the business with respect to dollar losses and operational interference.

1.2 DRP Scope

The scope of the plan is to recover computer information services provided by the Amerijet International data center and networks located at UUNet, Miami, Florida. The LAN network encompasses the following:

- e-Mail (Lotus)
- General business applications, such as word-processing, spreadsheet (Microsoft Office)
- Database storage (DAT) and application (SQL Server)
- Proprietary air cargo system (ACMS) and 3rd party freight forwarder system for ocean & air cargo (OASIS)
- Flight scheduling/routing (Geneva) and flight path planning (Navtech)
- Financial and accounting system (Southware)
- Document Imaging Server and application (Scanfast)
- Materials Inventory Control system (PMI)
- File servers supporting all business operations
- Proxy and Firewall support
- Web server
- Proprietary portal system (Websphere)
- Domain controllers
- VPN support (Cisco)

1.3 Authorization

The management of Amerijet International recognizes the need for a Disaster Recovery Plan for all operations directly or indirectly dependent on data processing. The Chief Information Officer for Amerijet International has authorized the development and ongoing maintenance of this plan.

1.4 Responsibility

Responsibility for the development and maintenance of the plan is assumed by the Information Technology group. Specific responsibility for ensuring the plan is maintained and tested rests with the Amerijet International DRP Support Group. In consideration of this responsibility, the end user community is responsible to coordinate with the Project Manager for their information technology requirements.

1.5 Key Plan Assumptions

The following assumptions have been established as the basis for the development of the Disaster Recovery Plan:

- The plan is designed to recover from the "worst case" destruction of the Amerijet International operating environment. The worst case excludes any non-data processing function that may be in close proximity to the data center or workstations.
- Although the plan is designed for worst case, inherent in the plan strategy is the ability to recover up to the most minor interruption, which is perhaps a more likely situation.
- The plan is base upon a sufficient number of center staff not being incapacitated to implement and affect recovery. Therefore, the level of detail of the plan is written to a staff experienced in the Company's computer services. Development, testing and implementation of new technologies and applications are suspended so that all resources are available to recover existing critical production processing.
- Off-site location of equipment and rapid acquisition of replacement equipment from vendors is considered to be the only resource with which to recover communications and computer processing.
- Amerijet maintains most of its servers at an external site that is constructed to resist natural disasters such as hurricane, flood, fire.
- We anticipate damage would be constrained to telephone lines, fax and imaging machines, satellites (where still used), employee computers, domain controllers, and the few servers that are still housed in offices. (HQ, our MIA Warehouse, our "Cargo City" Miami Airport facility, ITN, JFK, IAH, POS). .
- The computer facilities of any alternative data-entry sites is not within the scope of this plan and is assumed not to be impacted by any disaster which may interrupt computer operations at Amerijet International offices. UUNet, our external data center is advertised to be impervious to any disaster.

1.6 Disaster Definition

The Damage Assessment Team is charged with assessing the damage to the data center and reporting to the Management Team. The objective is to report the assessment of damage within four hours of the interruption.

The Management Team makes a decision whether to stay and repair the damage, or move local computer operations to off-site recovery locations. Therefore, the definition of a disaster is:

> Any interruption to the computer operation that prompts a decision to go to off-site recovery locations.

2.0 Business Impact Analysis

A Business Impact Analysis was conducted to ascertain the impact of a disaster on the operations of each operating unit within Amerijet International. The Business Impact Analysis drives the Disaster Recovery Plan by identifying and substantiating those applications and systems with the greatest impact on the business in the event of a disaster.

In turn, this provides for the determination of the most cost effective recovery time period for each system and application. Recovery times are established and accepted by the user community.

2.1 Scope

The scope of the Business Impact Analysis is the Amerijet International operating departments supported by data center facilities located at local offices and UUNet. This network encompasses the following information technology services:

- General business applications, primarily Excel spreadsheets
- SQL Server database applications
- e-Mail
- File servers supporting all business operations
- Accounting and Proprietary cargo management software.

To determine the maximum time frame allowable, the following Amerijet International operating departments were interviewed:

- Information Technology
- Finance & Accounting
- Business Development:
  Stations, Sales, Marketing, Interline, & Claims
- MIA Warehouse, HUB, & Security
- Flight Operations
- Material Services
- Human Resources
- Facilities Maintenance
- Customer Service
- ITN Consolidators

2.2 Objectives

The Business Impact Analysis is completed to determine the Critical Time Frame in which the application system capabilities and functionality must be available after a interruption in service to minimize the operational loss of control and potential loss of revenue. In addition, the Business Impact Analysis assists in identifying alternative manual procedures which may be use during an interruption in service. Therefore, the objectives of the Business Impact Analysis are:

- Educate user on the need for a disaster recovery plan
- Identify the Critical Time Frames for each application by user
- Identify alternative manual procedures which may temporarily minimize impact due to an interruption in computer service
- Identify the shortest Critical Time Frame for each application

2.3 Critical Time Frame

The purpose of the Business Impact Analysis is to determine the maximum time frame that each Amerijet International operating department can be without the functionality of the system without incurring material operational interference in the event of a disaster. This time frame will be referred to as the Critical Time Frame.

The Critical Time Frame (CTF) is defined in business days as the elapsed time between the point of the interruption up to the point where the system must be functional.

Recovery procedures in the plan are staged around the most critical application which has the shortest CTF to the application with the longest CTF. According to the Business Impact Analysis the application with the shortest CTF are the email and Southware/ACMS systems and the longest is the Material Services PMI module. Although each system may have a different time frame, the plan as a whole carries the time frame on the application with the shortest. Therefore, the plan as a whole has an 8 hour Critical Time Frame.

2.4 Application System Impact Statements

The result of the interviews with the Amerijet International operating departments is a narrative of the effect of a system outage or interruption assuming a worst case scenario. There is a narrative for each utilized application by operational department located in the Interview documents, available under separate cover.

The narrative indicates the operational departments dependency on computer support and indicates the Critical Time Frame that the operational department can be without the applications functionality.

Application System Impact Statements, the output of the Business Impact Analysis, are used to classify each application into the categories of essential, delayed or suspended.

1. Essential

An application is considered “essential” if its loss would affect Amerijet International’s ability to remain solvent through financial loss or impart a serious loss of operational control.

2. Delayed

An application is classified as “delayed” when the function can survive without computer processing support for a period of time. Resumption of computer processing begins only when resources are available in excess of the requirements for the essential category; however, the passage of time can escalate the criticality of the application.

3. Suspended

Some business functions may have computer support "suspended" or discontinued indefinitely. Resumption of processing begins again when full computer capability is restored. Typically, the passage of time does not cause the escalation of the criticality of suspended systems, however, they may be processed using any available resources when the requirements of the essential and delayed systems are satisfied.

2.5 Summary Conclusion

A summary of the Application System Impact Statements, outlining the period of time before an application's loss becomes critical and classifying each application as essential, delayed or suspended, is as follows:

Business Impact Analysis Matrix

Application	1-2 Days	3-5 Days	6-10 Days	11-14 Days	Two Weeks +	Category	Alternate Access - application/data?
Web browser, connection to Internet	CT					Essential	Employees' personal ISPs
Gen. Business Apps.(Excel)	MN	MD	CT			Delayed	Local on laptops
Email	CT					Essential	Internet
SQL server	MD	CT				Essential	
Southware/ACMS	MD	CT				Essential	
ADP Payroll Access	MN				MD	Delayed	Verbal (phone)
OASIS	MD	CT				Essential	
Geneva & Navtech	MD			CT		Essential	Internet processing
Flight Ops manuals	CT					Essential	Internet access
PMI	MN	MN	MD			Delayed	
Document Imaging	MN	MD				Delayed	Internet - retrieval

MN =	Minimum Impact
MD =	Moderate Impact
CT =	Critical Impact

Assumptions:

- All departments have backup of My Documents (users\login_name) directory and subdirectories from their building's domain controller server on CD-ROM for restore to local laptop drives.
- NetTerm and a VPN setup on all laptops.
- Finance/Accounting can maintain phone contact, wire services for fuel payments, fax and Internet connection to Bank of America
- Amerijet switchboard phone number delivers an message with the alternative contact numbers for Customer Service

3.0 Recovery Strategy

The Recovery Strategy developed is based upon the results of the Business Impact Analysis, including the Critical Time Frames and available alternative manual procedures in the event of an extended computer outage. The Recovery Strategy will be discussed in three sections as follows:

- Approach
- Escalation Plans
- Decision Points

3.1 Approach

The Critical Time Frame is the basis for selecting an external data center site to prevent a worst case scenario. Information Technology recommended the UUnet building in Miami and obtained a “cage” at that facility, totally devoted to Amerijet equipment and operations. This external site provides immediate access to critical servers and technical facilities to assist in the recovery process. There are no key contacts at UUNet. Whoever is on duty can assist. The UUnet site is located at:

Address: 1525 NW 98 Ct
Doral, FL 33172
Phone: 1-800-900-0241 Option 4

The decision to utilize alternative means for data entry into the UUNet-based network is dependent upon two factors: 1) the length of the anticipated outage and 2) the business cycle Amerijet International is in at the time of the outage. Therefore, based upon these two factors, three escalation plans have been devised to drive the recovery process.

