ADAMS STATE COLLEGE

COMPUTING SERVICES DEPARTMENT

INFORMATION TECHNOLOGY
DISASTER RECOVERY PLAN

Prepared Date:

30 June 2006

Revision Date:

Rev 1: 2 October 2006

ASC
IT Disaster Recovery Plan

Document Change Page

Revision	Prepared Date	Approved Date	Reason for Change
Original	30 June 2006		Draft IT Disaster Recovery Plan for Cabinet Review
Revision 1	2 October 2006		Final IT DR Plan for Cabinet Approval

Adams State College
Information Technology (IT)
Disaster Recovery Plan

Table of Contents

Section

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

1.0 INTRODUCTION

Adams State College (ASC) is a four year, Colorado, public college which, by statue, offers undergraduate Liberal Arts and Sciences, Teacher Preparation, and Business degree programs; a limited number of master's level programs; and two year transfer programs with a community college role and mission. Over time, Information Technology (IT) services have become critical to performing the educational mission of the college. As a result of this ever-increasing reliance on technology, IT services require a comprehensive Disaster Recovery Plan to assure these services can be re-established quickly and completely in event of a disaster.

This Plan summarizes the results of a comprehensive risk analysis conducted for all IT services; it provides general steps that will be taken in event of a disaster to restore IT functions; and it provides recommendations for "hardening" of the IT infrastructure that require executive-level management approval and additional funding to implement.

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

NOTE: All systems that are both necessary for the daily operations of ASC and the responsibility of the Computing Services Department are maintained under service contracts with the appropriate equipment vendors.

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 ASC 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 ASC.

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, ASC 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 ASC 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 ASC Cabinet and campus at large.

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

7.0 IT RISK ASSESSMENT

7.1 Level 1 - Computing Services (CS) Building and Central Computer Room

7.1.1 General

- The CS Building is a two story, concrete, structure located on the north end of campus behind the Rex Recreation Facility. 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 Adams State College 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
    - The CS building has a flat roof; the roof has leaked into the Central Computer Room in the past;
    - 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
    - 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 San Luis Valley 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 Richardson Hall 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:
    - Install a building and computer room alarm and monitoring system – both environmental, motion and video, with a remote-notification capability.
    - Construct a pitched roof to protect the computer room from possible water damage from rain or melting snow.
    - Improve building sealing to prevent access by birds, rodents, etc.
    - 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 RH 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

- Adams State College 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 ASC 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 ASC Telecommunications.
    - ASC 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. Adams State 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

7.2.2 Risk Assessment

7.2.2.1 Physical/Security Risk

- See paragraph 7.1.1.1 Physical/Security Risks for the Computing Services Building and Central Computing Room.

- There is one dial-in channel to the PBX for remote maintenance and a Qwest phone circuit for alarm reporting.
    - Anyone attempting to access the PBX would need to know the phone numbers, passwords and have knowledge of the PBX program language.

7.2.2.2 Environmental Risk

- See paragraph 7.1.1.2, Environment Risks for Computing Services Building and Central Computing Room.

- PBX's are designed to function in a wide variety of environments with a temperature range of 41F to 104F being acceptable.

7.2.2.3 Internal Systems Risk

- The PBX operates at 48 volts DC through a power inverter, via normal grid power.

- During a power outage the PBX will operate off of a back-up battery system.
    - The back up batteries are located in a 1st floor room in the Computing Services building and should provide up to 6 hours of system power
    - Computing Service has a standby generator that will provide electrical power during normal grid power outages.
        - 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.

- Though the PBX is susceptible to hardware and system failures, it has a redundant control system and software which monitors the system operations. In addition, a removable hard drive system is used to maintain and store the software operating system.
    - In the case of a component or software failure the Critical-I monitoring system will contact the ASC PBX maintenance provider, Altura, who will in turn contact the onsite ASC Telecommunication technician.

- In most cases, a component failure will only affect a part of the system operation. Once a determination is made as to what component has failed, a replacement part

can be on- site in as little as 8 hours. If additional technical assistance is needed a certified technician could be dispatched from Altura's New Mexico office.

- The call accounting system and voice mail systems are dependent upon the operation of the PBX and are also susceptible to hardware and system failures.

- The voice mail system runs on an older server utilizing several software programs to perform its function. Hardware and or software failure would be the most likely cause of a problem.
    - The voice mail system uses the OS2 operating system, which is no longer vendor supported, and which will not run on current server hardware.
    - There is no maintenance agreement for the voicemail system. .

- The majority of call accounting problems will also be related to internal hardware or software problems. These problems can normally be fixed by the Adams State College telephone technician. In cases where hardware replacement or additional support is needed the system is covered by a maintenance contract with Altura Communications.

7.2.2.4 External System Risk

- The PBX utilizes special circuits (T-1's) to provide connectivity to external phone systems. If these T-1's become damaged, or if there is equipment failure at a distance point, ASC's capability to make or receive calls will be impacted. These T-1's are maintained and serviced by Qwest, who is responsible for repair and restoration of service. Qwest contact information is located in Appendix C of this document.

- The PBX is dependent upon the cable plant copper wiring to provide ASC phone service.

- ASC is dependent upon Qwest Communications to provide long distance service.

7.2.3 Recovery Planning

- ASC maintains a PBX shared-maintenance agreement with Altura Communications. This agreement covers the PBX and call accounting system. Altura contact information is located in Appendix C.

