NORTH AMERICAN
UNIVERSITY
INSPIRATION INNOVATION GLOBAL COMPETENCE

North American University

INFORMATION TECHNOLOGY

DISASTER RECOVERY PLAN

Prepared Date:

3 April 2017

Table of Contents

Section

Attachment D Equipment and Software Inventory Attachment E Disaster Recovery Action Items & Improvement Recommendations

1.0 INTRODUCTION

North American University is a small university located in a diverse, metropolitan city full of opportunities. Here at North American University students receive personal attention and find many options for social engagement. Our student body represents the best of the United States of America and the world in diversity. Our faculty is highly qualified with doctorate degrees in their fields and a vast body of professional experience.

NAU is a private, non-profit, full-service college offering baccalaureate degree programs in three disciplines with several concentrations. We are located in South Houston, a few miles away from the famous City of Sugarland. NAU offers a student-centered learning environment where every student is valued and provided with opportunities to grow.

As an institution of higher learning committed to global cultural competency, North American University offers a unique educational experience to our diverse student body, and our custom-designed learning programs provide excellent opportunities to prepare for a globalized professional world where cultural competency is a great asset.
Our teacher-scholars value every student and reflect the core values of the college. Our community engagement programs offer excellent opportunities to get involved in the civic life of Houston and apply skills learned in the classroom in social settings.

2.0 OBJECTIVES

The primary objective of this Disaster Recovery Plan is to help ensure college business continuity by providing the ability to successfully recover computer services in the event of a disaster.

Specific goals of this plan relative to an emergency include:

- Detailing a general course of action to follow in the event of a disaster,
- Minimizing confusion, errors, and expense to the college, and
- Implementing a quick and complete recovery of services.

Secondary objectives of this Plan are:

- Reducing risks of loss of services,
- Providing ongoing protection of institutional assets, and
- Ensuring the continued viability of this plan.

3.0 SCOPE

This plan will only address the recovery of systems under the direct control of the Computing Services Department that are considered critical for business continuity. Also, given the uncertain impact of a given incident or disaster, it is not the intent of this document to provide specific recovery instructions for every system. Rather, this

document will outline a general recovery process which will lead to development of specific responses to any given incident or disaster. Three levels of risk, based on severity to campus operations, have been identified. A Level 1 risk is associated with the Computer Services building and central computer room which house the campus servers, router, PBX and serves as the primary hub for campus electronic and voice communications and connectivity. A Level 2 risk is associated with the campus network infrastructure and the telephone public exchange (PBX). The final risk level, Level 3, is associated with risks specific to unique applications or functionality. Though risk at all levels must be addressed for disaster recovery purposes, Level 1 risks will be given increased priority over other levels.. The same holds true for Level 2 versus Level 3 risks. The following major service areas are addressed in this plan:

- Level 1 - Computing Services Building & Central Computer Room
- Level 2 - Central Telephone Services
- Level 2 - 911 Emergency Services
- Level 2 - Network Infrastructure and Services
- Level 2 - Cable Plant
- Level 3 - File & Print Services
- Level 3 - ERP Services (Banner)
- Level 3 - Email Services
- Level 3 - Web Services
- Level 3 - Campus Card Services (1card)
- Level 3 - Student Residential Network Computing Services (RESNET)
- Level 3 - Technology Enhanced Classroom Support
- Level 3 - Student Computer Lab Services

4.0 ASSUMPTIONS

This disaster recovery plan is based on the following assumptions:

- The safety of students, staff, and faculty is of paramount; the safeguard of such will supersede concerns specific to hardware, software, and other recovery needs.

- Once an incident covered by this plan has been declared a disaster, the appropriate priority will be given to the recovery effort and the resources and support required as outlined in this IT Disaster Recovery Plan will be made available.

- Depending on the severity of the disaster, other departments/divisions on campus may be required to modify their operations to accommodate changes in system performance, computer availability and physical location until a full recovery

has been completed. The NAU Cabinet will encourage campus departments to have contingency or business continuity plans for their operations, which include operating without IT systems for an extended period of time.

