be locked at all times. Only those people with proper security clearances should be permitted into the machine room area. Suspicious parties should be reported to the police (they may not be terrorists, but they may have theft of expensive computer equipment in mind).

### Recommendations

Maintain good building physical security. Doors into the machine room area should be locked at all times. All visitors to the machine room should receive prior authorization and log in and out.

## 2.2 Disaster Preparation

In order to facilitate recovery from a disaster which destroys all or part of the machine room in the Administrative Building, certain preparations have been made in advance. This document describes what has been done to lay the way for a quick and orderly restoration of the facilities that Computing Services operates.

- *Disaster Recovery Planning*

  The first and most obvious thing to do is to have a plan. The overall plan of which this document is a part is that which Computing Services will use in response to a disaster. The extent to which this plan can be effective, however, depends on disaster recovery plans by other departments and units within the MBA.

  If the Administration Building were involved in a disaster the functions of the Purchasing Department could be severely affected. Without access to the appropriate procedures, documents, vendor lists, and approval processes, the Computing Services recovery process could be hampered by delays while Purchasing recovers.

  Every other department within the MBA should develop a plan on how they will conduct business, both in the event of a disaster in their own office or a disaster at Computing Services that removes their access to data for a period of time. Those departments need means to function while the computers and networks are down, plus they need a plan to synchronize the data that is restored on the central computers with the current state of affairs. For example, if the Payroll Office is able to produce a payroll while the central computers are down, that payroll data will have to be re-entered into the central computers when they return to service. Having a means of tracking all expenditures such as payroll while the central computers are down is extremely important.

- *Recovery Facility*

  If a central facility operated by Computing Services is destroyed in a disaster, repair or rebuilding of that facility may take an extended period of time. In the interim it will be necessary to restore computer and network services at an alternate site.

The MBA will have a number of options for alternate sites, each having a varying degree of up-front costs:

Remote Site-

This is probably the most expensive option for being prepared for a disaster, and is typically most appropriate for very large organizations or Government Agencies. A separate computer facility located in a different city can be built, complete with computers and other facilities ready to cut in on a moment's notice in the event the primary facility goes offline. The two facilities must be joined by high speed dedicated communications lines so that users at the primary site can continue to access the computers from their offices.

Disaster Recovery Company-

A number of companies provide disaster recovery services on a subscription basis. For an annual fee (usually quite steep) you have the right to a variety of computer and other recovery services on extremely short notice in the event of a disaster. These services may reside at a centralized hot site or sites that the company operates, but it is necessary for you to pack up your backup tapes and physically relocate personnel to restore operations at the company's site. Some companies have mobile services which move the equipment to your site in specially prepared vans. These vans usually contain all of the necessary computer and networking gear already installed, with motor generators for power, ready to go into service almost immediately after arrival at your site. (**Note:** Most disaster recovery companies that provide these types of subscription services contractually obligate themselves to their customers to not provide the services to any organization who has not subscribed, so looking to one of these companies for assistance after a disaster strikes will likely be a waste of time.)

Disaster Partnerships-

Some organizations will team up with others in a partnership with reciprocal agreements to aid each other in the event of a disaster. These agreements can cover simple manpower sharing all the way up to full use of a computer facility. Often, however, since the assisting partner has to continue its day-to-day operations on its systems, the agreements are limited to providing access for a few key, critical applications that the disabled partner must run to stay afloat while its facilities are restored. The primary drawback to these kinds of partnerships is that it takes continual vigilance on behalf of both parties to communicate the inevitable changes that occur in computer and network systems so that the critical applications can make the necessary upfront changes to remain operational. Learning that you can't run a payroll, for instance, at your partner's site because they no longer use the same computer hardware or operating system that you need is a painful reality.

One of the most critical issues involved in the recovery process is the availability of qualified staff to oversee and carry out the tasks involved. This is often where disaster partnerships can have their greatest benefit. Through cooperative agreement, if one partner loses key personnel in the disaster, the other partner can provide skilled workers to carry out recovery and restoration tasks until the disabled partner can hire replacements for its staff. Of course, to be completely

fair to all parties involved, the disabled partner should fully compensate the assisting partners for use of their workers unless there has been prior agreement not to do so. The MBA can seek assistance from the Puerto Rico Department of Transportation.