3.2 Escalation Plans

Since not all interruptions are expected to be worst case, a concise method of communicating the estimated outage time frame is established. The principal reason for these plans is based on an understanding with some users that interim procedures can be used while the system is out-of-service. The user needs to know as soon as possible what the estimated outage period is so that interim procedures can be implemented if necessary.

The escalation plans below have been developed based on the time frames depicted on the Business Impact Analysis matrix.

Plan 1: 1-3 days estimated outage - recovery will proceed at Amerijet International offices.

Plan 2: 4 -7 days outage - recovery location for each department will vary depending on business cycle interruption point. The Senior Recovery Manager will determine recovery site based upon damage assessment and current business cycle.

Plan 3: 8 days or longer estimated outage - recovery will commence at alternative sites.

Emergency notification procedures are contained in section 5.0 of this plan. When these procedures are activated, escalation plan 1, 2 or 3 is used to notify the company as a whole.

3.3 Decision Points

PLAN 1

Where the damage assessment indicates recovery is possible in 72 hours or less, the Management Team shall coordinate the recovery of the Amerijet International employee computers, telephones, and domain controller access on location.

Air Cargo data entry disruption depends on whether airplanes can leave or arrive at Miami Air Port..

ADP will accept a verbal release of the payroll in the event of a disaster. The password used for the electronic connection with ADP will serve as verification on a verbal request. Therefore, for purposes of this Disaster Recovery Plan, payroll processing will be treated external and independent from the LAN.

PLAN 2

Where the damage assessment indicates recovery is possible within 4 to 7 business days, the Management Team shall coordinate with Amerijet International department and division heads on the decision as to the recovery locations.

During this outage time period, minimal financial and operational impact to the operating divisions within Amerijet International is anticipated. However, access to the Accounting System Server may require recovery within 5 business days, depending upon the existing business cycle at the time of the outage. An ambitious recovery of a limited LAN environment containing 5 workstations, fax machine, and printers for the Finance and Accounting department at an alternative site is estimated to take 1 business day. Depending upon the business cycle, extent of damage to the existing LAN, equipment, network and communications availability; recovery within seven business days using VPN to the existing data center may prove to be the optimal solution.

PLAN 3

Where the damage assessment indicates recovery will take a minimum of eight or more business days at the present data center, the Management Team shall place the Recovery Team in full mobilization in executing a move to alternative data-entry locations to establish a temporary office with slower, but available contact with the UUNet data center.

During an outage of greater than 7 days, several Amerijet International operating departments will experience a significant loss in operational control, potential loss of revenue, and/or an increase in expenditures.

If an alternative data entry points are selected, the recovery strategy is to take laptops, printers, and fax machines to provide access to UUNet. This is a temporary short term solution to provide immediate access to the accounting systems and Bank of America during the recovery of the system.

An alternative access point is also needed for MIA Warehouse. The Load & Balance Team will relocate to near the airplanes if the fleet changes airports. Load & Balance needs fax machine, cell phones, and laptops. The warehouse already has a laptop set up for continued data entry.

Business Impact Analysis indicates that in most of the operational departments interviewed, one workstation/laptop would allow sufficient access on the LAN environment to continue operations with minimum inconvenience for at least one month. If the outage is anticipated to extend beyond one month, additional workstations attached to the LAN would be required.

In Information Technology, all employees routinely use laptops or home computers attached to the LAN. All software and database development would be discontinued. Production control would continue through local terminals installed in the UUNet cage.

4.0 Disaster Recovery Organization

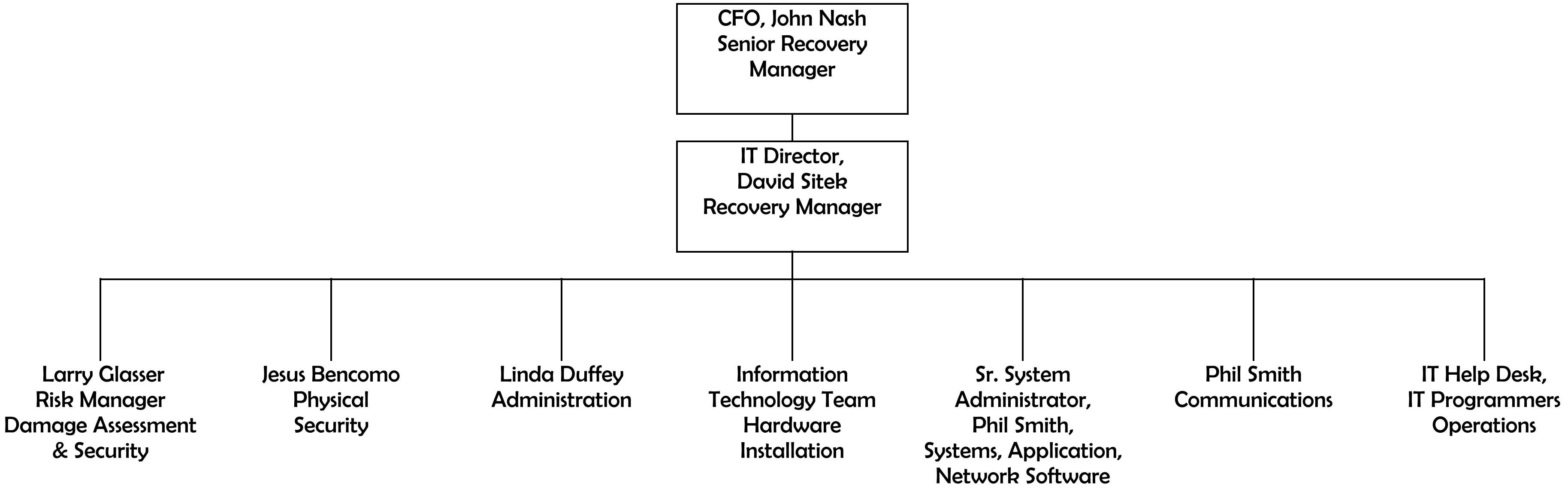
The effectiveness and operability of the Disaster Recovery Plan is dependent on the knowledge and expertise of the personnel who develop and execute the plan. It is essential to determine which talents are required and to assign personnel who meet those requirements.

A recovery from a disaster is best conducted by teams of personnel that are formed to perform specific functions (e.g., hardware acquisition, hardware installation, operations). The number and types of teams are dictated by the size and type of computer processing capabilities the plan is being developed to recover.

The Disaster Recovery Organization, therefore, is set up to accomplish:

- Expeditious and efficient recovery of computer processing.
- Intermediate and minor impact/expenditure decisions within the Information Technology personnel during the recovery process.
- Major impact/expenditure decisions at the management level.
- Streamline reporting of recovery progress from recovery teams upward to senior management and end-users.

4.1 Recovery Organization Chart



4.2 Disaster Recovery Team

Recovery Senior Manager:	John Nash
Alternate:	Robert Kaltenbach
Recovery Manager:	David Sitek
Alternate:	Phil Smith
Damage Assessment and Security:	Larry Glasser
Alternate	Cecil Hicks
Physical Security:	Jesus Bencomo
Alternate:	Jimmy Shields
Administration:	Linda Duffey
Alternate:	Christine Richard
Hardware Installation:	IT Help Desk
Systems, Applications & Network Software:	Phil Smith
Alternate:	Patrick Lawrence
Communications:	Phil Smith
Alternate	Patrick Lawrence
Operations:	Information Technology Team

4.3 Recovery Team Responsibilities

4.3.1 Recovery Management

The Recovery Management is responsible for managing the recovery effort as a whole, ensuring restoration occurs within planned Critical Time Frames and assists in resolving problems requiring management action. The Recovery Management Team consists of the Senior Recovery Manager and the Recovery Manager. The team is activated at the call of the Senior Recovery Manager when a disaster occurs. All other recovery teams report directly to the Recovery Management Team. Specifically, the Recovery Management Team is charged with:

Senior Recovery Manager Responsibilities

Pre-Disaster

Approve the final Disaster Recovery Plan
Ensure the Disaster Recovery Plan is maintained
Ensure Disaster Recovery Training is conducted
Authorize periodic Disaster Recovery Plan testing

Post-Disaster

Declaration of a Disaster
Determine the Plan strategy to be implemented (i.e.: Plan 1, 2 or 3)
Determine alternate team members and other support members of the recovery process
Authorize travel and housing arrangements for Team Members
Authorize expenditures in excess of $5,000
Manage and monitor the overall recovery process
Advise Senior Amerijet International and user management on the status of the disaster recovery efforts
Coordinate media and press releases

Recovery Manager Responsibilities

Pre-Disaster

Maintain and update the Plan as scheduled
Distribute Disaster Recovery Plan to Recovery Team Members
Appoint Recovery Team members and alternates as required
Coordinate the testing of the Plan
Train Disaster Recovery Team members in regard to the Plan

Post-Disaster

Assist in assessing extent of damage to Amerijet International Facilities and ability to provide data processing service to the organization
Initial notification of disaster declaration to Recovery Team
Coordinate all Recovery Teams
Notify alternative sites (hotels) and Laptop users of pending activation
Notify Systems, Application & Network Software Team to request off-site system backups, manuals, equipment and documentation
Notify Administration Team to make necessary travel or hotel accommodations for designated Recovery Team members
Authorize purchases and required disbursements
Reports to Senior Recovery Manager status of recovery effort

4.3.2 Damage Assessment and Salvage Team

Responsible for the damage assessment of the LAN and LAN facilities as quickly as possible following a disaster and reports the level of damage to the Disaster Management Team. Oversees salvage operations required to cleanup and repair the LAN data center. Reestablishes the LAN data center in the reconstituted site or a new site. Specifically, the Damage Assessment and Salvage Team is responsible for:

Damage Assessment and Salvage Team Responsibilities

Pre-Disaster

Understand role and responsibilities within the Disaster Recovery Plan
Work closely with Recovery Management Team to reduce possibility for disaster in the data center (See Preventative Measures in Appendix)
Train employees in emergency preparedness
Participate in Disaster Recovery Plan tests as required

Post-Disaster

Determine accessibility to building and Amerijet International's offices
Assess extent of damage to Amerijet International's LAN and data center
Assess need for physical security, such as security guards
Estimate time to recover based upon damage assessment
Identify salvageable hardware and communication equipment
Apprise the Management Team on the extent of damages, estimated recovery time, physical security required, and salvageable equipment
Maintain log of salvageable hardware and equipment
Coordinate with vendors and suppliers in restoring, repairing or replacing salvageable hardware and equipment.
Provide support in the cleanup of the data center following the disaster

4.3.3 Physical Security

The Physical Security Team provides personnel identification and access limitations to the building and floors and acts as liaison with emergency personnel. This is crucial during the time of a disaster because of the uncommonly large number of vendors, contractors and other visitors requiring access to the offices.

