Northern Oklahoma College

Disaster Recovery Plan

Revised 9/26/2023

Table of Contents

Northern Oklahoma College
Information Technology
Disaster Recovery Plan

Introduction

This document is the disaster recovery plan for Northern Oklahoma College, Information Technology. The information present in this plan guides administration and technical staff in the recovery of computing and network facilities operated by I.T. 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 in or at the Information Technology facility at 1220 E. Grand, Tonkawa, OK. There are sections that document the personnel that will be needed to perform the recovery tasks and an organizational structure for the recovery process.

As changes to the computing systems are made, this plan will be updated to indicate those changes.

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 computer systems of Northern Oklahoma College. 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 one can sustain and still remain operational following a disaster. Many organizations cannot function without their computers 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. 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 latest available off-site data. 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 Northern's campus.
2. Describe an organizational structure for carrying out the plan.
3. Provide information concerning personnel that will be required to carry out the plan and the computing expertise required.
4. Identify the equipment, procedures, and other items necessary for the recovery.

Overview of the Plan

Personnel

Immediately following a disaster, key personnel are notified and recovery teams are grouped to implement the plan. The plan has been designed to be usable even if some or all of the current, employed personnel are unavailable.

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. Depending on the disaster, they may have injuries affecting their physical abilities, the loss or injury of a loved one may affect their emotional ability, and they will have physical needs for food, shelter, and sleep.

Northern Oklahoma College must 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 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, magnetic tapes) are identified and either protected from the elements or removed to a clean, dry environment away from the disaster site.

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 back into working order. A decision is then made whether to use a location away from the scene of the disaster where computing and networking capabilities can be temporarily restored until the primary site is ready. Each NOC campus is outfitted with an analog (not on network) phone located in its main campus boardroom.

Purchase New Equipment

The recovery process relies heavily upon vendors to quickly provide replacements for the resources that cannot be salvaged. The college will rely upon emergency procurement procedures approved by the 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. 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 concentrating on the data recovery procedures.

Restore Data from Backups

Data recovery relies entirely upon the use of backups stored in locations off campus. First efforts focus on restoring the operating system(s) for each computer system. The recovery of application and user data from the backup directories 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

At this point the disaster recovery plans for users and departments (the application owners) must merge with the completion of the I.T. plan. Since 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, Northern Oklahoma College can reopen. Some applications may be available only to key personnel, while others may be available to all users.

Move Back to Restored Permanent Facility

When the permanent facility is ready for occupancy, the systems assembled at the far site are to be moved back to their permanent home. The logistics of this move will not be addressed.

Risks and Prevention

Taking measures to prevent a disaster is important. This portion of the plan reviews the various threats that can lead to a disaster, our vulnerabilities, and steps we should take to minimize our risk.

FIRE

The threat of fire in the Administration building posses 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 the college's operations.

Preventive Measures

Fire Alarms

The Administration building is equipped with a fire alarm system, with ceiling-mounted smoke detectors scattered widely throughout the building. The building is equipped with a sprinkler system.

Fire Extinguishers

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

Building Construction

The building is built primarily of non-combustible materials—concrete and sheet rock. 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

Detailed instructions on how to handle a situation concerning fire are present in The Campus Emergency Procedures Guide. Staff are trained on proper actions to take in the event of a fire.

Recommendations

A periodic review of the procedures should be conducted to ensure that they are current and up to date. Regular inspections of the fire prevention equipment are mandatory. Fire extinguishers and smoke detectors are periodically inspected as a standard policy.

FLOOD

Flood waters penetrating the server room can cause substantial damage. There could be potential disruption of power caused by the water and mud and silt that can destroy sensitive electrical connections. The presence of water in a room with high voltage electrical equipment can pose a threat of electrical shock to personnel within the room.

Preventive Measures

Our server equipment is housed in racks and shelving which are located off of the floor to help prevent water damage. The server room is equipped with a monitoring device that will alert I.T. personnel when the water reaches a certain level. The I.T. department is trained in shutdown procedures and other steps to remove equipment from water damaged areas.

TORNADOS AND HIGH WINDS

Damage due to high winds or an actual tornado is a very real possibility.

Preventive Measures

There are few preventive measures that we can take for tornados. Building construction will make a difference in the ability of a structure to withstand tornadic winds. Our Administration building has a basement that is designated as a storm shelter for the campus as well as the community. The I.T. server room is located in this area.

The I.T. Department has large 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 magnetic tape racks to prevent water and wind damage. Employees are trained how to properly cover the equipment. Northern Oklahoma College does have a large generator located between the Administration building and the Kinzer Performing Arts building. This generator provides power to NOC’s main server room allowing for critical services to stay up and available. This also allows for the connection to stay up between campus locations. Generator should be serviced once a month.

EARTHQUAKE

The threat of an earthquake in Northern Oklahoma is low. If the Administration building is damaged, it is highly probable that the entire campus and surrounding area may also be similarly affected. Recovery of the 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 repairs.

Preventive Measures

Earthquakes and tornados have similar preventative measures. Building construction is important as to whether the facility will survive or not. Even if the building survives, earthquakes can interrupt power and other utilities so standby power generators could be purchased or leased to provide power while commercial utilities are restored. Northern Oklahoma College does have a large generator located between the Administration building and the Kinzer Performing Arts building. This generator provides power to NOC's main server room allowing for critical services to stay up and available. This also allows for the connection to stay up between campus locations. Generator should be serviced once a month.