- In most situations, PBX problems will be related to internal hardware or software problems
    - These problems usually affect only a few subscribers or pose an inconvenience.
    - These problems are normally repaired by the Adams State College telephone technician.

- In cases where hardware replacement is needed, Altura can have the necessary part on site with in 8 hours.
- If the ASC on-site technician is unavailable, the Altura help desk can be contacted at 800-654-0715.
  - The ASC site number is 05616.
  - This contact information is also posted on the front of the PBX for quick reference.

- In the case of a catastrophic failure of the PBX, impact to the campus would be severe:
  - All phone and associated phone services would cease to function.
  - The ASC shared- maintenance agreement would not cover such a disaster
  - In the event of a total system failure, Altura Communications would be contacted and arrangements would be made to have another FUJITSU F-9600 PBX or similar type PBX delivered, set up and made operational by a team of Altura technicians.
    - This team most likely would respond within 8 to 16 hours from the New Mexico area.
    - Once the situation was normalized, financial negotiations with Altura for the switch replacement would have to be conducted.

- Repairs to the voice mail and call accounting systems will initially be attempted by ASC's onsite telecommunications staff.
  - Additional technical support would be requested from Altura, if needed, for the call accounting system.
  - The voice mail vendor, WSTC Communications, would be contacted for additional technical support if the ASC technician was unable to make the necessary voice mail repairs

7.2.4 Preventative Measures

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

- In-place preventive measures include:
  - Maintaining an annual "Shared Maintenance Agreement" with Altura Communications.
  - Maintaining a certified ASC PBX technician.
  - Backing up PBX configuration changes to a hard drive that is then stored in the ES building safe.
  - Making tape backups of the voice mail system on a regular basis. This does not include stored voice mail messages.
  - Making tape backups of the call accounting system and data on a regular basis.

- Additional preventive measures, to be considered, should include the following:
    - Installation of a fire suppression system in the central computer room.
    - Creating a "crash" kit with spare parts, such as digital or analog trunk cards to minimize PBX downtime.
    - Maintaining a spare server that will run the voice mail, OS2, operating system.
    - Develop a campus emergency communication strategy that assumes the PBX is inoperable. This strategy should:
        - Consider providing cellular phones to key ASC personnel or departments.
        - Consider the use of instant messaging as an internal campus communication option.
        - Review the use of voice over IP (VOIP) as a possible PBX alternative.

7.3. Level 2 - ASC 911 Emergency Services

7.3.1 General

- Adams State College provides 911 and enhanced (E911) services through auxiliary equipment attached to the PBX. The 911 system is dependant upon the PBX to function.

- The Primary 911 reporting unit is located in the Computer Services Building Central Computing Room, with a secondary reporting unit located at ASC Public Safety.

- The 911 system provides two functions; the first is a stand alone emergency reporting system for the college. The second function acts in tandem by reporting 911 calls to the local city emergency center.

- The enhanced 911 service provides a physical location for emergency for 911 calls. This physical address is stored in a data base within the local 911 system and in a second database maintained at an external Qwest site.

- The 911 database is maintained by the ASC telecommunications technician

7.3.2 Risk Assessment

7.3.2.1 Physical/Security Risk

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

7.3.2.2 Environmental Risk

- See paragraph 7.1.1.2, Environment Risks for Computing Services Building and Central Computing Room.

73.2.3 Internal Systems Risk

- The 911 system operates on a desk top PC and utilizes several software programs to perform its function. Therefore, hardware and/or software failure will be the most likely problem to occur.

- The 911 system operates off of 110 volts provided through a UPS which operates off normal grid power.
    - During a power outage, the 911 system will operate off of a backup battery system.
    - Computing Service has a stand by generator that provides electrical power during grid power outages. So, electrical concerns are minimal.
    - In the event of an electrical disaster, with the generator and backup battery system there would be little or no impact.

7.3.2.4 External System Risk

- The 911 system utilizes two special circuits to provide connectivity to external phone systems. If these circuits become damaged, or if there is equipment failure at a distance point, ASC's capability to make 911 calls will be impacted. As these circuits are maintained and serviced by Qwest Communications, it will be responsible for repair and restoration of service.

- If there is an external failure of these special circuits the E911 system will fail to function. However, the telephone system would automatically take over the 911 system and provide basic 911 services. That is, 911 calls will go the 911 operator but E911 location information would not be sent.

7.3.3 Recovery Planning

- In most situations, 911 system problems will be related to internal hardware or software problems. These problems are normally repaired by the Adams State College telephone technician. Assistance is also available from Teletronics Technical Support at 1-800-444-7434, pin # 6809162891

- If the 911 data base needs to be replaced, it can be downloaded from Qwest. This is considered our off site storage.

- In cases where hardware replacement is needed, the Altura help desk can be contacted at 800-654-0715; the ASC site number is 05616. This information is also posted on the front of the 911 system for quick reference.

7.3.4 Preventative Measures

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

- Current preventive measures include:
    - Maintaining an annual "Shared Maintenance Agreement" with Altura Communications
    - Maintaining a certified ASC PBX technician
    - Backing up 911 configuration changes to a hard drive that is then stored, offsite, in the ES building vault

- Other preventive measures to be considered include the following:
    - Installation of a fire suppression system in the central computer room

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

- 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.