The use of reciprocal disaster agreements of this nature may work well as a low-cost alternative to hiring a disaster recovery company or building a hot site. The primary drawback to these agreements is that they usually have no provision for providing computer and network access for anything other than predefined critical applications. So users will be without facilities for a period of time until systems can be returned to operation.

- *Replacement Equipment*

  This plan contains a complete inventory of the components of each of the computer and network systems and their software that must be restored after a disaster. The inevitable changes that occur in the systems over time require that the plan be periodically updated to reflect the most current configuration. Where possible, agreements will be made with vendors to supply replacements on an emergency basis. To avoid problems and delays in the recovery, every attempt should be made to replicate the current system configuration. However, there will likely be cases where components are not available or the delivery timeframe is unacceptably long. The Recovery Management Team will have the expertise and resources to work through these problems as they are recognized. Although some changes may be required to the procedures documented in the plan, using different models of equipment or equipment from a different vendor may be suitable to expediting the recovery process.

- *Backups*

  New hardware can be purchased. New buildings can be built. New employees can be hired. But the data that was stored on the old equipment cannot be bought at any price. It must be restored from a copy that was not affected by the disaster. There are a number of options available to us to help ensure that such a copy of your data survives a disaster at the primary facility.

Remote Dual Copy

This option calls for a disk subsystem located at a site away from the primary computer facility and fiber optic cabling coupling the remote disk to the disk subsystem at the primary site. Data written to disk at the primary site are automatically transmitted to the remote site and written to disk there as well. This guarantees that you have the most up-to-the-second updates for the databases at the primary site in case it is destroyed. You can simplify the recovery process by locating the remote disk subsystem at the disaster recovery site. This option is somewhat expensive, but not prohibitively so. It does not require that an entire computer system be built at a hot site, just the disk subsystem.

Automated Off-Site Tape Backup

This option calls for a robotic tape subsystem located at a site away from the primary computer facility and fiber optic cabling (the MBA backbone network would be suitable) coupling the subsystem to the primary computer facility. Copies of operating system data, application and user programs, and databases can be transmitted to the remote tape subsystem where it is stored on magnetic tape (optical writable disk media can also be used, but may be more expensive).

While this option does not guarantee the up-to-the-second updates available with the remote dual copy disk option, it does provide means for conveniently taking backups and storing them off-site any time of the day or night. Although such a system is expensive, it is not prohibitively so.

Off-Site Tape Backup Storage

This option calls for the transportation of backup tapes made at the primary computer facility to an off-site location. Choice of the location is important. You want to ensure survivability of the backups in a disaster, but you also need quick availability of the backups.

This option has some drawbacks. First, there is a period of exposure from the time that a backup is made to the time it can be physically removed off-site. A disaster striking at the wrong time may result in the loss of all data changes that have occurred from the time of the last off-site backup. There is also the time, expense, and energy of having to transport the tapes. And there is also the risk that tapes can be physical damaged or lost while transporting them.

MBA has a contract with a disaster recovery company to store their backup in hardened storage facilities. While this certainly provides for more secure data storage, considerable expense is undertaken for regular transportation of the data to the storage facility. Quick access to the data can also be an issue if the storage facility is a long distance away from your recovery facility.

- *Backup Procedure*

Every system that Information Systems operates is backed up regularly. The backup media for each of these systems is relocated to an off-site storage area where there is a high probability that the media will survive in the event a disaster strikes. One off-site storage locations are used.

Three sets of backups exist at any one time. When a new backup is made, the tapes are rotated and the oldest are retained for use with the next round of backups.

The procedures for making the backups for each individual computer system differ. In general, media-level or full file system level backups are taken in a given cycle (typically weekly). In some instances, there are additional application-level backups for a system that may be run on a daily basis. Some systems support incremental backups, and these are typically run on a daily basis.

# Section 3: Initiation of Emergency Procedures

## 3.1 Safety Issues

In almost any disaster situation, hazards and dangers can abound. While survival of the disaster itself can be a harrowing experience, further injury or death following the disaster stemming from carelessness or negligence is senseless. All personnel must exercise extreme caution to ensure that physical injury or death is avoided while working in and around the disaster site itself. No one is to perform any hazardous tasks without first taking appropriate safety measures.

- *Hazardous Materials*

There are hazardous materials present in the Administrative Building. Three primary sources exist for these materials:

- ✓ Janitorial supplies - hazardous chemicals are present in the janitorial closets scattered throughout the building. The door to each closet will contains a list of the chemicals present in the closet. If this information is not present at the scene of the disaster, contact the Physical Plant for a list of the chemicals located in the building.