Pre-Disaster

Understand role and responsibilities within the Disaster Recovery Plan
Work closely with Recovery Management Team to ensure physical security of existing system, LAN and facilities

Train employees in emergency preparedness
Become familiar with emergency phone numbers
Participate in Disaster Recovery Plan tests as required

<u>Post-Disaster</u>

Cordon off data center to restrict unauthorized access
Coordinate with Building Management for authorized personnel access
Provide security guards as required
Act as liaison with emergency personnel, such as fire and police departments.
Schedule security for transportation of files, reports and equipment
Provide assistance in any official or insurance investigation of the damaged site

4.3.4 Administration

The Disaster Recovery Administration team is responsible for providing secretarial, filing, procurement, travel and housing, off-site storage and other administrative matters not performed by other team members. Included is limited authority to provide funds for emergency expenditures other than for capital equipment and salaries.

Pre-Disaster

Understand role and responsibilities within the Disaster Recovery Plan
Train employees in emergency preparedness
Ensure sufficient comprehensive and business interruption insurance is maintained.
Ensure sufficient emergency funds will be available during recovery process
Assess need for alternative means of communication if telephones service is unavailable
Participate in Disaster Recovery Plan tests as required

Post-Disaster

Prepare, coordinate and obtain appropriate approval for all procurement request
Coordinate deliveries of all procurement requests
Process requests for payment of all invoices relating to recovery process
Arrange for travel and lodging as required by Recovery Team
Provide for acquisition of telephone equipment and services, including voice, dial-up data and leased lines.
Provide for alternative means of communication among Recovery Team in the event regular telephone service is unavailable.
Arrange for temporary secretarial, filing, and other administrative services required by the Recovery Team.

4.3.5 Hardware Installation

The Hardware Team is responsible for site preparation, physical planning, and installation of data processing equipment to meet the required processing capacity of Amerijet International in the event of a disaster. This includes responsibility for ordering and installing software on laptops and preparing the UUNet permanent site.

Pre-Disaster

Understand role and responsibilities within the Disaster Recovery Plan
Work closely with Recovery Management Team to reduce possibility for disaster in data center
Train employees in emergency preparedness
Participate in Disaster Recovery Plan tests as required
Maintain current system and LAN configuration in off-site storage

Post-Disaster

Verify with alternative sites, such as hotels, the pending occupancy requirements
Interface with Software, Communications and Operations Team members on space configuration
In the event of damage to office computers, coordinate transportation of salvageable equipment to an alternative site for evaluation and restoration
Notify Administration Team of equipment required
Ensure installation of VPN and NetTerm on all laptops that will function as temporary terminals connected to UUNet

4.3.6 Systems, Applications and Network Software

The Systems, Applications and Network Software Team is responsible for the installation and configuration of all systems, application and network software on the LAN.

Pre-Disaster

Understand role and responsibilities within the Disaster Recovery Plan
Work closely with Recovery Management Team to ensure physical security of existing LAN and facilities
Train employees in emergency preparedness
Participate in Disaster Recovery Plan tests as required

Post-Disaster

Arrange for delivery of off-site storage containers
Receive delivery of off-site storage containers
Restore operating system, applications and network software from backup medium
Test and verify operating system, applications and network software
Modify LAN configuration to meet alternative site configuration
Return backup medium in storage containers to off-site storage

4.3.7 Communications

The Communications Team is responsible for establishing data links to UUNet and telephones for voice communication with suppliers, banks, and customers. This includes connecting local and remote users to the UUNet.

Pre-Disaster

Understand role and responsibilities within the Disaster Recovery Plan
Work closely with Recovery Management Team to ensure physical security of existing system, LAN and facilities
Train employees in emergency preparedness
Participate in Disaster Recovery Plan tests as required
Maintain current communication configuration in off-site storage

Post-Disaster

Coordinate with Damage Assessment and Salvage Team on assessment of communications equipment
Retrieves communications configuration from off-site storage
Plans, coordinates and installs communication equipment at alternative sites
Plans, coordinates and installs network cabling at alternative sites, if required

4.3.8 Operations

The Operations Team is responsible for operating the production systems at the external data center and for assisting the other recovery teams in establishing operations from laptops at alternative sites.

Pre-Disaster

Understand role and responsibilities within the Disaster Recovery Plan
Work closely with Recovery Management Team to ensure physical security of existing system, LAN and facilities
Train employees in emergency preparedness
Ensure backups are completed as scheduled
Ensure backups are sent to off-site storage as scheduled
Participate in Disaster Recovery Plan tests as required

Post-Disaster

Assist Hardware, Software and Communications Teams as required
Initialize new tapes as needed in the recovery process
Conduct the backups at the off-site location
Ensure backup tapes are kept off-site for storage
Set up and operate a sign-in, sign-out procedure for all materials sent to and from the UUNet site
Check floor configuration of alternative site after disaster too assist Hardware, Software and Communications Teams in planning installation (completed in 2004)
Monitor security of the LAN network
Coordinates transfer of equipment, furniture and personnel, as necessary to alternative sites.

5.0 Disaster Recovery Emergency Procedures

The primary purpose of a Disaster Recovery Plan is to establish written emergency procedures which the Recovery Team can follow to expedite the recovery process. The procedures are in a structured step by step format. This format, during conditions of a disaster results in minimal confusion thereby expediting the recovery process. These procedures are dynamic in that as business requirements and environments change so will the emergency procedures. It is imperative each Team Member fully understands his/her role and responsibilities during a disaster and that the emergency procedures are tested on a recurring basis (see Plan Administration).

The emergency procedures have been structured to provide the individual recovery steps required and serve as a log of the recovery process. Following each step is a place to initial and indicate the date and time the step was completed.

The objectives of the emergency procedures are to:

- Minimize injury to personnel
- Minimize damage to equipment and facilities
- Achieve a report of injury to personnel and damage assessment within four hours of the interruption
- Recover the system and LAN capabilities and functionality within the Critical Time Frames specified earlier.

As the first objective indicates, the safety of every Amerijet International employee in the event of an emergency is of top priority. In an emergency situation where your life is threatened or you are in danger of physical harm, immediately leave the facility. Never place yourself in a dangerous situation or take unnecessary risks.

The emergency procedures to be discussed are follows:

- General
- Recovery Management
- Damage Assessment and Salvage
- Physical Security
- Administration
- Hardware Installation
- Systems, Applications, Network Software
- Communications
- Operations

5.1 General

Mission: To report a potential or actual disaster so appropriate action can be taken to minimize injury to Amerijet International personnel and damage to facilities and equipment.

IN A LIFE THREATENING SITUATION
STOP HERE
IMMEDIATELY LEAVE THE FACILITY

1) To report an emergency situation dial 8 (HQ) 9 (MIA) to obtain an outside line and then 911. Report the type of emergency and your name and office address.

   Amerijet International office addresses are shown in the appendix page 58.

Initials: __________ Date: __________ Time: __________

2) Immediately notify Risk Managemer, Larry Glasser, 954-648-3206 or Security Manager Jesus Bencomo, 786-201-4330 as to the type of emergency. If you cannot reach these persons, immediately notify your superior.

Initials: __________ Date: __________ Time: __________

3) Notify the Recovery Management Team of the potential or actual disaster. The Recovery Management Team may be reached at the phone numbers listed in the appendix.

Initials: __________ Date: __________ Time: __________

4) Evacuate the building as instructed by emergency personnel or as established by the building management.

Initials: __________ Date: __________ Time: __________

5.2 Recovery Management

Mission: To decide escalation plan to be implemented, oversee and coordinate the entire disaster recovery operation, notify user of estimated time of outage and assist in resolving problems requiring management action.

1) Upon notification of a potential or actual disaster, immediately notify the remaining Management Team members and the Damage Assessment and Salvage Team to conduct a survey and damage assessment of the data center facilities.

Initials: __________ Date: __________ Time: __________

2) Make an outage assessment based upon the verbal report from the Damage Assessment and Salvage Team.

Initials: __________ Date: __________ Time: __________

3) Senior Recovery Manager determines where the recovery will be conducted; at the Amerijet International office or alternative sites .