7.4.2.2 Environmental Risk

- See paragraph 7.1.1.2, Environment Risks for Computing Services Building and Central Computing Room.

- Wiring closets/MDF's are not environmentally controlled and subject the equipment to varying humidity and temperature extremes and exposure to excessive dirt and dust. There is a risk of equipment and cabling failure because of the lack of a reasonable operating environment.

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 ASC's remote location.
    - Adequate training and career growth opportunities must be provided to maintain ASC'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.

7.4.2.4 External System Risk

- Campus Internet connectivity is dependent upon a single Qwest Communication's fiber optic pathway into the San Luis Valley. This pathway can and has been damaged, resulting in the loss of external campus connectivity.

- There are currently no secondary (backup) data trunking pathways between campus buildings. If current cable plant pathways are damaged, network services will be impacted.

- Hackers could attempt to launch denial of service attacks and/or attacks against network equipment and IOS and/or configuration files.

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

- 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.

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:
  - Establish a network "refresh" program to replace aging network equipment on a regular basis.
  - Ensure that annual vendor maintenance agreements are in-place for all critical network systems.
  - 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.

- The fiber optical portion of the cable plant is terminated at only a single location – Computing Services.

7.5.2.4 External System Risk

- Fiber optic and copper pathways that connect the ASC cable plant with the Qwest data and phone infrastructure can and have been damaged, inadvertently. When this occurs, external network services will be impacted, until Qwest is able to repair its lines.

7.5.3 Recovery Planning

- In most situations when a cable or fiber optic is damaged on campus, the repair can be effected by personnel on staff.

- If damage occurs to off campus cables, the repairs have to be made by Qwest.

7.5.4 Preventive Measures

- Current preventive measures include properly installing copper wire and fiber optics in the proper pathways and in accordance with TIA / EIA standards.

- Periodical inspections of communication closets, pathways and vaults will help to eliminate potential problems.

- Cable damage from construction equipment could be reduced if construction plans were routed through Computing Services for review and approval.

- Controlled access to communication closets will reduce the probability of inadvertent storage-related damage and damage from vandalism.

- A reserve of emergency parts should be maintained to repair most anticipated types of damage.

7.6 Level 3 – File and Print Services

7.6.1 General

- ASC uses Novell Netware to provide campus file and print services. Netware File Services provide campus computer users networked disk space to store files in personal home directories and collaborative group directories. Documents, spreadsheets, databases, and other digital information and programs store and retrieve data from these servers.

- The Netware Printing Service provides centrally managed print processing for campus printers.

- The Netware servers are HP / Compaq hardware running Netware 6.0 or 6.5.

7.6.2 Risk Assessment

- This risk assessment will deal only with the Netware hardware, software and major dependencies required for proper operation of the Netware File and Print Services systems.

7.6.2.1 Physical/Security Risk

- All Netware servers are located in the Computing Services Central Computing Room. Reference Paragraph 8.1.2, Central Computer Room Risk Assessment, for a description of the physical, environmental, electrical, external and internal risks associated with this location.

7.6.2.2 Internal Risk Assessment

- ASC pays an annual maintenance licensing fees for all of the utilized Netware software products. In the event application software is lost due to equipment malfunctions, all required application and operating system software could be obtained from the vendor or via backup tapes or copied compact disks.

- Periodically, a complete restore of the NDS database and selected directories are made to a test environment to ensure the tapes and restore processes are current.

- All current production servers are covered under a basic HP/Compaq next day hardware warrantee. Access to this support is through HP at HP 800-474-6836

- If required Novell technical support is billed on per Service Request basis and can be obtained at 800-858-4000.

- The most significant software-related risk is that associated with losing institutional data stored on NetWare file servers. To mitigate this risk the following backup approach is currently in-place to support NetWare disaster recovery needs:
    - 4 week rotation of all tape sets.
    - Weekly backups of critical servers.
    - Incremental nightly backups of user, home, and 1Card directories.

7.6.2.3 External Risk Assessment

- Network connectivity is vital to the functionality of the Netware servers. Netware File and Print Services cannot operate without a functioning network.

7.6.3 Recovery Planning

- Assess which Netware service or services have been lost
- Notify the campus as to the service outage
- Trouble-shoot to isolate the cause of the service outage – if necessary, contact the appropriate vendor for diagnostic support.
- 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.
- Notify the campus as to the status of the effected service.
- Notify the campus when the service becomes available.

7.6.4 Preventive Measures

- Refer to the preventive measures for Computing Services Building and Central Computer Room (paragraph 7.1.3).
- Current preventative measures include:
    - Netware servers are replaced on a three-year life cycle to minimize problems associated with obsolescence and security.
    - Maintenance contracts are maintained on all Netware hardware during the operational life of the equipment.
    - Hardware and software patches and upgrades are installed on a regular basis.
    - Novell data backup is performed on a regular basis.
- Additional preventative measures include:
    - Review server clustering/high availability options to provide automatic failover and system redundancy in the event of hardware failure.

7.7 Level 3 –Enterprise Resource Planning (ERP) Services

7.7.1 General

- The Banner ERP system provides Adams State College with administrative information such as student finances, student records, payroll and employee

benefit information, and provides a framework for self-service products that are available through the campus portal. This system serves almost all administrative staff on campus and also the on-campus student population and off-campus student population.