- ✓ Battery acid - hazardous battery acid is present in large quantities in the Uninterruptible Power Supply equipment. Battery acid can cause caustic skin burns, blindness, and pulmonary distress if inhaled. If you come in contact with battery acid, immediately seek a source of water and wash the affected areas continuously until medical assistance can be sought.

- ✓ Automotive fluids - hazardous substances related to the operation of a motor vehicle are present in the MBA garages. These can include, but are not limited to, gasoline, motor oil, brake fluid, antifreeze, lubricants, and battery acid.

Approach any collection of a hazardous material with caution. Notify the nearest safety personnel in the event of a hazardous material spill. Unless you have had the necessary training to do so, do not attempt to clean up a hazardous material spill yourself. Allow the local Safety personnel team to evaluate, neutralize, and clean up any spills.

- *Stress Avoidance*

Recovery from a disaster will be a very stressful time for all personnel involved. Each manager should be careful to monitor the working hours of his staff to avoid over-exertion and exhaustion that can occur under these conditions. A good approach is to divide your team members into shifts and rotate on a regular basis. This will keep team members fresh and also provide for needed time with family.

Post-traumatic Stress Disorder (PTSD) is a very real condition that can affect survivors and recovery workers in a disaster. All recovery managers and coordinators should be alert to symptoms in their employees that indicate PTSD and seek assistance from the necessary counseling services.

## 3.2 Disaster Notification List

The disaster notification list for Information System as is shown below. These people are to be notified as soon as possible when disaster threatens or occurs.

- Emergency Fire, Ambulance, Rescue, Police, and Hazardous Material- **911**
- MBA Internal Security: Sr. Daniel Ruiz **(787) 698-3031**
- Physical Plant Service: Sr. Waldemar Quiles **(787) 552-4338**
- Information Systems Primary Notification: Sr. Wilfredo Ramos **(787) 698-1654**
- Other Computing Services Contacts: Sr. Ernesto Leon **(787) 698-3033**

## 3.3 Disaster Recovery Teams

To function in an efficient manner and to allow independent tasks to proceed simultaneously, the recovery process will be handled by teams. This plan calls for five teams that work together, but for which specific portions of the recovery are assigned.

The five Disaster Recovery Teams are:

- Recovery Management Team
- Damage Assessment Team
- Facility Recovery Team
- Network Recovery Team
- Administrative Support Team

As the recovery process gets underway, it is imperative that each of the recovery teams remain in close communication and strive to work together to complete the recovery as expediently as possible.

### *1. Recovery Management Team*

The Recovery Management Team oversees the whole recovery process. The other four teams are represented in the Recovery Management Team. The Recovery Manager leads the Recovery Management Team. The Manager has the final authority on decisions that must be made during the recovery. The Recovery Manager is responsible for appointing the other members of the

Recovery Management Team. Each member of the Recovery Management Team will have the responsibility for appointing the other members of the respective team(s).

The selection of the members of the Recovery Management Team is very important. Since it is almost impossible to document exactly what each of the individual recovery teams will be required to do (each disaster will have its own special set of circumstances, many of which will be completely unanticipated), each member of the Recovery Management Team must be capable of stepping in with the technical and management skills to make the on-the-spot decisions necessary to complete the task at hand.

The discussion that follows identifies those skills that are needed by members of the Recovery Management Team. If these positions are filled with qualified individuals, then the odds for a timely and successful recovery are very high.

- *Recovery Manager*

This individual needs to be a skilled manager/administrator who is accustomed to dealing with pressure situations. He should have a broad knowledge of the hardware and software in use at the site. He should be a "problem solver" as there will be many problems arise that have not been anticipated in advance. He must be able to delegate responsibility to others. He must also have signature authority to expend funds as a part of the disaster recovery process. The Recovery Manager is the leader of the Recovery Management Team and has the final authority regarding decisions during the recovery process. Each of the remaining individuals will be the leader of a specialized team that will address a portion of the recovery tasks. As the recovery process gets underway, there will likely be areas of overlap between teams and close communication will be required. The Recovery Management Team will have regular meetings scheduled to provide for communication between team coordinators.