5.0 DEFINITIONS

The following definitions pertain to their use in this IT Disaster Recovery Plan:

Backup/Recovery Tapes: Copies of all software and data located on the central servers, which are used to return the servers to a state of readiness and operation that existed shortly prior to the incident/disaster.

Disaster: A significant or unusual incident that has long-term implications to business continuity and the ongoing operations of NAU.

Incident: An event which impacts a specific IT service or server.

Level 1 Risk: Risk associated with the most critical IT services/capabilities, based upon

impact to the campus if the service or capability were lost.

Level 2 Risk: Risk associated with critical IT services/capabilities, based upon impact to the campus if the service or capability were lost.

Level 3 Risk: Risk associated with the loss of selected applications/functionality.

6.0 GENERAL DISASTER RESPONSE & RECOVERY GUIDELINES

1. In the event of a disaster, the CIO will notify the three primary IT Disaster Recovery Teams; network, administrative and telecommunications (see Appendix A, IT Disaster Recovery Teams).

2. Appropriate steps will be taken to safeguard personnel and minimize damage to any related equipment and/or software.

3. A damage assessment will be conducted by each team and recommendations made to the CIO for recovery of impacted services.

4. Individuals required to assist in recovery of these services will be identified. The CIO will communicate this need to the VP for Finance & Administration (see Appendix B, NAU Campus Contact List).

5. The campus will be informed as to IT system degradation and restrictions on IT usage and/or availability.

6. The CIO will develop an overall IT recovery plan and schedule, focusing on highest priorities of the campus infrastructure, first, as defined by the Cabinet.

7. Necessary software and hardware replacement will be coordinated with vendors and the NAU Purchasing Office, as required (see Appendix C for vendor contact information and Appendix D for a list of critical equipment).

8. The CIO will oversee the recovery of campus IT services based on established priorities.

9. The CIO will ensure that IT recovery efforts are properly coordinated with other campus recovery efforts.

10. The CIO will communicate recovery status updates to the NAU Cabinet and campus at large.

11. The CIO will verify restoration of the IT infrastructure to pre-disaster

functionality.

7.0 IT RISK ASSESSMENT7.1 Level 1 - Computing Services (CS) Building and Central Computer Room

7.1.1 General

The CS Building in 8th floor ,concrete, structure located on the north end of campus behind the Admission office . The Computing Services staff, in its entirety, is housed in the facility on the 1st and 2nd floors. The Central Computer Room is located on the 2nd floor of the Computing Services Facility. This room houses the main campus servers and router; the phone switch (PBX) and peripheral servers, such as voicemail and E-911. It is the location where all data and transmitted communications for North American University is redirected, combined, stored and retrieved. There is no off-site backup facility, currently identified, that could replace the functions of the Central Computer Room if it is rendered inoperable by an environmental or manmade disaster.

7.1.1 Risk Assessment

7.1.1.1 Physical/Security Risks

- The Computing Services Building can be accessed through three doors. Each door is keyed to a unique Computing Services key; a campus master key will not open the Computing Service building doors.

- There are a large number of windows on the 1st floor of the building which are susceptible to breakage and possible unauthorized entry. Many of the windows have screws or bolts on the outside frames, allowing for potentially undetected intrusion into the building.

- There is no alarm or camera system for the building doors or

windows.

·Periodically, in the evening, officers from the campus Public Safety Office will ensure that the building doors are secured.

·Entrance to the Central Computer room, located on the 2nd floor, is through a single, locked door; keyed with Computing Services, unique key; the room is comprised of concrete walls with no windows.

· The stairwell to the Central Computer Room is located by the rear entry door to Computing Services; periodically this rear entry door is propped open for equipment delivery, offering an opportunity for an unauthorized person to access the facility.

·There is no video surveillance inside the computer room.

7.1.1.2 Environmental Risks

Rain

o The CS building has a flat roof; the roof has leaked into the Central Computer Room in the past;

o There are no environmental sensing devices installed in the Computer Room to detect water leakage.

If a leak were to occur over a weekend, CS personnel may not be aware of it until the following Monday, possibly too late to mitigate equipment damage.

Flooding

o First floor offices would be impacted in the event of flooding PBX batteries are located in the first floor battery room and would

be ruined if flooding were to occur.

