Amherst County Public Schools
Technology Support Group
Disaster Recovery Plan

Introduction

This document is the disaster recovery plan for Amherst County Public Schools, Technology Support Group. The information present in this plan guides administrators and technical staff in the recovery of computing and network facilities operated by ACPS 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 Technology Center located at 257 Trojan Road. Each supported computing platform has a section containing 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.

General Information About The Plan

Over the years, dependence upon the use of computers in the day-to-day business activities of many organizations has become the norm. Amherst County Public Schools certainly is no exception to this trend. These machines are linked together by a sophisticated network that provides communications with other machines across our locations and around the world. Vital functions of ACPS depend on the availability of this network of computers.

Consider for a moment the impact of a disaster that prevents the use of the system to process Student Registration, Payroll, Accounting, or any other vital application for weeks. Students and faculty rely upon our systems for instruction and research purposes, all of which are important to the well-being of ACPS. It is hard to estimate the damage to the Division that such an event might cause. One tornado properly placed could easily cause enough damage to disrupt these and other vital functions of the Division. Without adequate planning and preparation to deal with such an event, the Division's central computer systems could be unavailable for many weeks.

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 Division's central computer systems. 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. Disaster recovery planning is much like the insurance business in many ways. 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 Division's 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. Significant effort will be required after the system operation is restored to (1) restore data integrity to the point of the disaster and (2) to 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 computer systems during the restoration phase of this plan and to cope with potential data loss and synchronization problems.

Primary Objectives of the Plan

This disaster recovery plan has the following primary objectives:

1. Present an orderly course of action for restoring critical computing capability to the ACPS Division.
2. Set criteria for making the decision to recover at a cold site or repair the affected site.
3. Describe an organizational structure for carrying out the plan.
4. Provide information concerning personnel that will be required to carry out the plan and the computing expertise required.
5. Identify the equipment, floor plan, procedures, and other items necessary for the recovery.

OVERVIEW of the Plan

This plan uses a "cookbook" approach to recovery from a disaster that destroys or severely cripples the computing resources at the Technology Center at 257 Trojan Road and possibly at other critical ACPS locations.

Personnel
Immediately following the disaster, a planned sequence of events begins. Key personnel are notified and recovery teams are grouped to implement the plan. Key departments are listed in the plan.

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 Division must take special pains 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 School Administration Office 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 magnetic storage media (hard drives) and critical hardware (routers, core switches, etc.) are identified and either protected from the elements or removed to a clean, dry environment away from the disaster site. The School Board office or Amherst Education Center will work.

Designate Recovery Site
At the same time, a survey of the disaster scene is done by appropriate personnel to estimate the amount of time required to put the facility (in this case, the building and utilities) back into working order. A decision is then made whether to use the Cold 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 Division will rely upon emergency procurement procedures requested in this plan and approved by the Division’s purchasing office 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 Technology Center. Backups can take the form of external hard 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 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 Technology Support Group's 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 Division's computer systems can reopen for business. Some applications may be available only to a limited few key personnel, while others may be available to anyone who can access the computer systems.

Move Back to Restored Permanent Facility

If the recovery process has taken place at the Cold Site, physical restoration of the Technology Center (or an alternate facility) will have begun. When that facility is ready for occupancy, the systems assembled at the Cold Site are to be moved back to their permanent home. This plan does not attempt to address the logistics of this move, which should be vastly less complicated than the work done to do the recovery at the Cold Site.

Disaster Risks and Prevention

As important as having a disaster recovery plan is, taking measures to prevent a disaster or to mitigate its effects beforehand is even more important. 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 Technology Center 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 Division operations. Wide area fires, such as those common in recent years in California, are also a possibility in dry times.

<u>Preventive Measures</u>

Fire Extinguishers
Hand-held fire extinguishers are required in visible locations throughout the building.

Building Construction
Monelison Middle School 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
Staff are required to demonstrate proficiency in periodic, unscheduled fire drills.

<u>Recommendations</u>

The Technology Center should be equipped with a fire alarm system, with ceiling-mounted smoke detectors scattered widely throughout the building. Smoke detectors should also be placed in the server room.

The server room should be protected by a Halon gas fire extinguishing system. Further, the ceiling-mounted sprinklers should be removed or disconnected.

Regular review of the procedures should be conducted to insure that they are up to date. 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 located in the Technology Center should be periodically inspected and tested.

FLOOD

Per FEMA's website, Monelison is not in a flood zone. However, we are close to a boundary dividing special flood hazard areas of different base flood elevations, flood depths, or flood velocities. These factors coupled with the chance of a storm that drops large amounts of rain in the Madison Heights area create the threat of flooding. Flood waters penetrating the server room 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 machine room.

Preventive Measures

Recommendations

Install a water detection system in the server room that would alert key personnel. And periodic inspections of the water detectors are also required to ensure their proper operation.

Staff in the server room should be trained in shutdown procedures.

TORNADOS AND HIGH WINDS

A tornado has the potential for causing the most destructive disaster we face.