Each coordinator should schedule a meeting for members of his team well in advance of their first planned activities. A first-meeting agenda might include:

1. Reviewing the current status of the recovery operation.
2. Emphasizing what the team's responsibilities are
3. Making sure that members are aware of any changes to the original recovery plan
4. Assigning tasks to individual team members
5. Setting up time and location for future team meetings

- *Facilities Coordinator*

  This individual needs some of the same skills as the Recovery Manager. However, he also needs to be familiar with the process of getting construction work scheduled and completed on time. He should be able to understand and oversee the setup of the electrical, environmental, and communications requirements of a data center.

- *Technical Coordinator*

  This individual needs to be highly skilled in a number of areas. He must have a strong background in the setup and interfacing of as many of the platforms in use as possible. He needs to be able to communicate easily with vendor technical representatives and engineers concerning installation options, performance issues, problem resolution, and a myriad of other things. This individual needs to be skilled in the area of network design and maintenance. He should be trained in diagnosing and correcting network outages and in connecting and debugging new additions to an existing network.

- *Administrative Coordinator*

  This individual needs to be skilled in the business operations of the MBA. He should be well acquainted with the day-to-day operations of MBA. He should also be a "people person" who can deal with employees and their families during hard times. This person must also be familiar with local and federal purchasing procedures and contracts.

### *2. Damage Assessment Team*

The Damage Assessment Team will be led by the Technical Coordinator. He will be responsible for selecting the other team members. Likely choices would be a member(s) from Physical Plant, Operations, Network Services, MBA Telephone Services, and Technical Services. This team will not be responsible for a detailed damage assessment for insurance purposes. The primary thrust for this team is to do two things:

1. Provide information for the Recovery Management Team to be able to make the choice of the recovery site.
2. Provide an assessment of the "salvageability" of major hardware components.

Based on this assessment the Recovery Management Team can begin the process of acquiring replacement equipment for the recovery.

### *3. Facility Recovery Team*

The Facility Recovery Team will be led by the Facilities Coordinator. He will be responsible for selecting the other team members. Likely choices would be member(s) from Operations, Network Services, Physical Plant, and Technical Services.

This team will be responsible for the details of preparing the recovery site to accommodate the hardware, supplies, and personnel necessary for recovery. Detailed layouts and instructions for the Remote Site preparation are included in the recovery plan.

This team will also be responsible for oversight of the activities for the repair and/or rebuilding of the primary site (the Administrative Building). It is anticipated that the major responsibility for this will lie within Physical Plant and contractors. However, this team must oversee these

operations to ensure that the facility is repaired to properly support the operation of mainframe and networking equipment per the original design of the primary site.

### *4. Network Recovery Team*

The Network Recovery Team will be led by the Technical Coordinator. He will be responsible for selecting the other team members. Likely choices would be member(s) from Network Services, Technical Services, User Services, and Physical Plant. It may also be helpful to have the building and/or network manager for the Remote Site building be a part of this team should it be necessary to use the Remote Site.

This team will be responsible for overseeing the restoration of the campus network and all network connections necessary at the recovery site. It is entirely possible in certain disaster situations that the Network Recovery Team may be the only team convened as a result of a campus disaster. For instance, should a fire occur at the Operations Building and destroy fiber optic connections and network equipment, this team will be charged with the recovery of operations out of that building or in another building on MBA in the most expedient manner.

Because there is such a high degree of reliance on the MBA network administrative purposes very high emphasis must be placed on restoring the network as quickly as possible.

### *5. Administrative Support Team*

The Administrative Support Team will be led by the Administrative Coordinator. He will be responsible for selecting the other team members. This team will provide administrative support to the other recovery teams as well as support to employees and their families. One of the most important functions that this team can provide is to take the burden of administrative details so that the engineers and technicians who are responsible for systems recovery can concentrate on their recovery work.

One member of this team should be designated as Family Contact. This person will be available throughout the recovery process to provide assistance to employee family members.

One member of this team should be a designated representative of the MBA Purchasing Office. This person will be the liaison to the Administration Office for the purpose of expediting all emergency purchases and ensuring that proper local and federal regulations for purchasing in an emergency are followed. The Purchasing Office has their own Disaster Contingency Plan that they will implement to aid departments needing to restore or rebuild facilities in the event of a disaster.

Some of the anticipated team tasks include:

1. Provide support for executing acquisition paperwork.
2. Assist with the detailed damage assessment and insurance procedures.
3. Determine the status of staff working at the time of the disaster.