Initials: __________ Date: __________ Time: __________

4) Gain approval for activation of the necessary Recovery Teams and alternative sites, if required.

Initials: __________ Date: __________ Time: __________

5) Notify other Recovery Team members of the disaster and request they assemble at a designated location for a briefing on the damage assessment and selected escalation plan. The designated location will either be the Amerijet International offices or an external facility, depending upon the severity of the disaster.

Initials: __________ Date: __________ Time: __________

6) Notify Amerijet International department and division heads on the severity of the disaster and the estimated recovery time.

Initials: __________ Date: __________ Time: __________

7) Conduct a briefing with all Recovery team members to apprise of the severity of disaster and determine:

- ▫ Travel and hotel arrangements
- ▫ Equipment acquisitions
- ▫ Equipment repairs

Initials: __________ Date: __________ Time: __________

8) Monitor the Recovery Teams that are functioning at alternative sites to resume operations.

Initials: __________ Date: __________ Time: __________

9) Assist the Recovery Teams as needed with procurement or any other problems which may require management involvement.

Initials: __________ Date: __________ Time: __________

10) The Recovery Manager, reporting to the Senior Recovery Manager provides the coordination and assistance to the Recovery Teams in performing their recovery functions.

Initials: __________ Date: __________ Time: __________

11) Coordinate and issue any media press releases regarding the disaster as it relates to Amerijet International.

Initials: __________ Date: __________ Time: __________

5.3 Damage Assessment and Salvage

Mission: To assess the damage to the systems and data center within four hours, notify the Management Team of assessment, and coordinate salvage of equipment where possible.

1) Assess the requirement for physical security to minimize possible injury to persons entering the facility and eliminate the potential for vandalism to Amerijet International assets.

Initials: __________ Date: __________ Time: __________

2) Utilizing the following checklist as a guideline, survey the systems and data center facilities to assess damage upon notification from the Management Team of the need for damage assessment.

I. Building
   A. Exterior
   B. Interior
      1. Walls
      2. Ceiling
      3. Floor
II. Environmental/Control
   A. Electrical
      1. UPS
      2. Transformers
      3. Emergency/Building
   B. HVAC
      1. Air Handling
      2. Air Conditioning
      3. Water
   C. Fire Suppression
      1. HALON
      2. CO 2
      3. Water
III. Computer Room Contents
   A. Equipment
      1. Servers
      2. Communications Modems
      3. Network Cabling
      4. Stand-alone workstations (Voice Mail)
   B. Other
      1. Spare Parts

2. Documentation (Vault)

IV. Amerijet International Office Contents

A. Workstations
B. Essential Periferals
C. Network Jacks and Cables
D. Electrical Outlets
E. UPS units

The purpose of the above checklist is to provide a guide in the review and assessment of damage following a disaster to Amerijet International facilities, the network and/or the data center facilities in HQ, MIA, CC. In using the checklist, the Damage Assessment and Salvage Team must consider:

- □ Is the area safe for employees or vendors to work in?
- □ Can the equipment under examination function, and if so, at what percent of normal capacity?
- □ What must be done to recover damaged equipment so that the LAN will be functional?
- □ How long will it take to repair or replace the damaged equipment so that the LAN will be functional?

Initials: __________ Date: __________ Time: __________

3) Based upon damage assessment, determine the estimated time to recover based upon to following guidelines.

Level I Minimal damage to facility and/or equipment. Estimated time to complete repairs is less than 72 hours.

Level II Moderate damage to facility and/or equipment. Estimated time to complete repairs is between 72 hours and 7 business days.

Level III Extensive damage to facility and/or equipment. Estimate time to complete repairs is greater than 7 business days.

Initials: __________ Date: __________ Time: __________

4) Identify equipment, documentation, or spare parts which are immediately salvageable or in need of repair.

Initials: __________ Date: __________ Time: __________

5) Verbally notify the Management Team of survey, assessment of damage, estimated time to recover from damage and potentially salvageable equipment.

Initials: __________ Date: __________ Time: __________

6) Document findings from the survey and damage assessment.

Initials: __________ Date: __________ Time: __________

7) Attend the recovery briefing as scheduled by the Senior Recovery Manager to apprise Recovery Team members of findings.

Initials: __________ Date: __________ Time: __________

8) If the Senior Recovery Manager decides recovery will take place at an external site, following insurance company and management approval, salvageable equipment is removed and prepared for transportation to an alternative site where is can be repaired.

Initials: __________ Date: __________ Time: __________

9) A log is prepared and maintained to record all salvageable equipment and is disposition and location.

Initials: __________ Date: __________ Time: __________

10) Coordinate with the Administrative Team, vendors and suppliers in restoring or replacing salvageable equipment.

Initials: __________ Date: __________ Time: __________

11) Assist in the cleanup of the disaster area in regard to the computer facilities to permit eventual renovation and/or reconstruction.

Initials: __________ Date: __________ Time: __________

Under no circumstances should the Damage Assessment and Salvage Team make any public statements regarding the disaster, its cause or its effect on the operation at Amerijet International.

5.4 Physical Security

Mission: To ensure the physical security of the disaster site, the external data center site, files, reports, and equipment while in transit and act as liaison with emergency personnel.

1) Upon notification of a disaster by the Management Team assemble at the designated site for a briefing on the extent of damages, escalation plan implemented and support required.

Initials: __________ Date: __________ Time: __________

2) Establish physical security at the Amerijet International facilities to restrict access to the damaged area to those individuals whose functions require their being in the immediate area, such as the Damage Assessment and Salvage Team, insurance company investigators, Amerijet International vendors, and building engineers.

   Considerations in the level of security required are:

   - Is entry into the damaged area safe?
   - Is the damage exclusively to the Amerijet International offices?
   - Is there damage to the entire building or has access to the building been restricted by emergency personnel or building management personnel?
   - Are guards required to restrict access to ensure personnel safety or to eliminate possible vandalism or theft of Amerijet International property?

Initials: __________ Date: __________ Time: __________

3) Depending upon the extent of the damage to the physical building, coordinate with emergency personnel and building management access to the various buildings by the Damage Assessment and Salvage Team, insurance company investigators and Amerijet International vendors.

   The Building Facilities contacts are:

   Cecil Hicks for HQ, 954-608-8810

Lou Montella for MIA and CC, 917-613-4078
Frank of Integrated Security, 305-302-9789 for FLL
Fadi Aftimos for ITN, 305-216-7787
For JFK, IAH, POS, contact the Station Manager for that site.
Cell phone numbers are available on the Intranet.

Initials: __________ Date: __________ Time: __________

4) Schedule security for all files, reports, and equipment in transit as requested by the Management Team.

Initials: __________ Date: __________ Time: __________

5) Assist in anyway possible the authorized investigation of the damaged site.

Initials: __________ Date: __________ Time: __________

Under no circumstances should the Physical Security Team make any public statements regarding the disaster, its cause or its effect on the operations at Amerijet International.

5.5 Administration

Mission: To provide administrative support to all Disaster Recovery Teams, including procurement of equipment and supplies, travel and housing arrangements, and other administrative functions not provided by other team members.

1) Upon notification of a disaster by the Management Team assemble at the designated site for a briefing on the extent of damages, escalation plan implemented and support required.

Initials: __________ Date: __________ Time: __________

2) Coordinate, prepare and submit for authorization to the Management Team procurement requests for equipment, supplies and services required to support the recovery process as requested by the Recovery Team members.

Initials: __________ Date: __________ Time: __________

3) Maintain log of all procurements in process and scheduled delivery dates. Notify Recovery Team members of scheduled delivery dates and coordinate with vendors to ensure deliveries or service requests are completed as required.

Initials: __________ Date: __________ Time: __________

4) Arrange for travel and lodging required by Recovery Team members or other Amerijet International personnel as directed by the Senior Recovery Manager.

Initials: __________ Date: __________ Time: __________

5) Complete the acquisition mobile telephones as required by the Recovery Team members.

Initials: __________ Date: __________ Time: __________

Under no circumstances should the Administration Team make any public statements regarding the disaster, its cause or its effect on the operations at Amerijet International.

5.6 Hardware Installation

Mission: To plan, design, schedule, install, and verify computing hardware required to provide computer capabilities within the time frame specified. Coordinates with the vendors in support of the equipment.

NOTE: All hardware was installed at UUNet prior to the 2004 hurricane season. Information Technology maintains, adds to, and configures equipment at UUNet on an ongoing basis.

1) Coordinate with the Administration Team in the procurement of any additional equipment required in the recovery process.

Initials: __________ Date: __________ Time: __________

2) Coordinate with the UUNet for installation and connection of 2-5 temporary terminals to provide additional access to the LAN servers for Amerijet International I.T. employees.

Initials: __________ Date: __________ Time: __________

3) Coordinate with Finance and Flight Operations if the airline is moved to an alternative airport and put into Charter Service.

Initials: __________ Date: __________ Time: __________

Under no circumstances should the Hardware Installation Team make any public statements regarding the disaster, its cause or its effect on the operations at Amerijet International.

5.7 Systems, Applications & Network Software

Mission: To obtain off-site tape backups, restore and test the operating systems, applications and network software needed to provide the capabilities required within the Critical Time Frames specified.

1) Upon notification of a disaster by the Management Team assemble at the designated site for a briefing on the extent of damages, escalation plan implemented and support required.

