Southwestern Oregon Community College
Integrated Technology Services
Disaster Recovery Plan

Last update: July 2021

Introduction

This document is the disaster recovery plan for Southwestern Oregon Community College, Integrated Technology Services Department. The information present in this plan guides College management and technical staff in the recovery of computing, network, and phone facilities operated by Integrated Technology Services 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 Integrated Technology Services facility in Randolph Hall server room or phone and network switch room. 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 updated on a regular basis as changes to the computing and networking systems are made.

The Disaster Recovery Plan

Section 1: General Information About The Plan

- Objectives and Overview

Section 2: Disaster Planning

- Disaster Risks and Prevention
- Disaster Preparation
- Backup Procedures
- Systems Configuration

Section 3: Initiation of Emergency Procedures

- Safety Issues
- Disaster Notification List
- Disaster Recovery Teams
- Activating the Disaster Recovery Plan
- Equipment Protection and Salvage
- Damage Assessment
- Emergency Requisition Procedures

Section 4: Initiation of Recovery Procedures

- Cold Site Preparation
- Platform Recovery Procedures
- Applications Recovery Procedures
- Critical Applications

Section 5: Maintaining the Plan

- Maintaining the Plan
- Document Numbers

Section 6: Attachments

- Windows Recovery Documentation
- Windows Servers Configuration

Section 1: Disaster Recovery Plan Objectives and Overview

Last update: July 2021

Over the years, dependence upon the use of computers in the day-to-day business activities of many organizations has become the norm. Southwestern Oregon Community College certainly is no exception to this trend. Today you can find very powerful computers in every department on campus. These machines are linked together by a sophisticated network that provides communications with other machines across campus. Vital functions of the College 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, all of which are important to the well-being of the

College. It is hard to estimate the damage to the College that such an event might cause. One fire properly placed could easily cause enough damage to disrupt these and other vital functions of the College. Without adequate planning and preparation to deal with such an event, the College'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 College's central computer systems operated by the Integrated Technology Services Department. The intent is to restore operations as quickly as possible with the latest and most up-to-date data available.

IMPORTANT NOTE!

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 College administration is willing to assume the risk of data loss and do without computing for a period of time in a disaster situation. To put it in a more fiscal sense, the College is saving dollars in up-front disaster preparation costs, and then relying upon business interruption and recovery insurance to help restore computer operations after a disaster.

Data recovery efforts in this plan are targeted at getting the systems up and running with the last available off-site data 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 campus within 14 days of initiation of the plan.
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 Randolph Hall on the Coos Bay Campus.

Personnel

Immediately following the disaster, a planned sequence of events begins. Key personnel are notified and recovery personnel are grouped to implement the plan. Personnel currently employed 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 will have physical needs for food, shelter, and sleep. The College must take special pains to ensure that the recovery workers are provided with resources to meet their physical and emotional needs.

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 (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 College will rely upon emergency procurement

procedures documented in this plan and approved by the College's purchasing office to quickly place orders for equipment, supplies, software, and any other needs. An inventory of the switch room, which includes the core switch, network appliances, firewalls and the pbx VOIP server and voicemail server will be kept in the fireproof safe in Randolph 3. An inventory of the server room, which includes the physical servers, the SAN and the UPS will be kept in the fireproof safe in Randolph.

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 kept 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 upon the use of backups stored in locations either at the disaster site or off-site from the Randolph Hall Building. Backups can take the form of magnetic tape, disk drives or cloud storage. Early data recovery efforts focus on restoring the operating system(s) for each computer system. Next, first line recovery of application and data from the backup tapes is done. Network and phone configuration data is on disk and in system and network administrators' possession.

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 Integrated Technology Services plan. They must take all new data collected since that point and input it into the application databases. When this process is complete, the College 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 Randolph Hall (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.

Section 2: Disaster Recovery Plan

Disaster Risks and Prevention

Last update: July 2021

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
- Flood
- High Winds
- Earthquake
- Computer Crime
- Terrorist Actions and Sabotage

FIRE

The threat of fire in the Randolph Hall, especially in the machine room 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. Not to be forgotten are the hydrogen gas producing batteries in the Uninterruptible Power Supply room where a spark could ignite a fire and explosion.

The computers within the facility also pose a quick target for arson from anyone wishing to disrupt College operations.

Preventive Measures

Backup Power Systems

The college has invested in a very large propane powered power generator that is directly wired into Randolph Hall switch room and server room. This system is tested once a week.

Fire Alarms

The Randolph Hall is equipped with a fire alarm system, with ceiling-mounted smoke detectors in the server and switch rooms. The server room has environment monitoring equipment that includes temperature, smoke and loss of power alarms. ITS personnel are automatically notified of any alarm events.

