dtop
TRANSPORTE
URBANO

13 de enero de 2011

Sr. Antonio Lafontaine ALF
Ayudante del Presidente 14 ene 11
Sistemas de Información

Lcda. Denise Rodríguez Flores
Vicepresidenta Ejecutiva

RE: DISASTER RECOVERY PLAN

Le acompaño, para su conocimiento y tramite correspondiente, el "Disaster Recovery Plan" de la Autoridad Metropolitana de Autobuses.

dtop
TRANSPORTE
URBANO

13 de enero de 2011

Lcda. Margarita Meléndez
Asesora Legal

Lcda. Denise Rodríguez Flores
Vicepresidenta Ejecutiva

RE: DISASTER RECOVERY PLAN

Le acompaño, para su conocimiento y tramite correspondiente, el "Disaster Recovery Plan" de la Autoridad Metropolitana de Autobuses.

dtop

TRANSPORTE
URBANO

11 de enero de 2011

Recibido por: Sonia I. Ortiz Robles
13/enero/2011
10:40 am

Sra. Sonia I. Ortiz
Directora
Oficina Auditoría Interna

Lcda. Denise Rodríguez Flores
Vicepresidenta Ejecutiva

RE: DISASTER RECOVERY PLAN

Le acompaño copia del "Disaster Recovery Plan", de la Autoridad Metropolitana de Autobuses, que ha sido enviado para la firma del Ing. Rubén Hernández Gregorat, Secretario DTOP.

Gobierno de Puerto Rico
Departamento de Transportación y Obras Públicas
AUTORIDAD METROPOLITANA DE AUTOBUSES
P.O. Box 195349 San Juan, Puerto Rico 00919-5349
TEL. 787-294-0500 FAX. 787-751-0527

Al contestar refiérase
a este número

22 de diciembre de 2010

Lcda. Denise Rodríguez-Flores
Vicepresidenta Ejecutiva
Autoridad Metropolitana de Autobuses y Ramas Anexas

Estimada Señora Rodríguez:

RE: Plan de Recuperación de Desastres.

Adjunto las copias del Plan de Recuperación de Desastres, para el Área de Tecnología Informática de la Autoridad Metropolitana de Autobuses y de la Autoridad de Carreteras y Transportación.

Evaluados los documentos de referencia entendemos que ambos planes de Recuperación de Desastres están de acorde.

Sin otro particular por el momento, me despido.

Lcda. Margarita Meléndez Renaud
Asesor Legal
Autoridad Metropolitana de Autobuses

RSP & Associates Law Office

Raúl Santiago Pérez, JD Managing Partner

21 de octubre de 2010

Lcda. Denise Rodríguez Flores
Directora de División Legal
Autoridad Metropolitana de Autobuses
Apartado 195349
San Juan, PR 00919-5349

RE: DISASTER RECOVERY PLAN

Estimada licenciada Rodríguez:

Evaluado el documento de referencia encontramos que el mismo cumple con todos los requisitos de ley. El único cambio sugerido va dirigido a que se establezca el periodo de los "Back up", el cual debe ser diariamente.

Sin otro particular, quedo a sus órdenes.

Cordialmente,

Raúl Santiago Pérez

c Sra. Pilar M. Díaz Guevara

mrp

MBA INFORMATION SYSTEM DEPARTMENT
Disaster Recovery Plan

Introduction

This document is the disaster recovery plan for the Metropolitan Bus Authority (MBA), Information System Department Services. The information present in this plan guides MBA management and technical staff in the recovery of computing and network facilities in the event that a disaster destroys all or part of the facilities.

Description

The Recovery plan is composed of a number of sections that document resources and procedures to be used in the event that a disaster occurs at the Information System facility at San Francisco Main Facilities. Each supported computing platform has a section containing specific recovery procedures. There are also sections that document the personnel that will be needed to perform the recovery tasks and an organizational structure for the recovery process.

This plan will be available through the Agency Business Portal in order to make it more generally available to Agency staff. But more importantly, a web document format permits it to be published in an online form that can be stored on flash drives or CD media for viewing with an Internet browser in file browse mode. This plan will be updated on a regular basis as changes to the computing and networking systems are made. Online publishing makes these changes immediately available to all those who are interested.