- Integrated with Banner are the Banner Self Service products and the Data Warehouse which both rely, heavily, on the Banner service being available.

- The Banner system currently runs on a Sun SPARC hardware platform, using a Sun Solaris Operating System.

7.7.2 Risk Assessment

- This risk assessment will deal only with the Banner hardware, software and major dependencies required for proper operation of the Banner system

7.7.2.1 Physical/Security Risk

- All Banner servers are located in the Computing Services Central Computing Room. Reference Paragraph 8.1.2, Central Computer Room Risk Assessment, for a description of the physical, environmental, electrical, external and internal risks associated with this location.

7.7.2.2 Internal System Risk

- The most significant software-related risk is that associated with losing institutional data stored in Banner's Oracle database. This risk has three components, which span both internal and external risks, including:
    - Internal database corruption which makes some or all of the data inaccessible
    - Unauthorized personnel access to the banner system through malicious intrusion/hacking
    - Unauthorized access to banner data through theft of data, such as theft of a laptop computer containing banner data.

- Banner software and associated commercial software (COBOL, SQR, etc.), as they are periodically updated, are all subject to software discrepancies, bugs and other associated problems.

- There are three operational Banner servers consisting of a database server, a (self-serve) web-server and an Internet-native Banner (INB) server. As with all computer systems, this Banner hardware is susceptible to failure.

- Hiring banner-experienced programmers and Oracle-experienced database administrators is extremely difficult, given the institutions salary limitations and ASC's remote location.

- Adequate training and career growth opportunities must be provided to maintain ASC's current banner programming and DBA staff.

7.7.2.3 External System Risk

- Network connectivity is vital to the functionality of the Banner DBS. Banner cannot operate without a functioning network.

- Unauthorized access to the Banner data base via malicious hacking/intrusion to obtain sensitive personnel data is a significant risk.

- Loss of banner data through laptop or other theft is a significant risk.

7.7.3 Recovery Planning

- Assess which Banner service or services have been lost.

- Notify the campus as to the service outage.

- Trouble-shoot to isolate the cause of the service outage – if necessary, contact the appropriate vendor for diagnostic support, i.e. SCT Sunguard for the Banner software and Sun Microsystems for the Banner hardware.

- 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.

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

- Notify the campus when the service becomes available.

7.7.4 Preventive Measures

- To mitigate the risk of data loss, a new tape backup system was purchased in CY 2005 for the Banner system. The following backup approach is currently in-place to support Banner disaster recovery needs:
  - Daily tape backups are created and archived offsite (vault in the ES building) for 3 weeks.
  - Weekly backup tapes are retained offsite for 6 weeks.
  - Monthly backup tapes are retained on the 3rd week of each month and stored offsite for 12 months.
  - Periodically, the test (SEED) database is restored using backup tapes to ensure the backup system is properly operating.

- The Banner system has it's own firewall to prevent unauthorized external access to Banner data
    - The current firewall is out of warranty, but a new firewall has been purchased and is currently being readied for installation
    - A redundant firewall will be purchased in calendar year 2007 and installed to support automatic failover

- A Computing Services Security Working Group was established to address campus IT security issues, including developing campus security training. Information, regarding the importance of date security has been provided to the Cabinet and appropriate departments. Additional, ongoing, training will be provided in the future.

- ASC pays an annual maintenance fee for all of the utilized Banner software products and associated software products (SQR, COBOL, etc.). As software bugs are identified, the appropriate vendor is notified. In the event application software is lost due to equipment malfunctions, all required application and operating system software could be obtained from the vendor or via backup tapes.

- Recognizing the growing importance of Banner to the institution as it transitioned to on-line services, such as, student registration, backup hardware was purchased for each Banner server to provide system redundancy. The backup hardware does not currently support automatic failover, but will do so by mid-2007.

- ASC has maintenance contracts for all Banner servers. Service requests go to the hardware vendor, Sun Microsystems, for repair. Service is handled primarily out of Sun Colorado Springs operations. Contracts are available at the Sun's Online Support Center at http://www.sun.com . ASC's current maintenance level is silver, which entitles the college to maintenance Monday through Friday between the hours of 8 a.m. and 5 p.m. Refer to Appendix B for Sun vendor contact information.

- The Banner system forces users to change their passwords at least every six months, reducing the risk of ASC employees, who no longer require access, being able to gain entry into the system
    - There is still the need to train personnel on the use of stronger and longer passwords to provide better security

- Provide adequate training and career growth opportunities to help maintain ASC's current banner programming and DBA staff.

7.8 Level 3 - Email Services

7.8.1 General

- Email services include email delivery, virus scanning, spam blocking and email storage. There is both a student email server and a faulty/staff email server.

7.8.2 Risk Assessment

7.8.2.1 Physical/Security Risk - Low

- If an attacker has physical access to the email servers, any and all other security measures can be bypassed.

- The campus email servers are located in the Central Computing Room. See paragraph 8.1.1.1 physical/Security Risks for the Computing Services Building and Central Computing Room.

7.8.2.2 Internal System Risk

- Internal system risks include software viruses and spam spread either intentionally or unintentionally throughout the network; viruses in particular can render the network unusable
    - Viruses; the vast majority of current viruses are transmitted via email. Viruses cause a reduction in productivity on workstations, and frequently require a Computing Services technician to clean or reclone the computer

    - Incoming spam; some estimates place unwanted email (spam) at 90% of all email traffic. This has a significant impact on the user's productivity. Further, spam can introduce viruses and/or spyware onto a user's workstation.