Initials: __________ Date: __________ Time: __________

2) Receive delivery of additional backup tapes, and documentation moved to the recovery site.

Initials: __________ Date: __________ Time: __________

3) On domain controllers and those servers housed outside of UUNet, restore the operating system, applications, network software and production data from the backup tapes.

Initials: __________ Date: __________ Time: __________

5) Test and verify that the restore completed successfully.

Initials: __________ Date: __________ Time: __________

6) If necessary, modify configuration of operating and network software to meet configuration.

Initials: __________ Date: __________ Time: __________

Under no circumstances should the Systems, Applications & Network Software Team make any public statements regarding the disaster, its cause or its effect on the operations at Amerijet International.

5.8 Communications

Mission: To design, install and verify the communications equipment and network cabling.

1) Upon notification of a disaster by the Management Team assemble at the designated site for a briefing on the extent of damages, escalation plan implemented and support required.

Initials: __________ Date: __________ Time: __________

2) Review the Hardware/Software Inventory list found in the appendix to determine the communications and network equipment required.

Initials: __________ Date: __________ Time: __________

3) The Communications Team coordinates with the Damage Assessment and Salvage Team on equipment to obtain an inventory of usable and salvageable communications equipment.

Initials: __________ Date: __________ Time: __________

4) Coordinate with the Administration Team in procuring communications equipment and telephone lines required in the recovery process.

Initials: __________ Date: __________ Time: __________

5) Coordinate with the Administration Team in procuring the necessary network cabling and cabling installation required in the recovery process.

Initials: __________ Date: __________ Time: __________

Under no circumstances should the Communications Team make any public statements regarding the disaster, its cause or its effect on the operations at Amerijet International.

5.9 Operations

Mission: To provide operating support for the production systems at the backup data center and assist the other recovery teams in establishing operations at the backup site.

1) Upon notification of a disaster by the Management Team assemble at the designated site for a briefing on the extent of damages, escalation plan implemented and support required.

Initials: __________ Date: __________ Time: __________

2) Complete daily backups of entire LINUX, email, SQL Server systems, and user directories; ensure tapes are sent off-site daily.

Initials: __________ Date: __________ Time: __________

3) Set-up and operate a sign-in, sign-out procedure for all materials sent to and from the UUNet site.

Initials: __________ Date: __________ Time: __________

4) Monitor security of the UUNet site and the network.

Initials: __________ Date: __________ Time: __________

5) Provide production support to users as required.

Initials: __________ Date: __________ Time: __________

Under no circumstances should the Operations Team make any public statements regarding the disaster, its cause or its effect on the operations at Amerijet International.

6.0 Plan Administration

This Disaster Recovery Plan is a living document. Administration procedures are for the purpose of maintaining the Disaster Recovery Plan in a consistent state of readiness. The procedures specify direct Information Technology administrative responsibilities and coordination responsibilities with users of the data center.

These procedures apply to the continued maintenance, testing and training requirements of the Disaster Recovery Plan.

They apply to Information Technology management and user management as a whole to promote awareness of the Disaster Recovery Plan and the need for disaster recovery preparedness. The procedures also apply to specific functional areas within Information Technology that have direct responsibility for maintaining the plan in a current and accurate state.

The coordination of the Disaster Recovery Plan is the responsibility of the Disaster Recovery Manager.

6.1 Disaster Recovery Manager

The function of the Disaster Recovery Manager is key to maintaining the plan in a consistent state of readiness. The Recovery Manager's role is multifaceted. Not only does the Recovery Manager assume a lead position in the ongoing maintenance of the plan, but is a member of the Recovery Management Team in the event of a computer disaster. The areas in which the Manager assumes a lead position and conducts reviews of effectiveness in the plan administration are as follows:

- Distribution of the Disaster Recovery Plan
- Maintenance of the Business Impact Analysis
- Training of the Disaster Recovery Team
- Testing of the Disaster Recovery Plan
- Evaluation of the Disaster Recovery Plan Tests
- Review, change and update of the Disaster Recovery Plan

6.2 Distribution of the Disaster Recovery Plan

The Recovery Manager is responsible for the authorized distribution of the plan and the location of each plan copy. As this document is confidential, the authorized distribution list is developed on a need-to-know basis. The distribution list is approved by the Director of Information Technology. The original and all copies of the Disaster Recovery Plan should be maintained in a secure location.

The concept of disaster planning is to minimize the likelihood of a disaster ever occurring and further, to minimize injury to personnel and damage to equipment and facilities if a disaster does occur. The Plan reveals in great detail the essence of Amerijet International's recovery strategy, personnel, addresses, locations and inventories which should not be for general publication to non-participating employees or outsiders.

The Recovery Manager must maintain a log to track the number of copies produced and/or distributed and their location. The master printout and electronic file containing the Disaster Recovery Plan must be kept in a secure place to avoid unauthorized duplication or misuse.

The distribution transmittal cover page should contain instructions regarding the proper handling and safekeeping of issued plan copies and the requirement for its return upon removal as a Recovery Team member. Recovery Team members will be assigned one copy of the Disaster Recovery Plan. Each Recovery Team member must be informed and signify their recognition of the confidential nature of the plan and maintain their copy in a secure location off-site, primarily in their principal place of residence. This will allow access to the plan by each Team member in the event access to the Amerijet International office is deemed unsafe or not permitted as a result of a disaster.

In addition to the Recovery Team members, one copy of the plan is maintained in the I.T. library (vault) as well as one copy at UUNet. Additional copies of the Disaster Recovery Plan will be assigned to personnel on an as-required basis and as approved by the Director of Informaton Technology.

6.3 Maintenance of the Business Impact Analysis

As Amerijet International's business and systems environment changes, so does the dependency on the computer systems used to support the business. Therefore, no less than every two years, the I.T. Publications Writer conducts a Business Impact (Risk) Analysis to update the Priority List and Critical Time Frames for the systems recovery process. This analysis will provide insight as to required plan modifications and whether a change in the overall recovery strategy is warranted.

6.4 Training of the Disaster Recovery Team

The Recovery Manager is responsible for the coordination of training relating to the Disaster Recovery Plan. The purpose of disaster recovery training is twofold:

- To train Recovery Team participants who are required to execute plan segments in the event of a disaster.
- To train Amerijet International management and key employees in disaster prevention and awareness and the need for disaster recovery planning.

Initially, upon the acceptance of the Disaster Recovery Plan, training of Amerijet International management in disaster recovery planning benefits and objectives is crucial. A Disaster Recovery Plan must have the continued support from Amerijet International's key user management to ensure future effective participation in plan testing and updating. As discussed later, it is not solely the responsibility of the Recovery Manager to initiate updates to the Disaster Recovery Plan. User management must be aware of the basic recovery strategy; how the plan provides for rapid recovery of their information systems support structure; and how the plans effectiveness may be compromised without notification to the Recovery Manager as their business operations evolve and expand significantly.

It is the responsibility of each Recovery Team participant to fully read and comprehend the entire plan, with specific emphasis on their role and responsibilities as part of the Recovery Team. On-going training of the Recovery Team participants will continue through plan tests and review of the plan contents and updates provided by the Recovery Manager.

6.5 Testing of the Disaster Recovery Plan

The Recovery Manager is responsible for testing of the Disaster Recovery Plan not less than once every year to ensure the viability of the plan and recovery of computing capabilities will be within the Critical Time Frames established by the Business Impact Analysis. On an on-going basis this frequency appears to be adequate considering the systems involved. However, special tests are to be given consideration whenever there has been a major revision to the plan or significant changes in the software, hardware or data communications have occurred.

The objectives of testing the Disaster Recovery Plan are as follows:

- To determine the effectiveness of the Plan procedures.
- To determine the state of readiness and ability of designated Recovery Team personnel to perform their assigned recovery responsibilities.
- To determine if sufficient recovery inventories are stored off-site to support the recovery process.
- To determine if the disaster recovery plan requires modifications or updates to ensure recovery within the Critical Time Frames established and accepted buy the users.

Plan testing is normally accomplished when there is less demand for information technology service to end-users since IT personnel and time will be committed to the test process. Costs to conduct such tests and availability of personnel are prime considerations in determining the scope and timing of the test(s). The initial test of the plan will be in the form of a structured walk-through and should occur within two months of the Disaster Recovery Plan's acceptance. Subsequent tests should be to the extent determined by the Recovery Manager that are cost effective and meet the benefits and objectives desired.

Test scenarios and frequency of tests for the Disaster Recovery Plan depend upon sufficient rationale concerning the benefits expected from the test and the specific objectives to be accomplished. Wide latitude is employed in developing test scenarios. Some considerations in development of the test scenario employed and test frequency are:

- Significant modifications to the recovery strategy or emergency procedures.
- Inclusion of Recovery Teams requiring more involvement to sustain familiarity with their respective functions.
- Different severity damage levels to files, documents, materials, and equipment required in support of the recovery process.
- Critical applications that are new or have not been previously tested.
- Re-testing plan segments which were determined to be deficient in past tests.
- Additions or changes to Recovery Team personnel.