Section 1: General Information

Over the years, dependence upon the use of computers in the day-to-day business activities of many organizations has become the norm. The MBA certainly is no exception to this trend. Functions of the MBA depend on the availability of it network of computers.

Consider for a moment the impact of a disaster that prevents the use of the system to process Payroll, Accounting, or any other vital application for days or weeks. It is difficult to estimate the damage to the MBA facilities that such an event might cause. In the Puerto Rico Tropical environment, one Storm could easily cause enough damage to disrupt these and other vital functions. Without adequate planning and preparation to deal with such an event, the MBA Network system could be unavailable for many weeks.

1.1 Primary focus of the Plan

The primary focus of this document is to provide a plan to respond to a disaster that destroys or severely cripples the MBA network systems operated by the Information Systems Department. The intent is to restore operations as quickly as possible with the latest and most up-to-date data available. All disaster recovery plans assume a certain amount of risk. The primary one being how much data is lost in the event of a disaster. There are compromises between the amount of time, effort, and money spent in the planning and preparation of a disaster and the amount of data loss you can sustain and still remain operational following a disaster. Time enters the equation, too. Many organizations simply cannot function without the computers they need to stay in business. So their recovery efforts may focus on quick recovery, or even zero down time, by duplicating and maintaining their computer systems in separate facilities.

The techniques for backup and recovery used in this plan do not guarantee zero data loss. The MBA administration is willing to assume the risk of data loss and do without computing for a period of time in a disaster situation. Data recovery efforts in this plan are targeted at getting the systems up and running with the last available **off-site backup tapes**. Significant effort will be required after the system operation is restored to:

1) Restore data integrity to the point of the disaster.

2) Synchronize that data with any new data collected from the point of the disaster forward.

This plan does not attempt to cover either of these two important aspects of data recovery. Instead, individual users and departments will need to develop their own disaster recovery plans to cope with the unavailability of the network system during the restoration phase of this plan and to cope with potential data loss and synchronization problems.

1.2 Primary objectives of the Plan

This disaster recovery plan has the following primary objectives:

- Present an orderly course of action for restoring critical computing capability to the MBA facilities within 14 days of initiation of the plan.
- Set criteria for making the decision to recover at a Remote Site or repair the affected site.
- Describe an organizational structure for carrying out the plan.
- Provide information concerning personnel that will be required to carry out the plan and the computing expertise required.
- Identify the equipment, floor plan, procedures, and other items necessary for the recovery.

1.3 Overview of the Plan

- *Personnel*

Immediately following the disaster, a planned sequence of events begins. Key personnel are notified and recovery teams are grouped to implement the plan. Personnel currently employed are listed in the plan. However, the plan has been designed to be usable even if some or all of the personnel are unavailable.

In a disaster it must be remembered that PEOPLE are your most valuable resource. The recovery personnel working to restore the computing systems will likely be working at great personal sacrifice, especially in the early hours and days following the disaster. They may have injuries hampering their physical abilities. The loss or injury of a loved one or coworker may affect their emotional ability. They will have physical needs for food, shelter, and sleep.

The MBA must take special care to ensure that the recovery workers are provided with resources to meet their physical and emotional needs. This plan calls for the appointment of a person in the Administrative Support Team whose job will be to secure these resources so they can concentrate on the task at hand.

- *Salvage Operations at Disaster Site*

Early efforts are targeted at protecting and preserving the computer equipment. In particular, any storage media (hard drives, magnetic tapes, flash drives) are identified and either protected from the elements or removed to a clean environment away from the disaster site.

- *Designate Recovery Site*

  A survey of the disaster scene is done by appropriate personnel to estimate the amount of time required to put the facility back into working order. A decision is then made whether to use the Remote Site, a location some distance away from the scene of the disaster where computing and networking capabilities can be temporarily restored until the primary site is ready. Work begins almost immediately at repairing or rebuilding the primary site. This may take months, the details of which are beyond the scope of this document.