4. Provide counseling services for staff or family members having emotional problems resulting from the disaster.
5. Assist the individual Team Coordinators in locating potential team members.
6. Coordinate food and sleeping arrangements of recovery staff as necessary.
7. Provide support to track time and expenses related to the disaster.
8. Provide delivery and transportation services to the Remote Site or other locations as required.
9. Provide public relations support (this function may be provided by MBA Press Office).
10. Assist in contracting with outside parties for work to be done in the recovery process (such as the installation of equipment, or consulting assistance for the installation or recovery of software systems).

## 3.4 Activating the Disaster Recovery Plan

- *Appointment of Recovery Manager*

The first order of business is to appoint the Recovery Manager. The person most appropriate for the position is the current Director of Information Systems. If the Director is unavailable, the appointment should be made by the Vice President of Administration. This person must have data center management experience and must have signature authority for the expenditures necessary during the recovery process.

- *Determine Personnel Status*

One of the Recovery Manager's important early duties is to determine the status of personnel working at the time of the disaster. Safety personnel on site after the disaster appraised the proposal carefully or first aid necessary to people caught in the disaster. However, the Recovery Manager should produce a list of the able-bodied people who will be available to aid in the recovery process.

The Recovery Manager should also quickly appoint the Administrative Support Coordinator, whose responsibility it will be to identify anyone injured or killed in the disaster. The Administrative Support Coordinator will work with families and employees, ministering to their needs and obtaining counseling services as necessary.

Taking care of our people is a very important task and should receive the highest priority immediately following the disaster. While we will have a huge technical task of restoring computer and network operations ahead of us, we can't lose sight of the human interests at stake.

- *Equipment/Media Protection and Salvage*

A primary goal of the recovery process is to restore all computer operations without the loss of any data. It is important that the Recovery Manager appoint the Technical Coordinator quickly so that he can immediately set about the task of protecting and salvaging any magnetic media on

which data may be stored. This includes any magnetic tapes, optical disks, CD-ROMs, and disk drives.

- *Establish the Recovery Control Center*

The Recovery Control Center is the location from which the disaster recovery process is coordinated. The Recovery Manager should designate where the Recovery Control Center is to be established. If a location in the Administrative Building is not suitable an off-site location of the center would be designated.

- *Activating the Disaster Recovery Plan*

The Recovery Manager sets the plan into motion. Early steps to take are as follows:

1. The Recovery Manager should retrieve an up-to-date copy of the Disaster Recovery Plan. This plan is in printed form as well on computer media (flash drive or CD-ROM). Copies of the plan should be made and handed out at the first meeting of the Recovery Management Team.

2. The Recovery Manager is to appoint the remaining members of the Recovery Management Team. This should be done in consultation with surviving members of the Computing Services staff and Physical Plant management, and with upper MBA administration approval. The Recovery Manager's decision about who sits on the Recovery Management Team is final, however.

3. The Recovery Manager is to call a meeting of the Recovery Management Team at the Recovery Control Center or a designated alternate site. The following agenda is suggested for this meeting:

    - ✓ Each member of the team is to review the status of their respective areas of responsibility.
    - ✓ After this review, the Recovery Manager makes the final decision about where to do the recovery.
    - ✓ The Recovery Manager briefly reviews the Disaster Recovery Plan with the team.
    - ✓ Any adjustments to the Disaster Recovery Plan to accommodate special circumstances are to be discussed and decided upon.
    - ✓ Each member of the team is charged with fulfilling his/her respective role in the recovery and to begin work as scheduled in the Plan.
    - ✓ Each member of the team is to review the makeup of their respective recovery teams. If individual's key to one of the recovery teams is unavailable, the Recovery Manager is to assist in locating others who have the skills and experience necessary, including locating outside help from other area computer centers or vendors.

- ✓ The next meeting of the Recovery Management Team is scheduled. It is suggested that the team meet at least once each day for the first week of the recovery process.

4. The Recovery Management Team members are to immediately start the process of contacting the people who will sit on their respective recovery teams and call meetings to set in motion their part of the recovery.

5. Mobile communications will be important during the early phases of the recovery process. This need can be satisfied through the use of cellular telephones and/or two-way radios. The MBA has an existing contract with a company for cellular service, and the Communication Center has two-way radio units that may be available upon request.