    - Outgoing spam; if the ASC network is used to relay spam out to the Internet, our systems will likely be blacklisted, preventing our users from sending legitimate messages to their contacts.

- File systems filling up do to storage limitations; if a file system is full, no additional data can be written to it. This can cause the transfer or delivery of email to fail, information to not be logged, etc.

- Hardware failure; physical failure of the hardware in the server will cause downtime and may cause data corruption.

- Data compromise via web application; there a number of different kinds of attacks on web applications such as Squirrel Mail. They can allow an attacker to run programs on the server, masquerade as the user, etc.

- System level compromise via various running services ("Remote" Compromises); a flaw in any service running on a server could potentially be used to compromise the server by a remote attacker unless additional measures are taken.

- System level compromise by a local user ("Local" Compromise); local users are those users that actually have an account on the server. By necessity, they have additional rights above those given to an anonymous user.

- Accidental misconfiguration by an administrator; the system administrator, by necessity, has the ability to make drastic changes to server functionality. These changes can cause major problems to the functionality of the server, if not done properly. Should the administrator that made the change not be available to correct the problem, the alternate administrator can have difficulties determining what changes were made and how to restore previous functionality.

- Passwords passed in the clear; most email services transfer a user's password in cleartext. This allows a malicious user to easily read the user's password and then masquerade as the user to send and receive messages as that user.

7.8.2.3 External System Risk

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

7.8.3 Recovery Planning

- 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.

    - 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.

- In the case of a major virus infection, ensure that campus virus protection software is updated and establish a Computing Services tiger team to clean infected campus computers

- If needed, student.adams.edu can be used as the email gateway, but it will operate without virus-scanning. This will require DNS changes, and opening SMTP access to the world in the QMAIL configuration.

- Restore email data from tape backups if necessary. The data backups are managed by Amanda (http://www.amanda.org/), using tar and gzip to actually perform the backup. csworkorder.adams.edu is acting as the tape server.

- If file systems have filled up, increase file system storage and/or request users to delete email stored on the server, but no longer needed.

- For hardware failure, acquire replacement parts as needed from Dell Corporation. The ASC contact there is Guy Youngblood, guy_youngblood@dell.com, 1-800-274-7799 ext. 40976. The service tags are as follows:
    - lurch.adams.edu: 5N8M051
    - student.adams.edu: C24NW21
    - faculty.adams.edu: 1B2V561

- In the case of malicious activity by a single user, disconnect the server from the network and determine the method of data corruption and the duration of inappropriate access. This may require the use of "clean room" techniques to ensure that ASC can prosecute, if desired. Secure the system as necessary, likely including a full system restore, followed by patching of the security flaw.

7.8.4 Preventive Measures

- Physical access to the server(s)
    - *Preventative Measures*: The door to the server room is kept locked.
    - *Action Items*: Ensure that the college's cleaning crew and other, non-CS staff, do not have access to the server room or ensure that those that do have access are properly educated about the security concerns. Better control of the "back room" by the front desk to ensure that visitors can not walk around Computing Services freely.

- Viruses
    - *Preventative Measures*: ASC uses Kaspersky Anti-Virus for Mail Servers on its email gateway. The virus definitions are updated every three hours. Each workstation has McAfee VirusScan installed and is set to automatically update
    - *Action Items*: none.

- Incoming spam
    - *Preventative Measures*: ASC is using the SpamHaus services at the email gateway to drop email delivery attempts from known spam/virus sources. ASC also enables SpamAssassin for all students, and make it available to any employee that wants additional email filtering.
    - *Action Items*: Possibly enable SpamAssassin by default for all employees. Look into additional black listing services.

- Outgoing spam
    - *Preventative Measures*: ASC is currently only allowing email relaying from its own IP address blocks. This prevents a remote spammer from using ASC's mail servers directly. ASC firewalls the campus workstations to prevent a spammer from using them to send spam, using ASC's mail servers indirectly. Finally, ASC is blocking the dorm networks from sending mail through its mail servers directly, preventing them from being used to send spam through our mail servers.
    - *Action Items*: Enable encrypted SMTP-AUTH to allow ASC users to send email from other networks, while preventing spammers from relaying through our network. Possibly block outgoing SMTP connections originating anywhere other than our mail servers to prevent workstations, particularly those in the dorms, from sending spam.

- Item of Concern: Data compromise via web application
    - *Preventative Measures:* Upgrade Safe Mode (SM) reasonably quickly after a new version release, allowing a short period for others to resolve any potential problems with the new release. Most web applications that are on the student/faculty mail servers are being migrated to the new Content Management System. PHP Safe Mode is enabled, preventing malicious students/faculty from accessing data housed by other web applications. Safe Mode Exec Dir only allows system commands from the SM directories. This is necessary for SM to display the user's quota.
    - *Action Items*: Possibly start using SquirrelMail CVS to get the most up-to-date code, limiting the potential duration a programming flaw can cause problems. Possibly look into further

limiting the Safe Mode Exec Dir to a single directory containing only the specific programs required to be run by PHP.