Fire Extinguishers

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

Fire Suppression System

The machine room and switch room are protected by a fire suppression extinguishing system.

Building Construction

Randolph Hall is not built primarily of non-combustible materials. The risk of 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 for dealing with fire are present in Emergency Evacuation Procedures documentation. Staff are not required to undergo training on proper actions to take in the event of a fire. Staff are not required to demonstrate proficiency in periodic, unscheduled fire drills.

A one or two hour fire proof safe has been purchased for storing of on-site Randolph Hall server room backup tapes.

Recommendations

Fire detectors and fire alarms should be installed throughout the building. Staff should be required to undergo training on proper actions to take in the event of a fire and to demonstrate proficiency in periodic, unscheduled fire drills.

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.

FLOOD

The chance of a storm that drops enough water to cause a disaster is very unlikely. Except for power outages, the College has weathered very severe storms with very little disruption of IT services.

Preventive Measures

Backup Power Systems

The college has invested in a very large propane powered power generator that is directly wired into Randolph Hall switch room and server room. This system is tested once a week. We also have a large battery backup that will provide 16 minutes of power for all servers and the phone switch. The generator will start within 10 seconds if there is an outage.

HIGH WINDS

As Southwestern Oregon Community College is situated on the Oregon Coast and high winds are a very real possibility. However, high winds do not have very much potential for causing a major disaster. They do have potential for causing power outages.

Preventive Measures

Backup Power Systems

The college has invested in a very large propane powered power generator that is directly wired into Randolph Hall switch room and server room. This system is tested once a week. We also have a large battery backup that will provide 30 minutes of power for all servers and the phone switch. The generator will start within 10 seconds if there is an outage.

EARTHQUAKE

The threat of an earthquake in the Coos Bay area is high. Scientists have predicted that a large earthquake along the San Andreas fault may happen any time in the next 50 years, and that its effects will be felt as far away as our area. 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 Randolph Hall is damaged, it is highly probable that the Cold Site on campus 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

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. The Cold Site should be situated in a building built to the latest earthquake codes.

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, the proliferation of iPads and smartphones, more potential for improper access is present than ever before.

The data breach incident response plan shall be followed in the event of a data breach.

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 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 should review these logs on a regular basis. Network access control is enforced by a security appliance. The NAC validates a device before it is allowed network access.

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

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, such as 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. A new more effective firewall has been put in place. All users are required to authenticate before gaining access to the wireless network. Peer2Peer traffic is a source of virus and Trojan infections. The college employs hardware and software to stop this kind of traffic.

TERRORISTIC ACTION AND SABOTAGE

The College's computer systems are potential targets by disgruntled employees and for terrorist actions, such as a bomb.

Preventive Measures

Good physical security is extremely important. However, 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.

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 Randolph Hall 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 server 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).

The server room has a security lock installed. Only those employees that need to be in the server or switch rooms have access.

Recommendations

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 their access monitored.

Disaster Recovery Plan

Disaster Preparation

Last update: July 2021

In order to facilitate recovery from a disaster which destroys all or part of the server room in the Randolph Hall, certain preparations have to be made in advance. This document describes what will be done to lay the way for a quick and orderly restoration of the facilities that Integrated Technology Services operates.

The following topics are presented in this document:

- Disaster Recovery Planning
- Recovery Facility
- Replacement Equipment
- Backups
- Disaster Lock Boxes

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 Integrated Technology 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 College.

For instance, if Tioga Hall or Dellwood Hall were to be involved in the same disaster as the Randolph Hall, 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 Integrated Technology Services recovery process could be hampered by delays while Purchasing recovers.

Every other business unit within the College 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 Integrated Technology Services 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 manually tracked until the system can be restored. 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 Integrated Technology 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 College 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.

Cloud Storage

Cloud storage could be utilized. This would hold a copy of our data on the cloud vendor's servers. Our data would be continuously backed up. In the event of a disaster, the data will be available for recovery when the hardware is restored.

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 <u>not</u> 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.)

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 computer and network systems 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.

Southwestern Oregon Community College has chosen to use the cold site approach for this disaster recovery plan. Integrated Technology Services plans to utilize space in the Student Recreation Center as its Cold Site. It has adequate space to house the hardware, with some office space available for operating and technical personnel. It has good connectivity to the campus fiber optic network. And a certain amount of preparation will be made for electrical and cooling capacity to support mainframes and network equipment. This work has not been done because of budget constraints. The actual work that needs to be done to renovate the space to be ready to receive the computer equipment is available in the Section Recovery at the Cold Site.

Replacement Equipment

This plan will contain 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 need to 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. The first two options, Remote Dual Copy, and Automated Off-Site Tape Backup, are not implemented at this time. They require additional equipment and setup. Cloud Storage is our primary recovery option.