- The Computer Room is located on the 2nd floor of a concrete structure which protects it from flooding

- There are no plumbing lines located above the computer room which could burst or leak

- The building generator is located at ground level and is susceptible to a flooding risk Fire

- Though the building structure is concrete, it houses a large number of desktop computers, a paper storage area, a PBX battery room and individual cubicles which contain documents, books and equipment

- The Computer Room contains large quantities of equipment, but minimal combustibles such as papers or documents – widespread fire is not likely, however small, contained fires are possible in the wiring and equipment.

- Within the Computer Room, the telecom wall is wood, plastic and PIC insulated wire – it is the most flammable part of the room.

- Storage of combustibles (cardboard, paper, plastics, liquids) is not allowed in the Computer Room

- There is no fire suppression system in the Computer Room to reduce damage to equipment.

Extreme Temperatures

- The Computing Services Building suffers from inadequate temperature regulation. Externally mounted, window, swamp coolers provide some cooling relief during the summer months; inadequate heating during the winter months has resulted in individual floor heaters being purchased for personnel cubicles

- Primary and backup air conditioners are available to cool the Central Computer Room. Either system is capable of providing the

necessary cooling for the room.

Only the primary air conditioner is generator powered. The backup unit automatically fails over in the event the primary unit stops operating

- Computer Room air conditioner units have heaters and the computers produce heat, so risk of too low a temperature is minimal.

Natural Disasters (earthquake, tornado, high winds)

- The CS building is a solidly constructed concrete structure which protects personnel and equipment from high winds.
- The Stafford region does not have a history of major earthquakes or tornados.

Other

- The building sealing is poor which has allowed birds to gain access to the interior of the building. If rodents are able to enter, as well, this has the potential to cause cabling or electronics damage.

7.1.1.3 Internal Systems Risk

Power is provided to the CS building from Excel Energy through the regular power grid. The building has 3-phase power utilizing transformers to provide power for the air conditioners and multiple step-down transformers to provide power for equipment in the computer room.

- The main building transformer and entry wiring is located on the west exterior wall of the Computing Services building.
- The transformer and wiring is not protected by a locked enclosure and is susceptible to vandalism. Standby power is provided by a natural gas powered generator.
- This generator provides power to the entire building except for the

elevator which is 440 volts and one air conditioner which is 440 volts.

These two items are not considered essential for disaster recovery.

- The generator performs a self-test each week. Cutover testing is performed on a periodic basis. The generator is serviced annually.

- The generator is located at ground level and is not protected by a fence or other locked enclosure. It is susceptible to flooding and vandalism.

    - Available computer room power is currently "maxed" out. Additional circuits must be freed up or installed to provide adequate power for additional server needs.

- Service outages could occur if additional hardware is added to circuits that are already fully utilized

    - Essential computers and equipment have battery UPS's to maintain power until the generator can run up in the event of a power outage. Many of the UPS's are operating well-beyond there recommended useful life and need to be replaced

7.1.1.4 External Systems Risk

Operation of the Central Computing Room is highly dependent upon the external campus cable plant which provides fiber and copper lines to carry data and telecommunication services.

- The cable plant was upgraded in CY2000 as part of the campus cable plant capital project The cable plant is estimated to have a ten year life expectancy

- Copper wiring and fiber optic cable is run in underground conduit that can be accessed via manholes

- The entry for all fiber optical cable and telephone cable is located at

ground level on the west side of the Computing Services facility; it is not protected by any type of physical barrier to prevent damage due to vandalism and/or accident.

7.1.2 Recovery Planning

- Recovery decisions will be based on the extent of the damage to the CS building and central computing room. A backup computing facility does not currently exist, so if the central computing room remains habitable, every effort will be made to re-establish services in the same area.

- If the central computer room is not habitable, the Computing Services area that existed on the 1st floor of the building will be established as a backup computer facility. Adequate fiber, copper and power must be brought into the facility in order to bring up partial services to the campus.

- If it appears recovery of individual services will take longer than a week to restore, on a selective basis, services will be evaluated for possible out-sourcing to commercial organizations.

7.1.3 Preventative Measures

- The CS building and Central Computer Room are the single most important IT resources on the campus. Restoring this facility will be both expensive and time consuming.