- Item of Concern: System level compromise via various running services
    - *Preventative Measures*: Services are configured to release root level privileges as soon as possible (such as, after binding to a low numbered port). Services that are not necessary are disabled. Services that are necessary, but do not need to be remotely accessed are firewalled both at the host level and at the primary firewall level. Services that must be remotely accessible are firewalled to only allow access from the required networks. Encrypted protocols are available for all services except SMTP, to help ensure the user's password. As the user's username & password are not transferred for sending of email (SMTP-AUTH), and the messages are transferred in the clear natively, this is not an issue. Root access is only allowed from specific networks controlled by Computing Services.
    - *Action Items*: Enable encrypted SMTP-AUTH to allow ASC users to send email via its network, even when they are connected via a different network. This is providing additional functionality, but ensuring the security of the new functionality.

- Item of Concern: System level compromise by a local user ("Local" Compromise)
    - *Preventative Measures*: Measures as listed above. Further, user filesystems are mounted noexec, preventing users from running any programs that they might upload to the server. Users are unable to create files in other locations in the filesystem other than in /tmp.
    - *Action Items*: Possibly move /tmp to a filesystem mounted noexec.

- Item of Concern: User corruption of their own email
    - *Preventative Measures*: Most mail clients, including SquirrelMail, move the message to the Trash folder by default. This allows the user to recover the lost message for up to two weeks. On the faculty/staff mail server, ASC is currently using rsync to backup user directories to disk, allowing a full week's worth of backups that are immediately available for the administrator to restore (assuming the user has emptied their trash).
    - *Action Item*: Consider using rsync for backups-to-disk on the student mail server. Determine a policy for retaining long term backups to allow restoration of data going further back in time than one week. This policy could also address maintaining a permanent archive of all messages sent and received by certain users.

- Item of Concern: Accidental misconfiguration by administrator

    - *Preventative Measures*: All email servers have Webmin, a web based administration tool that can prevent some erroneous changes and is set to automatically log all changes made through its interface. Logging into the root shell account displays a list of all recent changes as notated by the administrator. Logging out of the root shell account prompts the administrator to log any changes made to the system.
    - *Action Items*: Consider the use of a revision control system, such as CVS or Subversion, to track changes made to important system files.

- Item of Concern: File systems filling up
    - *Preventative Measures*: File systems are created with a sizeable amount of "extra" space. Disk quotas are enabled on the student mail server to prevent a single user from preventing other users from receiving email. Queuing of messages ensures delivery once space is available on the requisite file system or user account.
    - *Action Items*: Create a policy governing disk quotas on the faculty mail server. Further restrict the maximum size of email messages.

- Item of Concern: Hardware failure
    - *Preventative Measures*: All email servers are RAID 5 protected. This allows us to lose one hard drive without causing interruption in service. All servers have redundant power supplies, allowing us to lose a power supply without disruption in service. All servers are connected to UPSs, which ensure that the power entering the server is "clean". All data is backed up to tape daily, with a full backup performed at least every 3 days.
    - *Action Items*: Consider server clustering. Consider the use of a Network Attached Storage device with a hot spare server.

- Passwords passed in the clear
    - *Preventative Measures*: SquirrelMail forces the user to log in via HTTPS. We also provide IMAPS and POPS services to allow users of standalone clients (Outlook, Eudora, Thunderbird, etc.) to encrypt their connections.
    - *Action Items*: 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.

7.9 ASC Web Services

7.9.1 General

- Megalon.adams.edu provides ASC's web presence including Student One Stop services and the Portal.

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

- Hedora.adams.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 Adams State College Authenticator (ASCA), 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, ASC 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.

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

7.9.3 Preventative Measures

- Current preventive measures include:

    - ASC relies on onsite backups, error logs, regular security updates, security tripwire software, and the capability of hedora to replace either megalon or rodan for mitigation.

    - Regular server and software security patching is performed to minimize the risk of unauthorized intrusion and/or exploitation.

- The main ASC firewall is configured to block unnecessary external access to campus web servers.

- Future preventive measures

  - Since web backups are currently stored to disc and not on tape media, an offsite storage capability should be developed.

  - Given the user requirement for 24/7 web services availability, establishing high availability for the web services should be implemented to minimize loss of 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.

  - 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.

  - Hedora maintains local mirrors of Mandriva linux used for security and general software updates. This should be migrated to a production server.

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.

  - 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.

7.10 Level 3 – Campus Card Services

7.10.1 General

- ASC uses the General Meters 1-Card System for campus card services. This system provides identification and limited debit-card services for students, staff, and their families. Is used in the campus cafeteria and other locations for vending. Provides door access to selected Residence Halls.

- The 1-Card system was upgraded in 2004 with new server hardware, operating system, management utilities, and selected campus hardware.

- Loss of 1-Card impacts door access to various outside doors, meal plan vending, non-cash laundry vending and miscellaneous other non-cash vending.