Planning for the test is a two to six week process depending on the complexity of the tests employed and the number of individuals involved. However, without sufficient planning, achievable benefits and objectives from the testing process may never materialize. The steps in planning for the Disaster Recovery Test in checklist format are:

- Determine Objectives of the Test
- Determine Scope of the Test
- Determine Personnel Resource Requirements
- Establish Test Date and Duration
- Determine Anticipated Test Costs
- Schedule Test With Participants
- Schedule Test with VPN only access to servers at UUNet. (Bypass domain controllers)
- Develop Detailed Test Work Plan
- Ensure Recovery Material and Equipment Availability
- Notify Users of Test
- Review Work Plan with Participants

6.6 Evaluation of the Disaster Recovery Plan Tests

The Recovery Manager is responsible for coordinating the review and analysis of the test results and updating the plan accordingly. A Test Coordination Team is appointed and headed by the Recovery Manager for each test conducted. This team is charged with the following responsibilities:

- To be familiar with the entire plan.
- To understand thoroughly the objectives of the tests to be conducted.
- To organize itself to be able to monitor and observe all the activities of the Recovery Teams involved in the test.
- To inspect and review the results of the test from the point of view of the Information Technology personnel and the users.
- To document their findings related to the strengths and weaknesses observed during the test.

The Recovery and Test Coordination Teams document the test results immediately after the plan test. The Recovery Manager reviews the test results with the Recovery and Test Coordination Team during at postmortem meeting to discuss weaknesses and resolve problem areas. The Recovery Manager chairs the meeting and makes changes and updates to the plan accordingly.

6.7 Maintenance of the Disaster Recovery Plan

The Recovery Manager is responsible for ensuring that the plan is maintained current and in a state of readiness. The purpose of a plan review is to determine whether updates to the plan or additional training of Recovery Team personnel is required based on the occurrence of an event or action affecting the plan.

Two primary responsibilities of the Recovery Manager will drive revisions to the Disaster Recovery Plan; 1) updates to the Business Impact Analysis and 2) testing of the Disaster Recovery Plan. However, it is also the responsibility of all Amerijet International management to initiate a plan review when an event or action affecting the plan has occurred.

The following paragraphs incorporate checklists for Amerijet International management which could prompt a review and subsequent update of the plan:

Information Technology Checklist

- □ Change in LAN server(s), terminals, or personal computer workstations.
- □ Change in operating system and utility software programs.
- □ Change in the design of production systems or files.
- □ Addition of deletion of a production system.
- □ Change in the scheme of backing up data or equipment.
- □ Change in the communications network design.
- □ Change in personnel assignments or the Information Technology organization.
- □ Change in off-site storage facilities, location or methods of cycling items.
- □ Improvements or physical change to the current LAN data center.
- □ Review of time frames for availability and delivery of replacement computer components.

Corporate Checklist

- □ Has a new division or department been formed?
- □ Has a new system been developed for computer processing?
- □ Has a system for computer processing been discontinued?
- □ Have individuals within the Recovery Team been transferred, promoted or terminated?
- □ Has an internal system been significantly modified to change the basic functions, data flow requirements or accounting requirements?
- □ Has a sales office been opened, moved or closed?
- □ Are there any user computer equipment inventory changes?

7.0 Appendix

Amerijet International Domestic Stations

HEADQUARTERS
Mailing Address: 2800 S. Andrews Avenue
Fort Lauderdale, FL 33316
Phone: 954-320-5300 - Reception
954-320-5301 - Automated Attendant
800-786-6944 (Office & Voicemail)

ATLANTA
Address: 5192 South Ridge Parkway, Suite 100
College Park, GA 30349
Direct Dial: 5044
Phone: 770-909-4450

CHICAGO
Address: 860 Foster Avenue, Unit D
Bensenville, Il 60106
Phone: 630-860-3595

HOUSTON
Address:
15415 International Plaza Dr. Suite 180
Houston, TX 77032
Phone: 281-670-1100

SAN JUAN
Office Address:
P.O. Box 37247
San Juan, P.R. 00937-0247
Phone: 787-791-4570
Walk-in Address:
Base Aerea Muniz
Area de Carga, Local 2
Escalera B2
Carolina, P.R. 00984

MIAMI
Mailing Address: HQ
Location Address: 3401A, N.W. 72nd Avenue
Miami, FL 33122
305-593-5500 - Main Phone Line
800-927-6059 - Customer Service

LOS ANGELES
Address:945 Towne Avenue
Los Angeles, CA 90021
Phone:213-629-9033

NEW ORLEANS
Address: 200 Crofton Road
Building 9, Suite F
Kenner, LA 70063
Phone: 504-465-3291/3292

NEW YORK
Address: 179-02 150th Avenue
Jamaica, N.Y. 11434
Phone: 718-656-8356/6811/6812
800-276-5387

PORT OF SPAIN
Address: Amerijet Warehouse & Office Complex
Piarco International Airport
Port of Spain
Republic of Trindad & Tobago, W.I.
Phone: 868-669-2138 / 0058 or 868-627-7668

Recovery Team Phone List

Management

Name	Phone numbers	Alternate	Alternate Phones
John Nash, CFO Sr. Recovery Manager	0: 954-320-5329 C:954-401-8925 H: 954-915-0377	Bob Kaltenbach, Controller	O: 954-320-5352 C: 954-608-8807
Dave Bassett, CEO	O: 954-320-5380 O: 954-320-5381 C: 954-647-5727 C: 954-328-0988 H: 954-752-2813		
David Sitek, IT Director Recovery Manager	O: 954-320-5323 C: 305-505-8901 H:786-293-4977	Phil Smith	(See IT System Administrator)
Mark Stewart, VP Airline Operations Operation Recovery	O: 305-704-9667 C: 954-320-2010 H: 954-926-3631	Jay Klucar, Derry Huff	(See Airline and Cargo Team)
Pam Rollins, VP Bus Dev. Station Recovery	O: 954-320-5382 C: 954-608-0133 H: 954-791-2837	Warren Kroll	O: 954320 5359 C 954-608-7110
		Simon Pantin	0:868-669-2138 C:868-682-4510 (POS) C:954-608-0128 (FL) P: 954-248-6254

Airline & Cargo Operations

Name	Phone numbers	Alternate	Alternate Phones
Derry Huff, Director, Flight Operations	O: 954-635-2008 C: 954-655-8444 P: 954-248-7694 H: 305-895-8113	Julio Berard	O: 305-704-9630 C: 786-201-4330 P 954-965-4782 P: 305-493-8854
Lou Montella, Director, MIA Station & HUB	O: 786-437-8215 C: 917-613-4078	Jay Klucar	O: 786-305-8206 C: 786-201-0275
Janice Ambrosio, Sr. Director, Flight & Load Control	O: 786-431-8204 C:786-201-4347 H: 305-971-9714		
Jesus Bencomo, Security Mgr	0:786-431-8238 C: 786-201-4330 P: 305-306-1249 H: 954-436-3621	Jimmy Shields	0:786-431-8369 C: 305-201-4333 P: 305-306-9504

Administration

Linda Duffey	O: 954-320-5377 H: 954-680-5863	Christine Richard	O: 954-320-5354 C: 786-271-5778

IT Department

		Telephone		
Name	Title	Home	Office	Cell
Abby Knott	Sr. Technical Writer/Trainer	561-740-9387	954-320-5312	561-706-5016
Bibi Khan	Web Developer	954-452-9766	954-320-5328	954-593-2655
Constantin Lutchi	Sr. Programmer/Analyst III	954-349-1661	954-320-5319	954-817-8553
Denise Myers	Data Base Analyst I	954-917-8366	954-320-5334	954-937-8366
David Rubin	Sr. Computer Technician	561-732-8280	954-320-5327	954-608-1148
David Sitek	Sr. Director	786-293-4977	954-320-5323	305-505-8901
Ed Llerandi	Sr. Programmer/Analyst III	305-553-5781	954-320-5320	305-753-0520
Jay Singh	Data Base Administrator	561-218-1641	954-320-5314	561-212-3260
Joani Mullen	Webmaster	954-525-3256	954-320-5316	954-254-2028
Marco Dominguez	Computer Technician	305-493-1232	954-320-5325	786-280-4825
Patricia Williams	Programmer/Analyst III	954-584-3138	954-320-5313	954-849-3352
Patrick Lawrence	Network Engineer	954-435-8733	954-320-5321	954-663-7962
Phil Smith	Sr. Network Administrator	None	954-320-5322	954-655-2016
Rossina Prada	Programmer/Analyst III	305-378-9546	954-320-5388	305-505-0747
Victor Puyada	Help Desk Analyst	305-273-7026	954-320-5310	786-200-0079
On-call phone	954-993-6538			