- The current facility/room should be "hardened" to protect it from possible environmental or manmade damage. The following recommendations are made to protect this significant resource:

o Install a building and computer room alarm and monitoring system – both environmental, motion and video, with a remote-notification capability.

o Construct a pitched roof to protect the computer room from possible water damage from rain or melting snow.

o Improve building sealing to prevent access by birds, rodents, etc. o Designate additional storage areas outside of the CS building to reduce building clutter and reduce the amount of flammable material on-hand.

- Develop and document a "power" plan for the central computer room.

- Add additional electrical power and circuits to accommodate near-term and future equipment needs.

- Re-wire the backup air conditioner to allow generator operation for both air conditioners.

- Replace older UPS's and put all UPS's on a standard replacement cycle to ensure a seamless cutover to generator power, if and when, there are power failures.

- Protect the external building transformer and generator by protecting both with locked enclosures.

- Protect the fiber optic and telecom cable entry point via a physical barrier

- Provide better physical security for MDF's and wiring closets to preclude inadvertent or intentional damage.

- Establish a standby computer room on the 1st floor of the

building.

- The initial focus of this effort should be to bring enough fiber, copper and power connectivity to this area to support a partial recovery of campus services in the event of a disaster to the central server room.

  - Contact possible offsite service providers (commercial and educational) who could, on an interim basis, host critical campus services.

7.2. Level 2 - ASC Telecommunications

7.2.1 General

- North American University provides internal and external phone service through a Private Branch Exchange (PBX) telephone network used within the college. Use of a PBX saves the College from having to connect all of its telephone sets, separately, to the public telephone network. In addition to telephones, fax machines, modems and many other communication devices can be connected to a PBX. For this reason, all such devices are generally referred to as extensions.

- The NAU PBX has a redundant operating system with monitoring and trouble reporting equipment. However, it can and does experience problems. Most of the problems associated with the PBX are likely to cause partial phone outages or short-term inconvenience to customers. These problems can normally be fixed within a few hours. There are, however, some major problems that can occur and that take longer to isolate and repair due to multiple commercial companies being involved.

- In addition to basic telephone services, campus voice mail and call accounting services are also provided by NAU

Telecommunications.

- NAU uses the Repartee voice mail system Loss or the voicemail system would be a major inconvenience, but is not considered to be a critical loss to the campus. The voice mail system is no longer under warranty.

- The call accounting system is an integral part of the telecommunications services. The interruption or temporary loss of this service would result in the loss of call records and other billing information.

  - There are many PBX hardware manufacturers and models. NAU currently uses a FUJITSU F-9600. Vendor contact information can be found in Appendix C of this document. This contact information is also found on the PBX, itself.

  - The PBX equipment is installed on the 2nd floor of the Computing Service's building in the Central Computing Room.

  - There are several special circuits that the PBX utilizes to provide telecommunication related services:

- There are four T-1's that provide voice communication between the PBX and the external phone system.

- There are two special circuits that are used for the campus E 911 system.

- There are other special internal circuits that provide services and access to: Voice mail Call accounting Dial up services 911 Emergency Service

7.4 Level 2 – Network Infrastructure and Services

7.4.1 General

·Network services are provided via the wired and wireless network infrastructure. Network services include a wide variety of functions, such as network/file storage (including the associated backup), printing, routing, switching, DNS and DHCP services, web/internet services, bandwidth allocation and monitoring, firewalls, etc.

·Network services are totally dependent on the campus cable plant and a wide- variety of other commercial equipment including servers, switches, routers, wireless access points.

·Loss of network services impacts all other IT services. Although impact to telephone services is currently minor, dependencies could increase if the campus switches over to newer technologies, such as voice over IP (VOIP).

7.4.2 Risk Assessment

7.4.2.1 Physical/Security Risk

With the exception of the cable plant infrastructure and switching electronics located in the campus wiring closets and individual building main distribution facilities (MDF's), all other equipment supporting network services is located in the Central Computing room located in the Computing Services building.

· There is currently no offsite network data storage capability. Though selected data is backed up to tape (Banner, Novell, Linux) and stored offsite, data located on any disc backup system (web) would be lost if the Computing Services Computer Room was rendered inoperable.