## 3.5 Equipment Protection and Salvage

This document contains information on procedures to be used immediately following an incident to preserve and protect resources in the area damaged.

- *Protection*

  It is extremely important that any equipment, magnetic media, paper stocks, and other items at the damaged primary site be protected from the elements to avoid any further damage. Some of this may be "salvageable" or repairable and save time in restoring operations.

  - ✓ Gather all magnetic tape cartridges into a central area and quickly cover with plastic sheeting to avoid water damage.
  - ✓ Cover all computer equipment to avoid water damage.
  - ✓ Cover all undamaged paper stock to avoid water damage.
  - ✓ Ask the police to post security guards at the primary site to prevent looting or scavenging.

- *Salvage Magnetic and Optical Media*

  The magnetic and optical media on which our data is stored is priceless. Although we retain backups of our primary application systems off-site, magnetic tapes stored in the tape vault and machine room area contain extremely valuable information that would be tough to lose. If the media has been destroyed, such as in a fire, then nothing can be done. However, water and smoke damage can often be reversed, at least good enough to copy the data to undamaged media.

After protecting the media from further damage, recovery should begin almost immediately to avoid further loss. A number of companies exist with which the MBA can contract for large scale media recovery services.

- *Salvage Equipment*

  As soon as practical, all "salvageable" equipment and supplies need to be moved to a secure location. If undamaged, transportation should be arranged through the Recovery Manager to move the equipment to the Remote Site or to another protective area (such as a warehouse) until the Remote Site is ready.

  TAKE GREAT CARE WHEN MOVING THE EQUIPMENT TO AVOID DAMAGE.

  If the equipment has been damaged, but can be repaired or refurbished, the Remote Site may not be the best location for the equipment, especially if there is water or fire damaged that needs to be repaired. Contractors may recommend an alternate location where equipment can be dried out, repainted, and repaired.

- *Inventory*

  As soon as practical a complete inventory of all "salvageable" equipment must be taken, along with estimates about when the equipment will be ready for use (in the case that repairs or refurbishment is required). This inventory list should be delivered to the Technical Coordinator and Administrative Coordinator who will use it to determine which items from the disaster recovery hardware and supplies lists must be procured to begin building the recovery systems.

## 3.6 Damage Assessment

This damage assessment is a preliminary one intended to establish the extent of damage to critical hardware and the facility that houses it. The primary goal is to determine where the recovery should take place and what hardware must be ordered immediately.

Team members should be liberal in their estimate of the time required to repair or replace a damaged resource. Take into consideration cases where one repair cannot begin until another step is completed. Estimates of repair time should include ordering, shipping, installation, and testing time.

In considering the hardware items, consider first the equipment lists provided in the recovery sections for each platform. These lists were constructed primarily for recovery at the Remote Site so they consist of the critical components necessary to recovery. You will need to separate items into two groups. One group will be composed of items that are missing or destroyed. The second will be those that are considered "salvageable". These "salvageable" items will have to be evaluated by hardware engineers and repaired as necessary. Based on input from this process, the Recovery Management team can begin the process of acquiring replacements.

With respect to the facility, evaluation of damage to the structure, electrical system, air conditioning, and building network should be conducted. If estimates from this process indicate that recovery at the original site will require more than 14 days, migration to the Remote site is recommended.

## 3.7 Emergency Procurement Procedures

The success or failure of this plan's ability to ensure a successful and timely recovery of the network facilities hinges on our ability to purchase goods and services with lightening speed.

The MBA Purchasing Office has a disaster recovery plan of their own that will assist departments in the rapid turnaround of emergency procurements.

The liberal policy for emergency procurement, coupled with extensive Business Interruption Insurance, provides the Recovery Manager with a sound basis for aggressive recovery actions. Perhaps now is the time for a word of caution. There will always be a day of reckoning following every exciting event, when those actions taken under the stress of the moment will be examined and evaluated in the light of normality. You can significantly reduce your anxiety level in the eve of such an accounting by following preset rules and directives - to the extent possible under the circumstances - and most importantly, keeping records and logs of transactions.

The Administrative Support Coordinator is responsible for all emergency procurement for Computing Services. All Disaster Recovery Team members must submit their requests to the Coordinator. The Coordinator will follow the regulations established for emergency procurement and will work with the Buyer that has been appointed by the Purchasing Office to complete the acquisition.