- *Purchase New Equipment*

  The recovery process relies heavily upon vendors to quickly provide replacements for the resources that cannot be salvaged. The MBA will rely upon Federal Emergency Procurement Procedures documented in this plan to quickly place orders for equipment, supplies, software, and any other needs.

- *Begin Reassembly at Recovery Site*

  Salvaged and new components are reassembled at the recovery site according to the instructions contained in this plan. Since all plans of this type are subject to the inherent changes that occur in the computer industry, it may become necessary for recovery personnel to deviate from the plan, especially if the plan has not been keep up-to-date. If vendors cannot provide a certain piece of equipment on a timely basis, it may be necessary for the recovery personnel to make last-minute substitutions. After the equipment reassembly phase is complete, the work turns to concentrate on the data recovery procedures.

- *Restore Data from Backups*

  Data recovery relies entirely upon the use of backups stored in locations off-site from the Administrative Building. Backups can take the form of magnetic tape, disk drives, and other storage media. Early data recovery efforts focus on restoring the operating system(s) for each computer system. Next, first line recovery of application and user data from the backup tapes is done. Individual application owners may need to be involved at this point, so teams are assigned for each major application area to ensure that data is restored properly.

- *Restore Applications Data*

  It is at this point that the disaster recovery plans for users and departments (e.g., the application owners) must merge with the completion of the Information Systems plan.

Since some time may have elapsed between the time that the off-site backups were made and the time of the disaster, application owners must have means for restoring each running application database to the point of the disaster. They must also take all new data collected since that point and input it into the application databases. When this process is complete, the MBA computer systems can reopen. Some applications may be available only to a limited few key personnel, while others may be available to anyone who can access the network systems.

- *Move Back to Restored Permanent Facility*

If the recovery process has taken place at the Remote Site, physical restoration of the Administrative Building will have begun. When that facility is ready for occupancy, the systems assembled at the Remote Site are to be moved back to their permanent home.

Section 2: Disaster Planning

2.1 Disaster Risks and Prevention

This portion of the plan reviews the various threats that can lead to a disaster, where our vulnerabilities are, and steps we should take to minimize our risk. The threats covered here are both natural and human-created

- ***Fire***

The threat of fire in the Administrative Building, especially in the System Information area, is very real and poses the highest risk factor of all the causes of disaster mentioned here. The building is filled with electrical devices and connections that could overheat or short out and cause a fire. The computers within the facility also pose a quick target for arson from anyone wishing to disrupt MBA operations.

Preventive Measures

Fire Alarms

The Administrative Building should be equipped with a fire alarm system and smoke detectors scattered widely throughout the building.

Fire Extinguishers

Hand-held fire extinguishers are required in visible locations throughout the building. Staffs are to be trained in the use of fire extinguishers.

Halon System

The System Information room and tape vaults should be protected by a Halon gas fire extinguishing system.

Building Construction

The Administrative Building is built primarily of non-combustible materials. The risk to fire can be reduced when new construction is done, or when office furnishings are purchased, to acquire flame resistant products.

Training and Documentation

Staffs are required to undergo training on proper actions to take in the event of a fire. Staffs are required to demonstrate proficiency in periodic, unscheduled fire drills.

Recommendations

Regular review of the procedures should be conducted to insure that they are up to date. Unannounced drills should be conducted by an impartial administrator and a written evaluation should be produced for the department heads housed in the building.

Regular inspections of the fire prevention equipment are also mandated. Fire extinguishers are periodically inspected as a standard policy, but so should the Halon fire prevention system. Non-disruptive tests of the Halon system should also be conducted. Smoke detectors should be periodically inspected and cleaned.

- ***Flood***

Flood waters penetrating the Information Systems room or any area with electronic equipment can cause a lot of damage. Not only could there be potential disruption of power caused by the water, flood waters can bring in mud and silt that can destroy sensitive electrical connections. Of course, the presence of water in a room with high voltage electrical equipment can pose a threat of electrical shock to personnel within the System Information room or offices.

Preventive Measures

Water detectors will be installed in the Information Systems room and one sump pump will be installed in the machine room.

Recommendations

Periodic inspections of the water detectors are required to ensure their proper operation. Batteries within the detectors must be replaced on a regular schedule.