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. 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 (the campus 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.

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 cluster servers, file servers, distributed file systems, and personal computers. Although such a system is expensive, it is not prohibitively so.

Cloud Storage

Cloud storage is currently being used to back up the production data of the ERP system. This is being done once per week.

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.

Some organizations contract with disaster recovery companies to store their backup tapes in hardened storage facilities. These can be in old salt mines or deep within a mountain cavern. 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.

The College has opted to taking periodic backups of its primary mainframe system and servers and storing those backups in two locations. The primary storage location is in Randolph Hall Room 3 which is adjacent to the server room. The second location utilizes cloud storage for the college ERP data.

In general, backups for each subsystem are cycled through the two storage locations. Backups are initially placed in the Integrated Technology Services tape storage cabinet and weekly full backups are made to the cloud storage location.

The actual backup and cycling procedures vary somewhat depending on the computer platform. Details of these procedures are contained in the following document:

Disaster Plan Locations

To ensure that an up-to-date copy of this plan is available when a disaster occurs, procedures will be established to store a copy of the plan with other important recovery information at the Off Site backup tape storage area. Two sites will be designated to hold these materials. The contents of both sites are identical. One resides at the bank site; the other resides in the tape vault in R3 in Randolph Hall.

When changes to the contents are necessary, the plan at the Randolph Hall is first updated, and then it is delivered to the bank site and swapped with the plan stored there. That plan is returned to Randolph Hall and updated and replaced in the tape vault. This ensures that at least one copy of the plan is available at the recovery site.

The plans are to be secured at all times. Access to the plans are provided to several key people within the department, including:

- CIO of Integrated Technology Services – Rocky Lavoie
- Disaster Recovery Plan Coordinator – Jeff Whitey

The contents of the bank vault and the safe in Randolph will contain this plan, configuration information, and attachments.

Disaster Recovery Plan

Backup Procedures

Last update: July 2021

Every system that Integrated Technology Services operates is backed up regularly. The backup media for each of these systems is relocated to the storage vault in Randolph Hall.

Two sets of backups for the ERP exist at any one time. The most recent backups are stored in the vault of Randolph Hall. The second most recent are utilizing cloud storage.

The procedures for making the backups for each individual computer system differs. 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.

The following documents describe in detail the regular backup procedures and cycles for each of the computer platforms.

- Jenzabar Backups
- Windows 2003, 2008 and 2012 Server Backups
- Cisco Network Equip Backups

Disaster Recovery Backups

Backup Procedures
SQL Jenzabar server

Backups for the Jenzabar system are single Ultrium backup tapes. Full normal backups are created Monday through Friday at 11:59/pm. Every Sunday an incremental backup is transferred to the cloud storage site.

Windows Servers:
Windows servers are being transitioned to virtual servers. The virtual hard drive for each server is backed up. This allows complete recovery of the Windows network. Backups are kept in the media safe in R3. Full and incremental backups of the windows servers are stored in the media safe in R3.
Full Volume Backups

Network Configuration Backups:

Switch configuration backups are made periodically when changes to the configuration occur. Copies of the configuration files of network equipment are kept on a cd and stored in the media safe in R3.

Section 3: Disaster Recovery Plan

Initiation of Emergency Procedures

Last update: July 2021

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 Randolph Hall. 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 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 room located in the extreme northwest corner of the first floor of the building. 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.
- Propane and natural gas – The Randolph heating system uses a natural gas boiler. The boiler is equipped with auto shutoff devices. The meter and building shutoff is located on the north east end of the building. The generator runs off of propane. The tank and shutoff is located at the south east corner of the building.

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 HAZMAT 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.

PTSD - Post-traumatic Stress Disorder 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. Symptoms usually manifest themselves as:

Intrusions

The individual experiences flashbacks or nightmares where the traumatic event is re-experienced.

Avoidance

The individual tries to reduce exposure to people or things that might bring on their intrusive symptoms.

Hyper-arousal

The individual exhibits physiologic signs of increased arousal, such as hyper vigilance or increased startle response.

Disaster Notification List

Last update: July 2021

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

Safety Personnel

	On Campus Dial	Off Campus Dial
Emergency Fire, Ambulance, Rescue, Police, and HAZMAT	7911 or 9-911	911
Public Safety	7399	888-7399
Physical Plant Service Desk	7250	888-7250

Integrated Technology Services Primary Notification List

Person	Title	Phone Number
VACANT	CIO/IT Director	
John Taylor	Interim ITS Manager/Network Administrator	541-217-4208

Vacant	Resource Planning Systems Administrator	541-294-5752
James Chilson	Programmer Specialist	541-271-1957
Vacant	Web Systems Specialist	541-217-6102
Dallas Petenbrink	Media Services & Help Desk Manager	541-404-6068
Heather Balogh	Enterprise Information System Administrator	541-294-4081
Brian Parker	Windows System Administrator	541-404-7469

Recovery Manager

This individual needs to be a skilled manager/administrator who is accustomed to dealing with pressure situations. They should have a broad knowledge of the hardware and software in use at the site. They should be a "problem solver" as there will be many problems arise that have not been anticipated in advance. They must be able to delegate responsibility to others. They must also have signature authority to expend funds as a part of the disaster recovery process. The current Director of ITS is the first choice for the Recovery Manager.