The Administrative Support Coordinator is also responsible for tracking all acquisitions to ensure that financial records of the disaster recovery process are maintained and that all acquisition procedures will pass audit review.

The Administrative Support Coordinator must also be aware of the MBA insurance coverage to know what is and is not allowed under our policies. In the event an item to be purchased is disallowed by insurance coverage, or if expenses exceed the dollar limits of the insurance coverage, the Coordinator must consult with the Recovery Manager and other responsible MBA personnel.

# Section 4: Initiation of Recovery Procedures

## 4.1 Remote Site Preparation

- *Network Connections*

If the Recovery Management Team opts to use this site for recovery after the disaster, some work must be done to convert the space to be able to house the disaster recovery team personnel.

A variety of networking connections are needed for the communication with the Remote Site. In general, these consist of FDDI fiber optic links to the MBA backbone for the server equipment, with Ethernet links servicing some servers and any personal computers in use by recovery personnel in the area.

It is recommended that all Ethernet connections be using Category 6 UTP cabling. This requires that an Ethernet hub with sufficient ports be provided, with a connection to the router in MBA. The MBA System personnel may be able to assist with short-term networking equipment needs, and cabling may already be present in some office suites or work areas.

Although Category 6 UTP cabling is not as fragile as fiber optic cabling, provisions to protect the cable would be wise. Use of conduit or cable trays or cable hooks is advised.

IP Addresses - Each piece of equipment attached to the network will have to have a valid IP address. It is likely that the IP address for each system will be different than their counterpart in the damaged primary facility. As a result, the instructions for recovering each system include information on setting the IP addressing parameters.

## 4.2 Network Recovery Procedures

- *Restore Process*

To restore this system would be straight forward. Providing good backup tapes exist. The first step is to acquire and assembles equipment that matches the previous system as close as possible. Make a Duplicate of the file systems during the OS install to match the original layout. Restore the user community, mail spool and various files such as the password file. Below is an outline of how this process might occur.

To create a replacement system from scratch will involve the following steps:

1) Acquire replacement component parts (as detailed above)

2) Determine suitable site for assembling replacement system.

3) Put together the replacement system (Hardware)

4) Establish base operating system and network capability.

5) Restore file system layout to match previous system.

6) Restore directly from tape file systems from previous system.

7) Test and evaluate to see if all systems are in place.

## 4.3 Applications Recovery Overview

Once the platform system software and subsystems are operating correctly, the task of preparing the remaining end-user applications can begin. Each platform will have a unique recovery road to follow. In some cases, there may be very little to do except for general testing. In other cases, considerable analysis and data synchronization work will likely be required.

The Applications Recovery Team will be responsible for carrying out this phase of the recovery. Each application area will require a review. This review should be conducted by an analyst familiar with the application while working closely with an application user representative.

Items to be considered should include:

- ✓ Review of the user department Disaster Recovery Plan with special attention to any "interim" procedures that have been required in the time period since the disaster event occurred.
- ✓ Review of the application documentation concerning file and database recovery.
- ✓ Review the status of files and databases after the general platform recovery processing is complete.
- ✓ Identify any changes to bring the application to a ready for production status.
- ✓ Identify any areas where the application must be synchronized with other applications and coordinate with those application areas.
- ✓ Identify and review application outputs to certify the application ready for production use.

## 4.4 Critical Applications

The MBA has identified the payroll application as a critical application. This means that delaying the processing of this application could cause much hardship on employees and others that depend on it. Other applications that may be handled as critical or given very high priority in recovery are the Purchasing application and the Exchange server application since they will be needed during recovery.

There are two Payroll functions each month that are considered critical:

TUAMA PAYROLL

It is paid bi weekly

REGULAR PAYROLL

It is paid the days 15 and 30 of each month.

Should a disaster place the MBA in a position where these obligations cannot be met by the normal applications systems, a secondary plan is being developed.

- *Proposed Interim Solution*

Discussions are ongoing with the Payroll department to devise a set of manual procedures that would be implemented. These procedures would allow for regular payroll obligations to be met and records kept so that the automated system could be updated when ready. Further documentation for these plans will be published when completed.

# Section 5: Maintaining the Plan

Having a disaster recovery plan is critical. But the plan will rapidly become obsolete if a workable procedure for maintaining the plan is not also developed and implemented. This document provides information about the document itself, standards used in its construction, and maintenance procedures necessary to keep it up to date.