7.10.2 Risk Assessment

7.10.2.1 Physical/Security Risk

- The 1-Card server, 2 network managers and 2 repeaters are located in the Computing Services Central Computer Room. A third repeater is located in the Student Union Building "get smart room" and a fourth repeater is located in the Coronado Residence Hall MDF. There are approximately 60 card readers located throughout campus
    - 1-Card hardware located in the Central Computer Room is secure and environmentally protected
    - 1-Card hardware located in the SUB and Coronado is environmentally protected and behind locked doors, but is less secure
    - The 1-Card readers are attached to doors and vending devices and are subject to damage and vandalism

- The 1-Card office is not staffed on a full-time basis and there have been times when the room has been inadvertently left open with no one present

7.10.2.2 Internal System Risk

- An IPX protocol is utilized to limit external connectivity vulnerabilities

- User passwords are not changed on a regular basis, creating a security vulnerability

- The 1-Card software is only available from a single vendor

    - If General Meters went out of business, obtaining maintenance support would be difficult

- The 1-Card software is relatively stable and problem free; there are periodic updates, as with all software

- 1-Card backups are daily done in conjunction with Novell backups
    - There is not a perpetual backup of the 1-Card database, creating a situation where transactions made between backups could be lost in the event of a database failure

- Some readers and other associated equipment are over ten years in age.

- There are a number of Single Point of Failures in certain equipment including:
    - No backup 1-Card server
    - No backup card printer or card encoder

- General Meters is a single source vendor for the 1-Card System. Given the significant monetary investment in the 1-Card System, switching vendors would be a major challenge
    - This limits ASC's flexibility in pursuing lower cost maintenance alternatives, mixing and matching hardware, etc.

7.10.2.3 External System Risk

- 1-Card is dependent upon the network/cable plant for continued operation

7.10.3 Recovery Planning

- Contact information for General Meters in Colorado Springs is (800) 486-4462. Email: support@1card.com .

- Depending on the scope and logistics of recovery, priority items would include:

    - Server rebuild or replacement
    - 1-Card database repair, recovery, or reinstall from backups
    - Network Manager(s) rebuild or replacement including proprietary cards installed
    - Campus Card Office Photo ID Services rebuild or replacement
    - Food Court Point of Sale equipment rebuild or replacement.
    - Door controller(s) repair or replacement
    - Other End-point repair or replacement

7.10.4 Preventive Measures

- Supplement the major single point of failure equipment. This includes: server, card printer and card encoder.

- Obtain an extra repeater for spare to the four existing repeaters.

- The Campus Card Office needs to be properly staffed or relocated to an area where staff consistently reside

- A redundant, perpetual backup of database would help lessen problem of any lost transactions that have occurred between an existing backup and loss of primary database.

- There needs to be a periodic review of Campus Card administrative accounts and administrative terminals, combined with a policy of password change requirements

7.11 Level 3 - Service: Residential Computing Services (ResNet)

7.11.1 General

- ResNet Services provides electronic, phone, and direct technical support for students living on-campus accessing the Internet using our wired and wireless network.

- If ResNet Services becomes unavailable due to a disaster, all on-campus students would lose their ability to access the internet from their residence halls.

7.11.2 Risk assessment

7.11.2.1 Internal System Risk

- Items of concern:
    - Lack of hardware redundancy in Cisco Clean Access (CCA) system
    - Cost of licensing for redundancy
    - Lack of training in the use of CCA

7.11.2.2 External System Risk

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

7.11.3 Preventative Measures

- Purchase additional Clean Access hardware to provide necessary system redundancy.

- Continue the current maintenance support agreement with Cisco in case of a disaster (TAC).

- Continue nightly backups of both the Clean Access Manager and the Clean Access Server using RSYNC.

- Send the CCA system administrator to vendor training.

7.11.4 Recovery Plan

- 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.

    - 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.

- In the case of a disaster with the Cisco Clean Access product, Cisco Support can be requested at www.cisco.com/tac/ . For immediate assistance from Cisco, a TAC request can be submitted by calling 1-800-553-2447 or 1-408-526-7209.

- Depending upon the length of time required to replace or repair the Clean Access System, it is possible to bypass the system to provide Resnet network access.

7.12 Level 3 - Academic Instructional Technology Classrooms

7.12.1 General

- Instructional technology classrooms fall into two categories. These include:
    - Technology Enhanced Classrooms (TECs)

        - These classrooms normally contain an instructor computer, gyro mouse, projector, combination VCR/DVD player, SmartBoard, sound system and document imager.
    - Dual Purpose Student Computer Laboratories in which classes are also taught.

7.12.2 Risk Assessment

- The IT services necessary to support technology enhanced classrooms are covered in other areas of this document and include items such as: cable plant, network, email & WebCT. Once these basic services are restored most IT-dependent classes can continue.

7.12.2.1 Internal System Risk

- Computer hardware and peripherals are subject to normal, random component failures

7.12.2.3 External System Risk

- Academic TECs are highly dependent upon the IT connectivity provided by Computing Services through the campus cable plant and network
- Classroom equipment is susceptible to theft and malicious damage.
- The academic buildings do not have backup power. All classroom IT equipment uses commercial power and is subject to periodic power outages and power fluctuations.

7.12.3 Recovery Planning

- In the event of the loss of a Technology Enhanced Classroom or building to the level of constituting a disaster, classes will be rescheduled in other TECs across campus
- Reconstruction of the TECs will be prioritized along with other IT components impacted by the disaster.

7.12.4 Preventive Measures

- Current Preventive Measures:
    - Computing Services, through the campus instructional technology fee, has established an equipment refresh schedule for the approved TECs. This provides a reasonable equipment replacement cycle and the ability to develop, overtime, a spares pool consisting of the replaced hardware.