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.

Preventive Measures

All 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 at a minimum of every 90 days. All security systems log invalid attempts to access data and security administrators check these logs regularly.

Network traffic within the datacenter is isolated by VLAN/subnet. Northern's network traffic is protected with firewalls, security groups and access control lists (ACLs). Data traffic from the data center to the campus is usually sent over an IPsec point-to-point virtual private network (VPN).

We continue to improve security functions on all platforms, regularly remind and train users of the importance of keeping their passwords secret, and continue to improve network security.

TERRORIST ACTION AND SABOTAGE

The college's computer systems are always potential targets for terrorist actions, such as a bomb. The threat of kidnapping of key personnel also exists.

Preventive Measures

Terrorist 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.

The building is adequately lit at night on all sides. All doors leading into the server room are strong and continually locked with access granted only to I.T. employees and a few key personnel. Only those people with proper security clearances are permitted into the server room area. Suspicious parties are reported to security and/or the police.

Backups

Backups for the Student Data Mainframe and the Document Management System done using various types.

Full Volume/Remote Backup Services

Student Data Mainframe (Jenzabar Hosted SaaS)
In a catastrophic situation (server is lost), the restoration process would occur from the point in time of the last full backup of the server (which typically occurs during the late evening/early morning hours). If a server is lost (the SAN remains operational), then the SQL Server logs can also be restored to a more recent point-in-time to minimize any data loss from transactions completed since the point of the full backup. If the data center were totally destroyed (the SAN included), then the systems would be restored to a secondary data center from the last full backup that is located/maintained at a secondary facility.

All Data centers that we use have N+1 Redundancy and are 'purpose built' facilities (to withstand most threats including storms, floods, fires, etc.)

As a standard practice, Jenzabar maintains a 30-day rolling back up procedure. Clients may optionally elect to have additional/more frequent, or longer retention periods for backup. In this case Jenzabar will work with the customer to determine the special backup procedure and provide any associated costs to implement the requested process.

Document Management System
Full volume backups are done remotely each Sunday. Northern's contracted vendor, BIS (Business Imaging Systems) provides access to a remote copy of the images within hours of a disaster. This facilitates the recovery of images and applications stored at a remote and secure site in the event of a disaster. The connection is a WatchGuard appliance that uses IPSEC encryption. Once the data is copied to the BIS network in Oklahoma City, the volume where the data is stored is replicated to our DR site in Tulsa. In the event of a catastrophic event, BIS would attach a copy of the SQL backup and provide access within 24 hours.

Safety Personnel

These people are to be contacted as soon as a disaster is threatened or strikes.
Emergency Fire, Ambulance, Police dial: 911 (on or off campus)
Campus Security dial: Tonkawa - (580) 628-6277; Enid – (580) 977-9448; Stillwater (405) 744-4196

Information Technology Primary Contact List

Mike Machia, Director of Information and Instructional Technology Services
Office (580) 628-6267
Cell (580) 478-2115
Email michael.machia@noc.edu

Linn Laughrey, Network/Server Administrator
Office (580) 628-6332
Cell (580) 628-1978
Email jeff.foss@noc.edu

Shannon Lorg, Webmaster
Office (580) 628-6330
Cell (580) 767-0100
Email shannon.lorg@noc.edu

Jay Schnoebelen (Vendor)
Jenzabar
Office (918) 437-4920 (ext. 67208)
Tulsa, OK 74136
Email jay.schnoebelen@jenzabar.com

Jared Bryant (Vendor)
BIS
Office (405) 418-7433
Edmond, OK 73013
Email jbryant@bisok.com

Recovery Team

The selection of the members of the Recovery 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 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.

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.

Protection

It is important that any equipment, media, paper, and other items at the disaster site be protected to avoid any further damage as some may be salvageable or repairable and save time in restoring operations.

- Cover all computer equipment.
- Cover all undamaged paper.
- Ask the NOC Security officer or local police to patrol the site to prevent looting or scavenging.
- Supplies and any equipment that might be salvageable needs to be moved to a secure location.

Damage Assessment

Damage assessment is intended to establish the extent of damage to hardware and the facility where it is located. We need to determine where the recovery should take place and what equipment must be ordered immediately.

The Recovery Team should be liberal in their estimate of the time required to repair or replace damaged resources. They must take into consideration cases where one repair cannot begin until another is completed. Estimates of repair time should include ordering, shipping, installation, and testing time.

Evaluation of damage to the building structure, electrical system, heat and air systems, and building network should be conducted. If time estimates indicate that recovery at the original site will require more than 14 days, a remote location will be used.

Maintaining the Plan

Having a disaster recovery plan is critical and it should be routinely evaluated once each year. All portions of the plan will be reviewed by the Information Technology Department. As changes occur at Northern Oklahoma College, I.T. management will determine if changes to the plan are necessary.

Changes that affect recovery will be made by the management in the department. After the changes have been made, each department employee, technical or not, will be advised that the updated documents are available. The changes will be incorporated into the body of the plan and distributed as needed.