Preventive Measures

While a fire can be as destructive as a tornado, there are very few preventative measures that we can take for tornados. Building construction makes a big difference in the ability of a structure to withstand the forces of high winds. Are any areas such as a flat roof susceptible to wind damage? Strong winds are often accompanied by heavy rain, so a double threat of wind and water damage exists if the integrity of the roof is lost.

Recommendations

All occupants at Monelison Middle should know where the strong points of the building are and directed to seek shelter in threatening weather.

The Technology Center should have large tarpaulin or plastic sheeting available in the server room area ready to cover sensitive electronic equipment in case the building is damaged. Protective covering should also be deployed over all racks to prevent water and wind damage. Operators should be trained how to properly cover the equipment.

EARTHQUAKE

The threat of an earthquake in the Madison Heights area is low, but should not be ignored. According to vaemergency.gov, Virginia has had 11 earthquakes in 107 years. Buildings in our area are not built to

earthquake resistant standards like they are in quake-prone areas like California. So we could expect light to moderate damage from the predicted quake.

An earthquake has the potential for being the most disruptive for this disaster recovery plan. If the Technology Center is damaged, it is highly probable that the cold site nearby may also be similarly affected. 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 tornado. 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

The Technology Center should have large tarpaulin or 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 all 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

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

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

Recommendations

Implement a password change policy. Administration should support and encourage a password change policy. The amount of time required to change a password is small compared to the time required to investigate a data breach.

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. Implement stronger security mechanisms over the network, such as one-time passwords, data encryption, and non-shared wire media.

TERRORISTIC ACTION AND SABOTAGE

The Division's computer systems 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 server room will likely breach the wall and cause damage within the room.

Given the freedom that we enjoy within the United States at this time, almost no one will accept the wide-scale planning, restrictions, and costs that would be necessary to protect the Technology Center from a bomb. Some commonsense measures can help, however.

The building should be adequately lit at night on all sides. All doors into the server room area should be strong and have good locks. Entrances into the server room proper should be locked at all times. Only those people with proper security clearances should be permitted into the serve 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).

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

Recommendations

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 the Technology Support Group 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 Division.

For instance, if the Administration Building were to be involved in the same disaster as the Technology Center, the functions of the Business Manager's Office, or more in particular, the Purchasing Office, could be severely affected. Without access to the appropriate procedures, documents, vendor lists, and approval processes, the Technology Support Group recovery process could be hampered by delays while Purchasing recovers.

Every other business unit within the Division should develop a plan on how they will conduct business, both in the event of a disaster in their own building or a disaster at the Technology Center that removes their access to data for a period of time. Those business units 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.

If the Technology Center 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 Division has a number of options for alternate sites, each having a varying degree of up-front costs.

Hot Site
This is probably the most expensive option for being prepared for a disaster, and is typically most appropriate for very large organizations. A separate computer facility, possibly even 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 communications lines so that users at the primary campus can continue to access the computers from their offices and classrooms.

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 bitter pill that no one should swallow.

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. A partnership with the County of Amherst IT would probably be our only choice.

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. And they can be used in conjunction with other arrangements, such as the use of a cold recovery site described below. 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.

Cold Site

A cold recovery site is an area physically separate from the primary site where space has been identified for use as the temporary home for the Technology Group while the primary site is being repaired. There are varying degrees of "coldness", ranging from an unfinished basement all the way to space where the necessary raised flooring, electrical hookups, and cooling capacity have already been installed, just waiting for the computers to arrive.

The Technology Support group recommends using the cold site approach for this disaster recovery plan. The necessary agreements have been made for the Technology Support Group to utilize space in Amherst Education Center as its Cold Site or off-site location. It has adequate space to house the

hardware, with some office space available for operating and technical personnel. It has good connectivity to the Division's fiber optic network. A certain amount of preparation needs to be made for electrical and cooling capacity to support mainframes and network equipment.

Replacement Equipment

This plan contains an 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 have been 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 Technology Support Group will hopefully be able 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 Technology Center 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. This option is typically limited to mainframe disk systems only.

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 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. Another huge advantage is that backups can be made from mainframes, file servers,

distributed (unix-based) systems, and personal computers. 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.

Hybrid Off-Site Backup Storage

The Technology Support Group has opted to taking periodic backups of its databases, and file servers and storing those backups at Amherst Education Center.

Personnel and Organizational Chart – Who is effected and who is responsible for synchronization of data after a restore as close to the date of disaster as possible.

ACPS Website – All Staff, Technology Support Group
Active Directory – All Staff, Technology Support Group
AS400 – Business, Finance, Payroll, Technology Support Group
Destiny – Librarian, Technology Support Group
Internet Access/WAN Access – All Staff, Technology Support Group
Phone System – All Staff, Technology Support Group
Point of Sale – Child Nutrition, Technology Support Group
PowerSchool – All Staff, Technology Support Group
Ren Place – All Staff, Technology Support Group
School Level Files – All Staff, Technology Support Group
School Websites – All Staff, Technology Support Group
TransFinder – Transportation, Technology Support Group