Operators should be trained in shutdown procedures and drills should be conducted on a regular basis. Also, staff in the machine room should be trained in responding to victims of electrical shock.

- ***Storms and High Winds***

As the MBA facilities is situated along "Storm Alley", damage due to high winds or an actual Storm is a very real possibility. A Storm has the potential for causing the most destructive disaster we face.

Preventive Measures

While a fire can be as destructive as a Storm, there are very few preventative measures that we can take for Storms. Building construction makes a big difference in the ability of a structure to withstand the forces of high winds. The Administrative Building is a strong building, but strong winds are often accompanied by heavy rain, so a double threat of wind and water damage exists so the accessibility of the facilities must be compromise.

Recommendations

All occupants of the Administrative Building should know where the strong points of the building are and directed to seek shelter in threatening weather. The System Information room should be equipped with a weather alert radio.

Computing Services should have large plastic sheeting available in the System Information room area ready to cover sensitive electronic equipment in case the building is damaged. Protective covering should also be deployed over magnetic tape racks to prevent water and wind damage. Operators should be trained how to properly cover the equipment.

• ***Earthquake***

An earthquake has the potential for being the most disruptive for this disaster recovery plan. If the Administrative Building is damaged, it is highly probable that the Remote Site may also be similarly affected (due to the small territorial extension of Puerto Rico). Restoration of computing and networking facilities following a bad earthquake could be very difficult and require an extended period of time due to the need to do wide scale building repairs.

Preventive Measures

The preventative measures for an earthquake can be similar to those of a Storm. Building construction makes all the difference in whether the facility will survive or not. Even if the building survives, earthquakes can interrupt power and other utilities for an extended period of time. Standby power generators could be purchased or leased to provide power while commercial utilities are restored.

Recommendations

Computing Services should have larger plastic sheeting available in the machine room area ready to cover sensitive electronic equipment in case the building is damaged. Protective covering should also be deployed over magnetic tape racks to prevent water and wind damage. Operators should be trained how to proper cover the equipment.

• ***Computer Crime***

Computer crime is becoming more of a threat as systems become more complex and access is more highly distributed. With the new networking technologies, more potential for improper access is present than ever before.

Computer crime usually does not affect hardware in a destructive manner. It may be more insidious, and may often come from within. A disgruntled employee can build viruses or time bombs into applications and systems code. A well-intentioned employee can make coding errors that affect data integrity (not considered a crime, of course, unless the employee deliberately sabotaged programs and data).

Preventive Measures

MBA systems have security products installed to protect against unauthorized entry. All systems are protected by passwords, especially those permitting updates to data. All users are required to change their passwords on a regular basis. All security systems should log invalid attempts to access data, and security administrators review these logs on a regular basis.

All systems are backed up on a periodic basis. Those backups are stored in an area separate from the original data. Physical security of the data storage area for backups must be implemented. Standards are established on the number of backup cycles to retain and the length of their retention.

Recommendations

Continue to improve security functions on all platforms. Strictly enforce policies and procedures when violations are detected. Regularly let users know the importance of keeping their passwords secret. Let users know how to choose strong passwords that are very difficult to guess. Improve network security. Shared wire media Ethernet are susceptible to sniffing activities, which unscrupulous users may use to capture passwords. Implement stronger security mechanisms over the network, such as one-time passwords, data encryption, and non-shared wire media.

- ***<u>Terroristic Action and Sabotage</u>***

The MBA Administrative Facilities are always potential targets for terroristic actions, such as a bomb. The threat of kidnapping of key personnel also exists.

Preventive Measures

Good physical security is extremely important. However, terroristic actions can often occur regardless of in-building security, and they can be very destructive. A bomb placed next to an exterior wall of the System Information room will likely breach the wall and cause damage within the room.

Given the freedom that we enjoy as a United States Territory, almost no one will accept the wide-scale planning, restrictions, and costs that would be necessary to protect the Administrative Building from a bomb. Some commonsense measures can help, however.

The building should be adequately lit at night on all sides. All doors into the System Information room area should be strong and have good locks. Entrances into the machine room proper should