Facilities Coordinator

This individual needs some of the same skills as the Recovery Manager. However, she also needs to be familiar with the process of getting construction work scheduled and completed on time. She 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. They must have a strong background in the setup and interfacing of as many of the platforms in use as possible. They 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. They must also be able to schedule and manage people.

Administrative Coordinator

This individual needs to be skilled in the business operations of the College and the State of Oregon. She/He should be well acquainted with the day-to-day operations of a College department. She/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 State purchasing procedures and contracts.

Network Coordinator

This individual needs to be skilled in the area of network design and maintenance. She/He should be trained in diagnosing and correcting network outages and in connecting and debugging new additions to an existing network.

Applications Coordinator

First choice for this individual would be someone from the existing application support group. The person should have exposure to a cross section of the currently used applications. The most critical areas are Payroll, Accounting, and Student Records. If no one from the current staff is available, the most important technical skills are: Jenzabar application experience, and experience testing and debugging applications developed for them. The person will need to use available tools to ascertain the status of files and data base objects and be prepared to restore later versions from backups if required. She/He will also need to interface with users to verify that applications are functioning as expected or analyze and develop solutions to problems that arise.

The following table contains a sample list of the people currently employed who could fill the positions on the Recovery Management Team. Alternates are listed, but there are other qualified individuals who could step in should any of these persons not be available.

Disaster Recovery Team

Last update: July 2021

Selecting Personnel for the Recovery Management Team

Sample Recovery Management Team Roster

Position	Primary	Alternates
Recovery Manager	CIO/IT Director	John Taylor
Facilities Coordinator	Jeff Whitey	Emerald Brunett
Technical Coordinator	CIO/IT Director	Brian Parker
Admin Coordinator	Jeff Whitey	Emerald Brunett
Network Coordinator	Brian Parker	John Taylor CIO/IT Director

Applications Coordinator	Vacant	James Chilson Vacant

Disaster Recovery Team Responsibilities

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. The following section provides a brief description of the responsibilities for each team.

Recovery Management Team

The Recovery Management Team is responsible for the coordination of the entire project. It is composed of seven skilled people:

1. Recovery Manager
2. Facilities Coordinator
3. Technical Coordinator
4. Administrative Coordinator
5. Network Coordinator
6. Applications Coordinator

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

Damage Assessment Team

The Technical Coordinator will be responsible for providing an assessment of what can be salvaged of the hardware components. Based on this assessment, the Recovery Management Team can make

the choice of the recovery site and begin the process of acquiring replacement equipment for the recovery.

Facility Recovery Team

The Facility Recovery Team will be led by the Facilities Coordinator. She/He will be responsible for selecting the other team members. Likely choices would be member(s) from Operations, Network Services, Physical Plant, Cold Site Building Representative, 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 Cold 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 Randolph Hall). 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.

Network Recovery

The Network Recovery Coordinator will be responsible overseeing the restoration of the campus network and all network connections necessary at the recovery site.

Because there is such a high degree of reliance on the campus network, for instruction, research, and administrative purposes, very high emphasis must be placed on restoring the network as quickly as possible.

Platform Recovery Team

The Platform Recovery Team will be responsible for restoring one or more of the computer platforms described in this plan.

Each platform recovery will follow this general plan of action:

1. Review damage assessment.
2. Determine which hardware, software, and supplies will be needed to start the restoration of a particular system.
3. Communicate list of components to be purchased and their specifications to the Administrative Support Team.
4. Review the recovery steps documented in this plan and make any changes necessary to fit the situations present at the moment.
5. When hardware begins to arrive, work with vendor representatives to install the equipment.

6. When all components are assembled, begin the steps to restore the operating system(s) and other data from the off-site backup tapes.
7. Attempt to recreate status of all systems up to the point of the disaster if possible. If not, the system is handed off to the Application Recovery Team.

Application Recovery Team

The Application Recovery Coordinator will be responsible for conducting activities leading up to the approval and acceptance of application systems for production use. In general, this team's activities will begin after the Platform Recovery Team has completed work on the target platform. Some of the team members may in fact be from the platform recovery teams.