- *Web Server Accessible*

This disaster recovery plan has been designed to will be accessible as a World Wide Web document retrievable from a web server or through a browser (e.g., Explorer file browse mode). This will makes it easy to access the plan for periodic review and provides a convenient means for structuring the plan in an online fashion. It is presently maintained on the MBA system as a set of HTML-formatted text files and image (GIF) files.

- *Basic Maintenance*

The plan will be routinely evaluated once each year. All portions of the plan will be reviewed by Technical Services. In addition the plan will be tested on a regular basis and any faults will be corrected. The Disaster Recovery Plan coordinator has the responsibility of overseeing the individual documents and files and ensuring that they meet standards and consistent with the rest of the plan.

- *Change-Driven Maintenance*

It is inevitable in the changing environment of the computer industry that this disaster recovery plan will become outdated and unusable unless someone keeps it up to date. Changes that will likely affect the plan fall into several categories:

1. Hardware changes
2. Software changes
3. Facility changes
4. Procedural changes
5. Personnel changes

As changes occur in any of the areas mentioned above, Computing Services management will determine if changes to the plan are necessary. This decision will require that the managers be familiar with the plan in some detail. A document referencing common changes that will require plan maintenance will be made available and updated when required.

Changes that affect the platform recovery portions of the plan will be made by the staff in the affected area. After the changes have been made, Technical Services will be advised that the

updated documents are available. They will incorporate the changes into the body of the plan and distribute as required.

- *Changes Requiring Plan Maintenance*

The following lists some of the types of changes that may require revisions to the disaster recovery plan. Any change that can potentially affect whether the plan can be used to successfully restore the operations of the department's computer and network systems should be reflected in the plan.

Hardware

1. Additions, deletions, or upgrades to hardware platforms.

Software

1. Additions, deletions, or upgrades to system software.
2. Changes to system configuration.
3. Changes to applications software affected by the plan.

Facilities

1. Changes that affect the availability/usability of the Remote Site location.

Personnel

1. Changes to personnel identified by name in the plan.
2. Changes to organizational structure of the department.

Procedural

1. Changes to off-site backup procedures, locations, etc.
2. Changes to application backups.
3. Changes to vendor lists maintained for acquisition and support purposes.

Estado Libre Asociado de Puerto Rico
Autoridad Metropolitana de Autobuses

# PLAN DE TRABAJO RESGUARDO DE CINTAS MAGNETICAS

**Objetivos: Implantación del sistema de resguardo**

| Actividades | Recursos | Fechas |
|---|---|---|
| 1. Resguardo de Cintas Magnéticas | -Área de Tecnología y Sistemas de Información<br>-Compañía de resguardo | Año 2010 |
| 1.1 Resguardo de todo los sistemas en 8 cintas magnéticas sustituidas cada dos semana | -Área de Tecnología y Sistemas de Información | Año 2010 |
| 1.2 Cada viernes se llevara tres (3) cintas magnéticas conteniendo los resguardos de la Autoridad Metropolitana de Autobuses, al área de resguardo externa. Se conservaran por 6 semanas en el área de resguardo externa y al finalizar el periodo serán retiradas para rehusarse y comenzar con un nuevo ciclo de resguardo. | -Área de Tecnología y Sistemas de Información<br>-Compañía de resguardo | Año 2010 |

**Objetivos: Implantación del sistema de resguardo**

| Actividades | Recursos | Fechas |
|---|---|---|
| 1.3 Se conservaran por día, dos (2) cintas magnéticas del sistema MS Dynamics GP y una (1) cinta magnética del sistema general, de la Autoridad Metropolitana de Autobuses en la caja fuerte de resguardo del Área de Tecnología y Sistemas de Información. | -Área de Tecnología y Sistemas de Información | Año 2010 |
| 1.4 Cada noventa (90) días se realizara pruebas de reinstalación de los sistemas | -Área de Tecnología y Sistemas de Información | Año 2010 |

**REVISED AND RECCOMENDED BY:**

Antonio Lafontaine, Gerente
Área de Tecnología y Sistemas de Información
Autoridad Metropolitana de Autobuses

**REVISED AT LEGAL DIVISION BY:**

Lcda. Margarita Meléndez Renaud
Asesora Legal
Autoridad Metropolitana de Autobuses

**APPROVED BY**:

Sr. Mike O'Neill Rosa
Presidente y Gerente General
Autoridad Metropolitana de Autobuses