· Telephone and data switching electronics are located in main distribution facilities (MDFs) and/or wiring closets located in

each of the major campus buildings.

- Though each closet is locked, in many cases, particularly in the residence halls, these closets are also used for miscellaneous storage and are accessed by other than Computing Services personnel.

    - The risk for inadvertent damage and possible malicious damage is medium to high in these areas.

    - Many closet environments are excessively dusty/dirty and suffer from significant humidity and temperature fluctuations. This can cause a higher than normal network electronic failure rate and reduce the lifetime of the copper network and telephone terminations/cabling.

- Wiring closet security is not up to industry standards. In many cases, doors that do have locks are warped and do not close properly. Also, access to the closets is not monitored or controlled. In some cases the ceilings are not hardened.

- Network printers are occasionally located in unsecured areas leaving them vulnerable to vandalism.

7.4.2.3 Internal Systems Risk

Hardware or software failure impacting individual network services is a significant risk.

- Most network services do not have redundant hardware or failover systems in-place. There are numerous unique hardware items that represent potential single points of failure.
- Equipment is used beyond its advertised/supported life due to budgetary constraints. Failed equipment will be replaced by spare, older, equipment obtained during equipment upgrade cycles.

- Hiring experienced network engineers and technicians is nearly impossible, given the institutions salary limitations and NAU's remote location.

- Adequate training and career growth opportunities must be provided to maintain NAU's current network technical staff

  - Systems documentation, OS and configuration backup procedures, and training for backup personnel is accomplished on an ad hoc basis, resulting in differing levels of available documentation and competently trained personnel in the event of a major incident.

  - All network equipment configurations are backed up nightly to a configuration change management server called Device Authority. This server is not backed up and resides on the first floor of Computing Services.

  - Without establishing appropriate individual and group directory quotas, network storage availability could be exceeded, preventing any additional storage from occurring.

  - Directory tree corruption could potentially require manual reinstallation of all network printer information for each individual device.

  - Wiring closet UPS systems are not tested and/or replaced in a systematic manner.

7.4.3 Recovery Planning

Given the wide-variety of potential problems which could impact network services, the following generic recovery planning steps will be utilized to identify and resolve network problems:

o Assess which network service or services have been lost. o Notify the campus, by whatever means available as to the service outage. o Trouble-shoot to isolate the cause of the service outage – if necessary, contact the appropriate vendor for diagnostic support

o Once the problem is isolated, take appropriate action to restore the service(s).

o In the event the service cannot be restored in a timely fashion, assess possible workarounds, including temporary outsourcing, if feasible.

o Notify the campus as to the status of the effected service.

o Notify the campus when the service becomes available.

7.4.4 Preventative Measures

- Refer to the preventive measures for Computing Services Building and Central Computer Room (paragraph 7.1.3).

- Maintenance agreements are maintained on all critical servers and systems to help mitigate the lack of redundancy and to ensure rapid vendor response to problems. See Attachment C for a listing of vendor contacts and Attachment D for a server inventory.

- Recommended preventive measures include:

o Establish a network "refresh" program to replace aging network

equipment on a regular basis.

o Ensure that annual vendor maintenance agreements are in-place for all critical network systems.

o Maintain a pool of harvested, functional spares to provide replacement of failed, obsolete and un-repairable network switches.

- Procure backup hardware for critical, single point of failure systems.

- Work with the local community and Qwest to establish a redundant fiber optic pathway into the San Luis Valley.

- Develop a secondary campus core server and switching/routing plant with redundant connection to major building wiring closets.

- Develop and implement a plan for offsite storage/backup of major IOS and configuration files.

- Provide more well-defined career growth opportunities for the network staff.

- Provide adequate training opportunities for the network staff to ensure technical proficiency in assigned areas of responsibility.

- Ensure that backup personnel are assigned for each critical network service.

- Provide adequate training to backup personnel on use of recovery procedures for network services.

- Buildup and maintain a stock of wiring closet hardware.

- Improve and standardize backup power to switches located in wiring closets.

- Where possible, do not use wiring closets for storage purposes. Where not possible, build locked cages around wiring closet electronics.