Some of the anticipated tasks include:

1. Analysis of need for additional recovery activities such as data base restores or individual file restores
2. Developing programs/procedures to address specific problems
3. Interfacing with application users to test applications

Administrative Support Team

The Administrative Support Team will be led by the Administrative Coordinator. She/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 College's Purchasing Office. This person will be the liaison to the Business Manager's Office for the purpose of expediting all emergency purchases and ensuring that proper College and State 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 Cold Site or other locations as required.
9. Provide public relations support (this function may be provided by College Relations).
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).

Activating the Disaster Recovery Plan

Last update: July 2021

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 CIO of Integrated Technology Services. If the CIO is unavailable, the appointment should be made by the VP of Administrative Services. This person must have data center management experience and must have signature authority for the expenditures necessary during the recovery process. You can refer to Disaster Recovery Teams for the responsibilities of the Recovery Manager and a suggested list of people who can fill this and other coordinator roles.

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 will affect any rescues 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. 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 she/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. The

section Equipment Protection and Salvage contains valuable information on salvaging damaged magnetic media.

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 Randolph Hall is not suitable, cold site has been designated as the location of the center.

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 the Disaster Recovery Plan located in the bank vault site and one from R3 media safe, to obtain an up-to-date copy of the Disaster Recovery Plan. This plan is in printed form as well on computer media (USB stick or CD-ROM). Copies of the plan should be made and handed out at the first meeting of the Recovery Management Team. The Recovery Manager is responsible for the remaining contents of the plan, which should probably be stored in the media safe in Randolph 3, if possible.
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 Integrated Technology Services staff and Physical Plant management, and with upper College 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:
    1. Each member of the team is to review the status of their respective areas of responsibility.
    2. After this review, the Recovery Manager makes the final decision about where to do the recovery. If the cold site suite is to be used, the Recovery Manager is to declare emergency use of the facility and notify the Dean of Administrative Services and the President immediately.
    3. The Recovery Manager briefly reviews the Disaster Recovery Plan with the team.
    4. Any adjustments to the Disaster Recovery Plan to accommodate special circumstances are to be discussed and decided upon.
    5. 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.
    6. Each member of the team is to review the makeup of their respective recovery teams. If an individual 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.

7. 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. The VP of Administrative Services and Maintenance Supervisor are responsible for immediately clearing the Recovery Control Center room, cold site, for occupation by the Recovery Management Team. This includes the immediate relocation of any personnel occupying the room. The VP of Administrative Services should assist the Administrative Coordinator in locating baseline facilities for the recovery room:
    1. Office desks and chairs
    2. Telephones
    3. Dell personal or notebooks
    4. Hewlett-Packard LaserJet printer
    5. Fax machine
    6. Copier
6. 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 College has an existing contract with Sprint for cellular service, and the Physical Plant has two-way radio units that may be available upon request.

Equipment Protection and Salvage

Last update: July 2021

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 tarpaulins or 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 savaging.

Salvage Magnetic and Optical Media

The magnetic and optical media on which our data is stored is priceless. Although we retain backups of our disk subsystems and 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 College can contract for large scale media recovery services. A list of the companies that might be able to provide these services is found in Section Media Recovery Services.

If more immediate attention is required than can be provided by a contractor, Section Recovery of Damaged Magnetic Tape and Optical Disk Media describes the recovery process that can be used on-site.

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 Cold Site, or to another protective area (such as a warehouse) until the Cold 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 Cold 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.

Damage Assessment

Last update: July 2021

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 cold 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 System Administrator 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 cold site will be evaluated. Administration will need to activate emergency Procurement Procedures.

Requisition Procedures

Last update: July 2021

EMERGENCY REQUISITION PROCEDURES:

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

The Southwestern Oregon Community College Purchasing Regulations lend themselves to a very liberal interpretation which provides the College with considerable latitude in emergency procurement of goods and services. The College's 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 normalcy. 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 Integrated Technology 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 College's 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 College personnel (such as the College's Business Manager).

The following entries document the state regulations and other related information regarding emergency procurement and insurance coverage. Please also reference the disaster recovery plan for the College's Purchasing Office for more information.

- Requisition Procedures
- Insurance Coverage
- Business Interruption Coverage
- Purchasing Vendor List

1. Obtain a Requisition number from Integrated Technology Services Requisition number list.
2. Fill-in Quotation forms with descriptions of items and/or services for which quotations are being solicited (e.g., equipment make and model numbers, installation services for equipment/software listed, etc.)
3. FAX the Item Description Page to at least three vendors likely to be able to provide needed goods or services. Call the vendor to insure that they know the FAX has been sent and understand the need for a quick response. Timeframes for responses can be very short; just be reasonable for the goods requested.
4. Summarize the vendor responses to the Quotation Abstracts and prepare a Quotation Abstract Quotation Summary Page .
5. Attach the vendor responses, any contacts or agreements, and the Quotation Summary Page to Requisition(s) made out for the lowest qualified bids.
6. If quotations are completed during normal College business hours, provide the Requisition, Quotation Abstracts, and any contracts to the Purchasing Office for issuance of Purchase Orders. Due to the immediate need, Purchase Order numbers should be called to the appropriate vendor, or copies should be Faxed, depending upon the policies of the vendor(s) receiving the order(s).