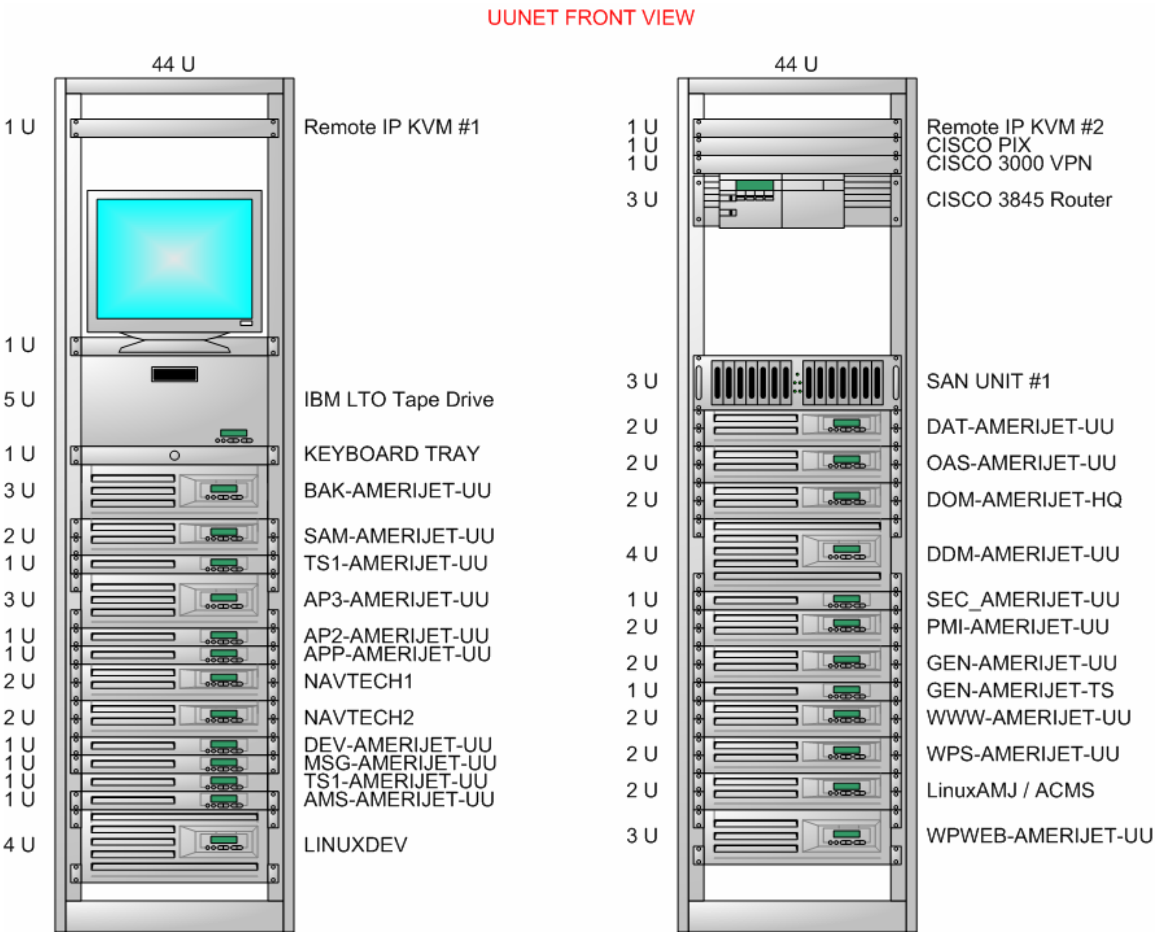
Vendor Phone/Address List

Vendor Name and Address	**Contact/Phone Number**	**Comments**
Don Hillman Inc	954-467-6755	Generator
Kenwood Electric	Richard Hawkins 954-444-5029	
Insight	George Carrillo, 800-467-448 (x6404)	Software, PCs, Server components
CDW	Amanda Snodgrass, 866-448-3720	
PC Mall	Mark Ledingham, 800-555-6255 (x8844)	

Servers

Application	Server name
Web Server:	www-amerijet-uu
Email	dom-amerijet-hq (located at uunet)
Southware /ACMS	linuxAMJ(production), linuxdev (development)
SQL Server	dat-amerijet-uu, san unit high volume disk storage
Geneva	gen-amerijet-uu (production), gen-amerijet-ts (test)
Miscellaneous applications	app-amerijet-uu, ap2-amerijet-uu, ap3-amerijet-uu
Websphere	wps-amerijet-uu, wpweb
Sametime	sam-amerijet-hq
Seta PMI	pmi-amerijet-uu
OASIS	oas-amerijet-uu
Navtech	navtech1 navtech2 (Both at UUNet)
Terminal Services	ts1-amerijet-uu (UUNet), ts1-amerijet-hq (HQ building)
AMS	ams-amerijet-uu
MessageScreen spam filter	msg-amerijet-uu
Internet Proxy	sec-amerijet-uu (future)
Server w/ tape backup units	bak-amerijet-uu
Application development	dev-amerijet-uu
Document Imaging	doc-amerijet-mi (at MIA warehouse)
Document Management	ddm-amerijet-hq (eventually, one DDM per building)
Retrofax	fax-amerijet-hq
Call routing	Zeacom (at MIA Warehouse)
Domain controllers	dc1-amerijet-hq,dc2-amerijet-hq, dc3-amerijet-hq dc1-amerijet-fl (moved to cargo city; will be renamed) dc1-amerijet-mi dc1-amerijet-it (ITN) dc1-amerijet-cc (MIA airport, cargo city) dc1-amerijet-ia (Houston IAH station) dc1-amerijet-an (JFK station) dc1-amerijet-po (Port of Spain regional office)