- Standardize wiring closet access.

- Improve climate control in wiring closets where there are significant temperature fluctuations.

- Relocate priority printing devices from vulnerable areas to more secure physical locations.

7.5 Level 2 - Cable Plant 7.5.1 General

·The cable plant is a complex integration of copper wire and fiber optics. The cable plant is, in essence, the nerve system for campus communications. The cable plant provides the connectivity and communication paths for campus telephone and network users.

·The campus cable plant contains over 260,000 feet or roughly 500 miles of cable. The cable is installed underground and within each of the campus buildings.

·The management focal point for the cable plant system is the Computing Services Central Computer Room, from which point it branches out all over campus.

7.5.2 Risk Assessment

7.5.2.1 Physical/Security Risk

· See paragraph 7.1.1.1 physical/Security Risks for the Computing Services Building and Central Computing Room.

·The cable plant is subject to damage from vandalism and unintentional damage caused by construction projects. Unintentional damage is the most common physical/security risk to the cable plant.

7.5.2.2 Environmental Risk

·The cable plant is subject to the effects of extreme temperature ranges and moisture.

·Over time, environmental conditions such as temperature and moisture will affect the reliability and quality of the cable plant.

7.5.2.3 Internal System Risk

The cable plant was designed and engineered to conform to TIA/EIA industry standards to reduce the risk of installation damage and to ensure the required quality of service. Once installed, there is a minimal risk of component failure.

7.9 ASC Web Services 7.9.1 General

- www.na.edu provides NAU's web presence including Student One Stop services and the Portal.

- www.na.edu provides database back ends for web services, runs the content management system, and serves a read only replica of our LDAP directory.

- www.na.edu is a test server and hardware backup.

7.9.2 Risk assessment

7.9.2.1 Internal System Risk

- Access to many online services rely on the NAU Authenticator (NAUA), which uses Megalon and Rodan. When ASCA is unavailable these services become unavailable. Current reliant services include: Banner Web, Student One Stop, Portal, and WebCT.

- Since there currently is no definition of acceptable downtime for these services, NAU relies on a manual disaster recovery process (i.e. server rebuild).

- Software bugs and hardware failure are the primary internal system risks to the Web services area.

7.9.2.2 External System Risk

- Campus web services are dependent upon the network/cable plant for continued operation. This includes fiber controlled by Qwest Communications.

- NAU web services could be comprised by hackers via web application exploits.

7.9.4 Recovery Plan

Recovery requires adapting to the specific disaster which has occurred. The following general recovery scenario is provided, which can be tailored, as necessary.

General Recovery Steps:

- Assess which network service or services have been lost.
- Notify the campus, by whatever means are available, as to the service outage.
- Trouble-shoot to isolate the cause of the service outage. o Once the problem is isolated, take appropriate action to restore the service(s).
- In the event the service cannot be restored in a timely fashion, assess possible workarounds, including temporary outsourcing, if feasible.
- Notify the campus as to the status of the effected service.
- Notify the campus when the service becomes available.

Appendix E
IT Disaster Recovery Plan
Action Items

AI #	Area	Action Item	Status	Comments
1	7.1 Computing Services (CS) Building and Central Computer Room	Install a building and computer room alarm and monitoring system – both environmental, motion and video, with a remote-notification capability		
2	7.1 Computing Services (CS) Building and Central Computer Room	Construct a pitched roof to protect the computer room from possible water damage from rain or melting snow		
3	7.1 Computing Services (CS) Building and Central Computer Room	Designate additional storage areas outside of the CS building to reduce building clutter and reduce the amount of flammable material on-hand		
4	7.1 Computing Services (CS) Building and Central Computer Room	Develop and document a "power" plan for the central computer room		
5	7.1 Computing Services (CS) Building and Central Computer Room	Add additional electrical power and circuits to accommodate near-term and future equipment needs.		
6	7.1 Computing Services (CS) Building and Central Computer Room	Re-wire the backup air conditioner to allow generator operation for both air conditioners		
7	7.1 Computing Services (CS) Building and Central Computer Room	Replace older UPS's and put all UPS's on a standard replacement cycle to ensure a seamless cutover to generator power, if and when, there are power failures		
8	7.1 Computing Services (CS) Building and Central Computer Room	Protect the external building transformer and generator by protecting both with locked enclosures.		
9	7.1 Computing Services (CS) Building and Central Computer Room	Protect the fiber optical and telecom cable entry point via a physical barrier		
10	7.1 Computing Services (CS) Building and Central Computer Room	Provide better physical security for MDF's and wiring closets to preclude inadvertent or intentional damage.		
11	7.1 Computing Services (CS) Building and Central Computer Room	Establish a standby computer room on the 1st floor of the RH building.		
12	7.1 Computing Services (CS) Building and Central Computer Room	Contact possible offsite service providers (commercial and educational) who could, on an interim basis, host critical campus services		