   If the quotations are completed after hours, instruct the appropriate vendors to proceed with processing the order. Obtain the purchasing approvals and Purchase Orders as soon as possible during the next available business hours.

If no College purchasing staff are available due to the nature of the disaster, instruct the appropriate vendors to proceed with processing the order, and forward Requisition(s) and Quotation Abstract(s) to the Office of State Purchasing for issuance of Purchase Order(s).

VENDOR CONTACT INFO:

Vendor participation in the procurement and recovery process will be vital. Vendor support personal should be enlisted to assist with installation and recovery.

1. Dell Purchasing

   Chris Rodriguez
   Account Manager, Sales
   Dell Technologies | Medium Business
   Office: 512-725-4109
   Chris_Rodriguez@Dell.com

2. NEC Phone switch

   A3 Telecom
   Greg Lopata, Mike Lopata 206-307-3030

3. Douglas FastNet Charter

   Dfn.net
   800-516-5251 Ops Center NOC: 866-603-3199

5. Cisco

   Rick Howard | Account Executive
   Presidio | www.presidio.com
   2 Centerpointe Drive Suite 100, Lake Oswego, OR 97035
   D: 503.594.0364 | C: 503.341.8458 | rhoward@presidio.com

   Ethan Barrow
   5400 Meadows Road, Suite 300 Lake Oswego
   ebarrow@cisco.com
   Phone: **+1 503 598 7138**

Section 4: Initiation of Recovery Procedures

Cold Site Preparation

Last update: July 2021

This document focuses on the preparation of the designated Cold Site for the recovery of primary computing and network facilities after a disaster has occurred. If the Recovery Management Team opts to use an alternate site for recovery after the disaster, some work must be done to convert the

space from its present use to be able to house the computer systems, network equipment and disaster recovery team personnel. Those sites may require additional work to prepare for the special power and cooling requirements of the mainframe equipment. Suggested alternate sites on campus include: Student Recreation Center and OCCI switch room. Before considering off-campus sites, be sure to consider the need for proper telecommunications and networking connections to the building, including fiber optic cable to the campus network. The new Health & Science building could have the cold site included in the design.

Cold Site Spaces

The Cold Site will be the Student Recreation Center.

Quick Review of Site Preparation Work

The Cold Site will have minimal advanced preparations, so much work is to be done in the early stages of the recovery process to make the site ready. Here is a quick review of the facilities and work that must be done.

- All occupied offices in the proposed site must be cleared to make the space available for Integrated Technology Services staff and select users to do their work.
- Adequate power capacity should already available within the building. The design phase of the cold site should incorporate connection to the battery backup/generator system.
- The cold site facility should have air conditioning equipment installed.
- The site should have a raised floor such as found in major computer rooms.
- The entrance to the cold site will need to be wide enough to accommodate the larger pieces of equipment that will be installed.
- The Cold Site should have electronic entry security, with doors controlled by a security system. It will be necessary to enter all personnel needing access to the area into the security system.
- Terminations to the fiber optic cabling for the campus backbone network should be located within the Cold Site. Additional fiber optic cable will need to be installed to extend the backbone to other points within the site. An alternative is to set up wireless bridges to the other buildings on campus.
- Telephone cabling will have to be brought into the cold site. An alternative would be to setup ip telephony. The phone system is currently licensed for 150 VOIP phones.

Cold Site Preparation Detailed Documents

The following documents provide detailed information on the recovery of and rebuilding of the data center at the Cold Site.
Cold Site Preparation: **Physical Facility:**

Cold Site Preparation: **Electrical**

Cold Site Preparation: **Air Conditioning**

Cold Site Preparation: **Network Connections**

Cold Site Preparation: Physical Facility

Last update: July 2021

Preparing the Facility

The physical dimensions of the room must be large enough to accommodate eight standard equipment racks. The servers, disk and tape arrays, phone switch, and networking switches will be mounted in these racks. The racks also will contain the patch panels for Ethernet / fiber connections. The room should have a raised floor for ease of cabling. The room should also accommodate several workstation / consoles.