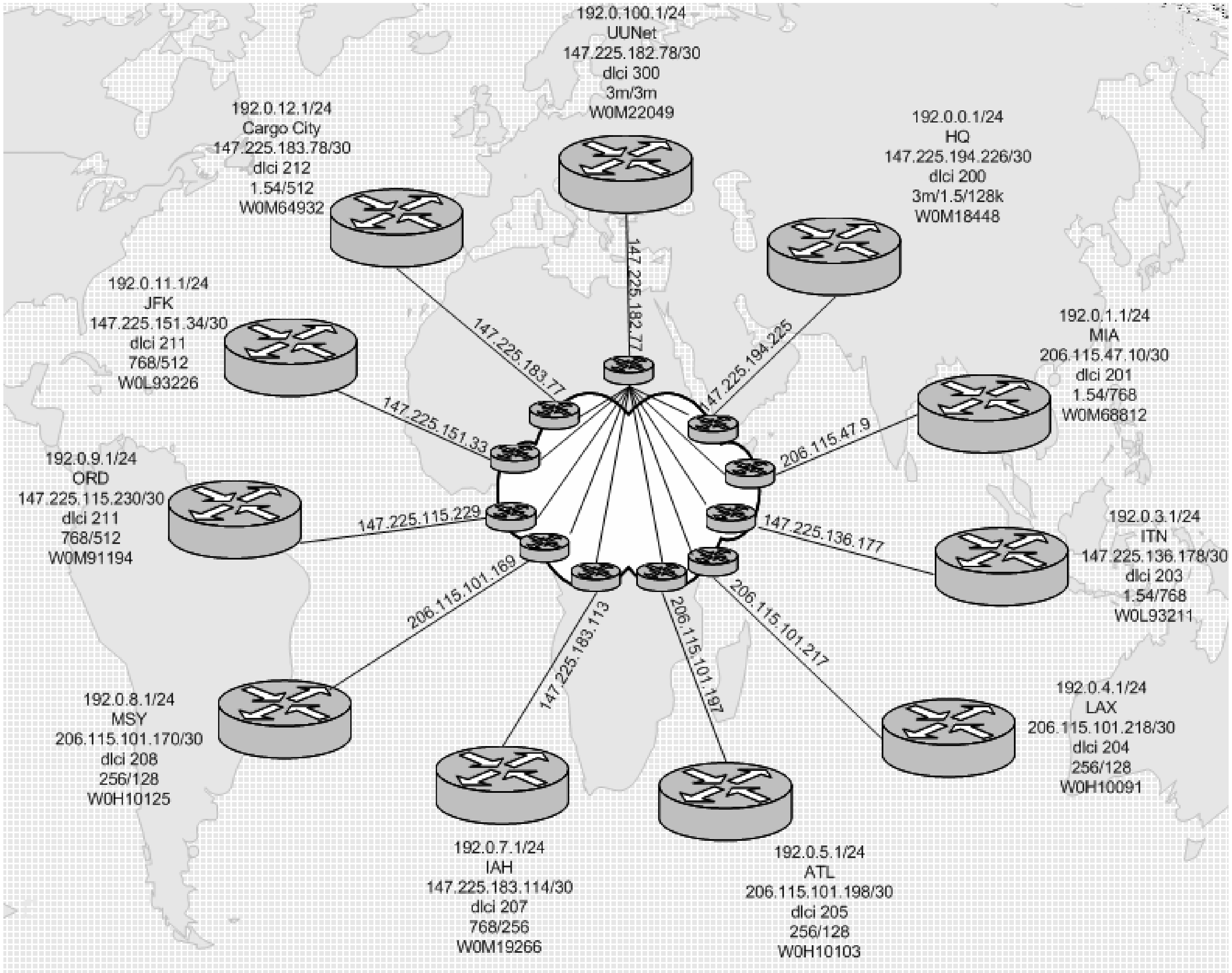
UUNet Server Racks



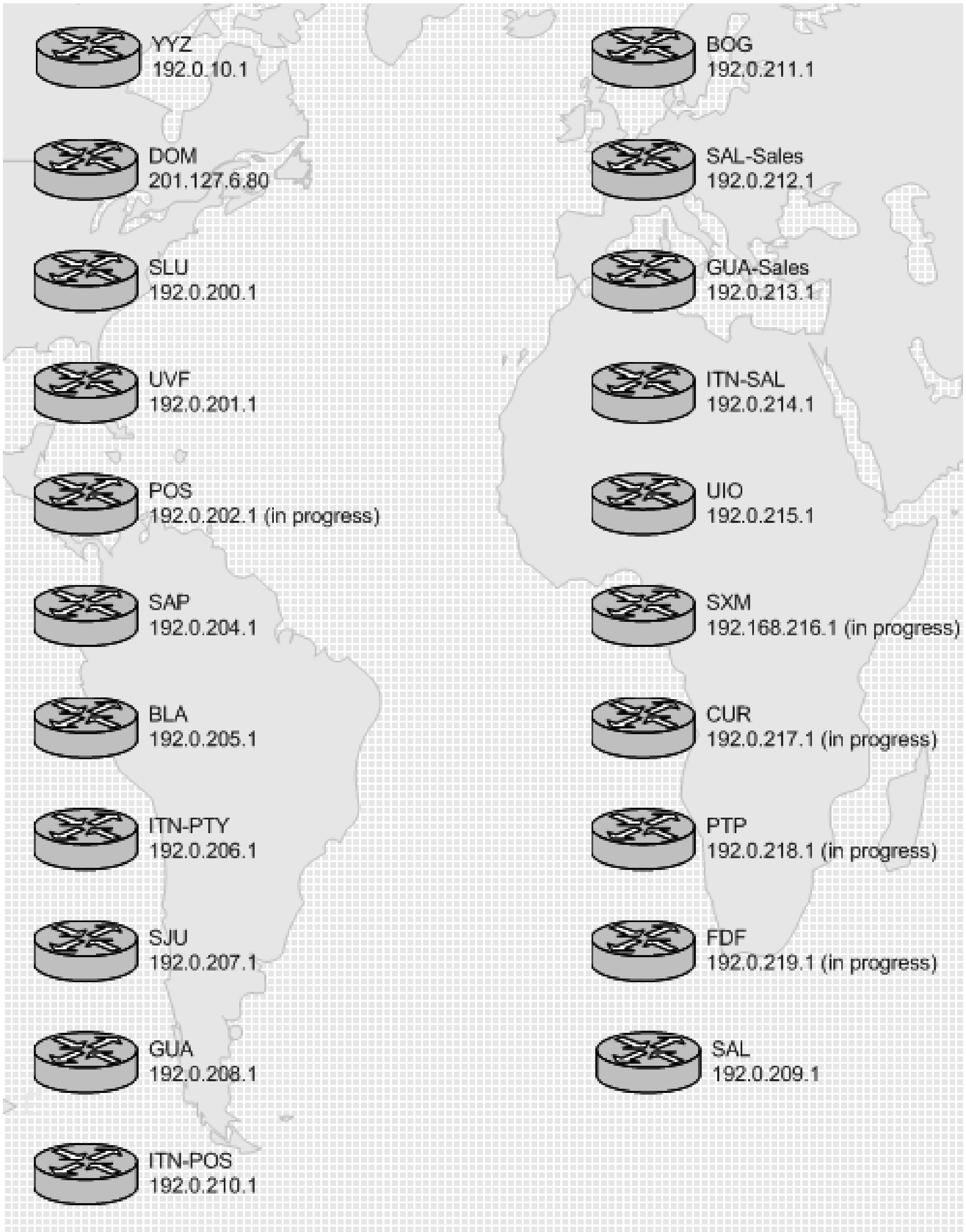
PBX Units

The following locations have PBX boxes:
HQ, IP 192.0.0.8, 192.0.0.9
MIA, IP 192.0.1.8, 192.0.1.9
CC, IP 192.0.12.8, IP 192.0.12.9
IAH, IP 192.0.7.8, 192.0.7.9
ORD, IP 192.0.9.8, 192.0.9.9
JFK IP 192.0.11.8, IP 192.0.11.9
ITN also has a Nortel PBX box (no IP address).
(ITN moves to the MIA warehouse in Summer, 2005.)

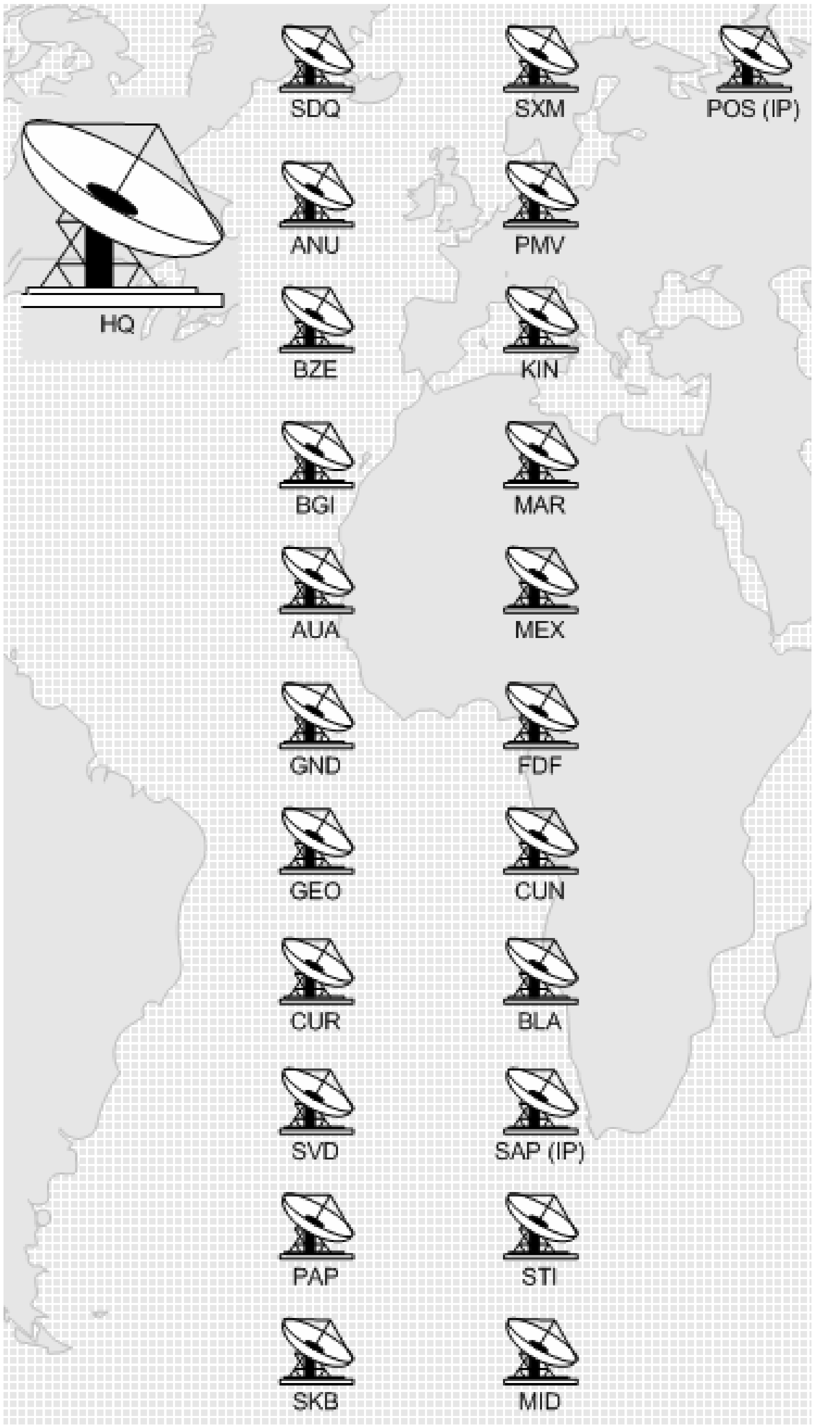
Cisco Routers



Communications – VPN/DSL



Communications – Satellite



People Interviewed

All Interviews were conducted for the 2003 DRP. Some titles have changed and other personnel moved into those positions in 2005. All 2005 employee changes occurred recently, too close to Hurricane season to allow time for new interviews.

Name	**Title**
Janet James	Accounts Payable Manager
Cecil Hicks	HQ Facilities
Robert Kaltenbach	Controller
Santiago Franco	General Ledger Coordinator
Christine Richard	Marketing Director
Layda Garcia, Clara Del Pozo	Interline Partner Management
Jeannine Nelson	Claims Manager
Jorge Cereceda	Customer Service Manager
Jim Tabor	Former Accounts Receivable Manager
Pamela Rollins	Vice President, Business Management
Fadi Aftimos	Vice President, ITN
Jay Klucar	Former MIA Station Manager
Janice Ambrosio	Load & Control Sr Director
Derry Huff	Director, Flight Operations
Tom Paterson	Former Material Services Manager
Jesus Bencomo	Director, Security
John Hughe	Former Financial Planning Manager
John Nash	CFO

Preventative Measures

A Disaster Recovery Plan is an essential document to ensure continued computer operations in the event of a disaster. However, it is also essential for preventative measures be taken to reduce the possible likelihood of a disaster ever occurring. Following are several preventative measures that, when implemented and monitored on a regular basis will reduce the chance of a computer disaster ever occurring or minimize its impact. (This does not imply these procedures are not currently being followed).

- Restrict access to the computer facility to authorized personnel only
- Ensure there are no combustible materials located in the computer facility, such as solvents, paper, etc.
- Conduct regularly scheduled service on support systems, such as the Air Conditioning, Fire Retardant and UPS systems
- Check for overloaded circuits or worn/damaged electrical and power cables
- Perform regularly scheduled backups and store at off-site facility.
- Store copies of vital documentation off-site, such as the Disaster Recovery Plan, Configuration Schematics, Maintenance and Service Contracts, etc.