Appendix E
IT Disaster Recovery Plan
Action Items

AI #	Area	Action Item	Status	
13	7.2 Telecommunications 7.3 E911 Services	Installation of a fire suppression system in the central computer room		
14	7.2 Telecommunications	Creating a "crash" kit with spare parts, such as digital or analog trunk cards to minimize PBX downtime		
15	7.2 Telecommunications	Develop a campus emergency communication strategy that assumes the PBX is inoperable.		
16	7.2 Telecommunications	Maintain a spare server that will run the voice mail, OS2, operating system		
17	7.4 Network Infrastructure & Services	Establish a network "refresh" program to replace aging network equipment on a regular basis.		
18	7.4 Network Infrastructure & Services	Ensure that annual vendor maintenance agreements are in-place for all critical network systems.		
19	7.4 Network Infrastructure & Services	Maintain a pool of functional spares for equipment replacement		
20	7.4 Network Infrastructure & Services	Work with the local community and Qwest to establish a redundant fiber optic pathway into the San Luis Valley.		
21	7.4 Network Infrastructure & Services	Develop a secondary campus core server and switching/routing plant with redundant connection to major building wiring closets.		
22	7.4 Network Infrastructure & Services	Develop and implement a plan for offsite backup of major IOS and configuration files.		
23	7.4 Network Infrastructure & Services	Ensure that backup personnel are assigned for each critical network service.		
24	7.4 Network Infrastructure & Services	Provide adequate training to backup personnel on use of recovery procedures for network services.		
25	7.4 Network Infrastructure & Services	Buildup and maintain a stock of wiring closet hardware.		
26	7.4 Network Infrastructure & Services	Improve and standardize backup power to switches located in wiring closets.		
27	7.4 Network Infrastructure & Services	Where possible, do not use wiring closets for storage purposes. Where not possible, build locked cages around wiring closet electronics.		
28	7.4 Network Infrastructure & Services	Standardize wiring closet access.		

Appendix E
IT Disaster Recovery Plan
Action Items

AI #	Area	Action Item	Status	Comments
50	7.8 Email	Consider the use of a revision control system, such as CVS or Subversion, to track changes made to important system files.		
51	7.8 Email	Create a policy governing disk quotas on the faculty mail server. Further restrict the maximum size of email messages.		
52	7.8 Email	Consider server clustering. Consider the use of a Network Attached Storage device with a hot spare server.		
53	7.8 Email	Require users of standalone clients to use the encrypted protocols instead of the unencrypted ones. This may break functionality with PDAs, as they tend to have extremely limited functionality		
54	7.9 Web Services	Since web backups are currently stored to disc and not on tape media, an offsite storage capability should be developed		
55	7.9 Web Services	ASC has action items to configure WebCT and Banner Web to use the LDAP authentication database. When that happens, access to WebCT and Banner Web will not be reliant on the One Stop or Portal, alleviating the effects of any ASCA, Portal or OneStop downtime.		
56	7.9 Web Services	Our production thin clients currently rely on X font services and LPD printing services on hedora. These services need to be migrated out of the test environment, off of hedora.		
57	7.9 Web Services	Hedora maintains local mirrors of Mandriva linux used for security and general software updates. This should be migrated to a production server.		
58	7.10 1-Card System	Supplement the major single point of failure 1 card equipment. This includes: server, card printer and card encoder.		
59	7.10 1-Card System	Obtain an extra repeater for spare to the four existing repeaters.		