1. The Facilities Coordinator is responsible for coordinating the relocation of any computer equipment, furniture, or personnel to the Cold Site. The Administrative Coordinator should offer to locate additional assistance in moving the equipment and furniture. Maintenance may be able to supply the labor, and some Integrated Technology Services staff may also be available to help. EVERY EFFORT SHOULD BE TAKEN TO ENSURE THAT ALL EQUIPMENT IS MOVED CAREFULLY TO AVOID DAMAGE.
2. The Facilities Coordinator is to contact the necessary contractors to start preparing the Cold Site.
3. The entire facility must be cleaned to remove dust and dirt.
4. Any painting should be completed before moving equipment into the site.

Cold Site Preparation: Electrical

Last update: July 2021

The proposed cold site will have adequate power the equipment to be installed in the room. All circuits should be labeled. 24 120V outlets will be needed for the servers, possibly more.

Electrical contractors may need to be hired to install the necessary power distribution system and cabling for attachment of the computer equipment. The Facilities Coordinator is responsible for obtaining the necessary skilled staff and the power equipment and supplies needed.

Mainframe Electrical Cabling

- The mainframe requires two NEMA L6-20 Plug 220-240V, two 220V 3809BOX plugins, and a 40Amp circuit for the phone switch rectifier. The SAN disk array requires two 120 20A circuits. 28 120V 20A outlets (7 circuits) will be needed for the other equipment.

- Conduit is being added to the cold site construction for the purpose of running phone and fiber circuits. Fiber will need to be run to the nearest connecting vault and spliced into existing fiber. The phone lines will need to be run to the wiring vault and spliced, also. An alternative to running fiber and copper for network and phone connections is wireless point to point bridges to campus buildings.

Cold Site Preparation: Air Conditioning

Existing air conditioning and climate control facilities in the proposed cold site should be sufficient to handle the requirements of a mainframe system. The mainframe equipment by itself requires nearly 300,000 BTUs cooling capacity. Additional equipment for the power distribution system, distributed systems (large UNIX servers, file servers, etc.), network equipment, and human operators raise the total to 5 tons cooling capacity.

Cold Site Preparation: Network Connections

A variety of networking connections are needed for the equipment to be housed in the Student Recreation Center. In general, these consist of fiber optic links to the campus backbone for the key buildings: Dellwood, Stensland, Tioga and Newmark equipment, with Ethernet links servicing the mainframe and most of server equipment and any personal computers in use by recovery personnel in the area.

The scope of the disaster will determine the appropriate response. Loss of network switch room in Randolph or the complete loss of Randolph Hall would necessitate the move to an alternate location.

The following is a recommended list of networking equipment and cabling for the recovery facility.

Total loss of Randolph Hall or the Network room - Relocation to the Cold Site

The campus network is a star topology. The center of this star is the network room in Randolph Hall. Total loss of the network room will require relocation to the cold site. New fiber will have to be run to the vaults and spliced to the remaining fiber runs. An alternative to running new fiber would be the use of wireless bridges to connect campus buildings to the core switch.

Layer 1 Physical Infrastructure:

Orca Communications will have to run new fiber to the cold site and configure their network equipment.

Fiber Connections for the cold site:

Termination Panel with ST connectors

Single Mode Fiber will have to be connected from the cold site to the following buildings:

Stensland

Tioga
Dellwood
Newmark

We will look into using dark fiber to connect to key buildings. Wireless bridges can also be deployed to connect buildings.

Equipment- the network Core switch:

4500x	
Allot	NAC
ASA 55xx	Gold Beach vpn
VPN 3005	

Core Switch Electrical Requirements:

Two dedicated Input-Hardwired connection: 220=8.2A, NEMA L6-20
Two dedicated Input-Hardwired connection: 20A 208AV, NEMA 6-20
Two UPS units with NEMA 6-20 outlets

Configuration Recovery:

Switch configuration is stored on cd in the media safe
A second copy of the switch configuration is in John Taylor's possession.
Installation and restoration of the 4500x configuration will be done with assistance from cisco tech support.

The ASA 5525x is the college firewall. It will need to be replaced and configured before any outside connections are allowed.

The VPN 3000 is a separate entrance to the network for offsite connections. This will need to be replaced and configured to allow remote access.

Ethernet Cabling:

It is recommended that all ethernet connections be 1000 Base-T using Category 5e or Category 6 UTP cabling. Any new fiber runs should be single mode fiber.

Platform Recovery Procedures

Last update: July 2021

This portion of the plan documents the detailed recovery procedures for each of the computer and network systems to be restored at the recovery facility. Each procedure documents the list of equipment necessary to restore service, power and cooling requirements, cabling and networking

requirements, operating system and data restoration procedures, and procedures for placing the system into final form for general use.

Platform Recovery Procedures

- Vendor Contact Info
- Installation Media and Materials Checklist
- Mainframe Systems
- Windows Servers
- Network Equipment
- Phone system

I. INSTALLATION MEDIA AND MATERIALS CHECKLIST

Installation media inventoried and kept in the media safe. Codewords, installation keys, and other installation data should be included.

1. Microsoft HyperV hosts

- 2012, 2016 Datacenter edition Server software
- 2012, 2016 SQL software
- Codewords
- Recovery tapes

2. SAN and Dell software

3. Windows current server OS cd's

4. Exchange email server cd (if used)

5. MDaemon server cd for list email

6. Symantec Antivirus cd

7. Matworx phone console cd

8. UM8700 software & MicroCall call accounting software

Voicemail backup media

IV. RECOVERY: Windows Servers

Windows 2008R2 and 2012 domain controllers will be recovered first. The recovery process is a "bare metal restore" for windows servers. Recreate the Cluster and virtual hosts. Restore vhd

from backups. This system will change with the current virtualization process. The SAN and SAN switches will also need to be replaced.

A detailed set of documents for these procedures are in the Attachments section of the Disaster Recovery Plan Index

Get and keep configurations and procedures in the lock box

Windows Restore Procedures listed in Attachments section.

It's difficult to offer a precise estimate of time required for "cold recovery" of socc.edu under these circumstances. Once new hardware is received, a minimum of three working days should be expected. The time required will vary according to the ability of the person performing system recovery and the speed of the tape subsystem used to perform restores.

V. RECOVERY: Network Equipment

Network recovery depends on the severity and location of the disaster. A disaster that warrants relocation to the cold site will involve a much larger scale recovery process. Cabling must be run where needed. Equipment will have to be replaced. The configuration files will need to be loaded. Cisco tech support will assist the Network Administrator with getting the configurations loaded and modified as needed. The loss of one of the outlying switch rooms will result in a similar recovery process, but on a smaller scale. Equipment in the switch closets are listed in this section.

Total Loss of Building Switch Closet

Recovery from the destruction of a switch closet will depend on which building the loss occurred. Some switch closets contain multiple switches, such as Dellwood, others contain a single switch. Tioga and Newmark switches affect a large number of users. Newmark switch room also contains the phone wiring for the building. Loss of a single leg of the star topology, while serious, will allow a more rapid recovery than the destruction described in the total loss of the network room. Equipment will need to be replaced, cabling repaired, and configurations loaded and modified as needed. Cisco tech support will assist with the configuration process.

Network Equipment List is in the Attachments

Configuration Requirements: Uploading configuration file
Switch configurations are stored on Keith's computer.
A second copy of the switch configurations are in the safe in Randolph 3.
Installation and restoration of the lost switch and configuration will be done with assistance from cisco tech support. Any damage to the local cabling will also have to be repaired by wiring contractors.

Ethernet Cabling:

It is recommended that all ethernet connections be 1000 Base-T using Category 5e or Category 6 UTP cabling. This requires that a Gigabit Ethernet switch with sufficient ports be provided, with a connection to the Cisco Core 4500x redundant switches.

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. IP address assignments are based on the class A 10.x.x.x private IP address scheme. A detailed list of the address assignments will be placed in the lock boxes.

VI. RECOVERY: Phone system

The phone system is an NEC SV8500 IPX with upgrade to SV8700. The loss of the phone switch and its associated wiring will be labor intensive to replace. There are almost 2000 pairs of phone lines that will need to be spliced and connected to the replacement switch. Cable pair maps are kept in an excel spreadsheet located on Keith Lehman's computer and another copy is in his possession. The switch configuration file is kept on the mat terminal in the switch room computer and in the safe in Randolph 3.

Cell phone use would be the backup communication method until the switch and wiring could be replaced.

Applications Recovery Procedures

Last update: July 2021

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.

Critical Applications

Last update: July 2021

The College has identified the payroll application as a critical application. This means that delaying the processing of this application could cause much hardship on faculty, staff, students, 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 Web server application since they will be needed during recovery.

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

REGULAR PAYROLL

Normally paid on the 10 of every month.

Should a disaster place the College 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: Disaster Recovery Plan

Maintaining the Plan

Last update: July 2021

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.

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, Integrated Technology 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 Cold Site location (Student Rec Center).
2. Changes to RANDOLPH HALL that affect Cold Site choice such as enlargement cooling or electrical requirements etc.

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.

Section 6: Disaster Recovery Plan

Attachments:

- **Windows Recovery Documentation**
- **Server Room inventory**
- **Windows Servers Configuration**
- **Network Equipment inventory**

Southwestern Oregon Community College does not discriminate on the basis of race, color, gender, sexual orientation, marital status, religion, national origin, age, disability status, gender identity, or protected veterans in employment, education, or activities as set forth in compliance with federal and state statutes and regulations.