- A limited stock of spare equipment is maintained by Computing Services to provide a swap out capability.

- Computing Services is striving to make each TEC identical, in terms of IT equipment, to simplify the hardware repair and replacement process.

- Computers are re-cloned on a periodic basis to bring the software operating systems and applications back to an original state, removing any miscellaneous programs that may have been installed by student users.

- Recommended Preventive Measures:

  - Any academic area which has a unique IT service that is not addressed elsewhere in this document, must list the service with Computing Services to ensure it can be prioritized in the event of a disaster
    - Nursing is the only area that is known to have such a service at this time. A unique circuit, required for distance-learning classes, is used by this program

  - For non-disastrous equipment failures or network outages, instructors should have alternative lesson plans and backup material available

7.13 Level 3 – Student Computer Lab Services

7.13.1 General

- ASC provides over 20 student computer laboratories, containing over 320 desktop computers.

- Student computer laboratories are located in every major academic building, with the exception of the Plachy Hall Field House.

- A 24-hour student computer lab is provided in the Student Union Building

7.13.2 Risk Assessment

- The IT services necessary to support student computer labs are covered in other areas of this disaster plan and include items such as: network infrastructure, email and WebCT. Once these basic services are restored most IT-dependent classes can continue.

7.13.2.1 Internal System Risk

- Computer hardware and peripherals are subject to normal, random component failures.

7.13.2.2 External System Risk

- Student computer labs are highly dependent upon the IT connectivity provided by Computing Services through the campus cable plant and network.

- Student computer lab equipment is susceptible to theft and malicious damage.

- The academic buildings do not have backup power. All student computer lab equipment uses commercial power and is subject to periodic power outages and power fluctuations.

7.13.3 Recovery Planning

- In the event of the loss of a student computer lab or building to the level of constituting a disaster, student computer labs in other academic buildings will be available to support campus needs.

- Reconstruction of the student computer labs will be prioritized along with other IT components impacted by the disaster.

7.13.4 Preventive Measures

- Current Preventive Measures:

    - Computing Services, through the campus instructional technology fee, has established an equipment refresh schedule for the approved student computer laboratories. This provides a reasonable equipment replacement cycle and the ability to develop, overtime, a spares pool consisting of the replaced hardware.

    - A limited stock of spare equipment is maintained by Computing Services to provide a swap out capability.

    - Computing Services is striving to make each student computer lab identical, in terms of IT equipment, to simplify the hardware repair and replacement process.

    - Computers are re-cloned on a periodic basis to bring the software operating systems and applications back to an original state, removing any miscellaneous programs that may have been installed by student users.

    - Desktop computers in the student labs are secured via cable and locking mechanisms to prevent theft.

- The 24-hour student computer lab uses security cameras to help deter vandalism or theft during off-hours.

- Recommended Preventive Measures: None

8.0 MAINTENANCE OF THE IT DISASTER RECOVERY PLAN

The effectiveness of this disaster recovery plan is impacted by changes in the environment that the plan was created to protect. Some major factors, which will impact the plan, are new equipment, changing software environment, staff and organizational changes, and new or changing applications.

Annually, the Chief Information Officer will ensure that the document is reviewed and updated (if required) by a team of Computing Services personnel. This review will include an assessment and update of recommended action items found in Attachment E.

9.0 APPENDICES

Appendix A: IT Disaster Recovery Teams

Appendix B: ASC Campus Contact List

Appendix C: Vendor Contact Information

Appendix D: Computing Services Server Listing

Appendix E: IT Disaster Recovery Plan Action Items

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	Comments
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
29	7.4 Network Infrastructure & Services	Improve climate control in wiring closets where there are significant temperature fluctuations.		
30	7.4 Network Infrastructure & Services	Relocate priority printing devices from vulnerable areas to more secure physical locations.		
31	7.4 Network Infrastructure & Services	Procure backup hardware for critical, single point of failure, systems.		
32	7.4 Network Infrastructure & Services	Provide more well-defined career growth opportunities for the network staff.		
33	7.4 Network Infrastructure & Services	Provide adequate training opportunities for the network staff to ensure technical proficiency in assigned areas of responsibility.		
34	7.5 Cable Plant	Install copper wire and fiber optics in accordance with TIA / EIA standards.		
35	7.5 Cable Plant	Periodically inspect the communication closets, pathways and vaults to help eliminate potential problems.		
36	7.5 Cable Plant	Cable damage from construction equipment could be reduced if construction plans were routed through Computing Services for review and approval.		
37	7.5 Cable Plant	Controlling access to communication closets will reduce the probability of inadvertent storage-related damage and damage from vandalism.		
38	7.5 Cable Plant	Maintain a reserve of emergency parts to repair the most anticipated types of damage.		
39	7.6 Network File & Print	Review clustering/high availability options to improve system availability.		
40	7.7 Banner ERP System	Implement a more-frequent password change policy to provide better overall banner sercurity		
41	7.7 Banner ERP System	There is still the need to train personnel on the use of stronger and longer passwords to provide better security		
42	7.7 Banner ERP System	Provide adequate training and career growth opportunities to help maintain ASC’s current banner programming and DBA staff.		

Appendix E
IT Disaster Recovery Plan
Action Items

AI #	Area	Action Item	Status	Comments
43	7.8 Email	Ensure that the college's cleaning crew and other, non-CS staff, do not have access to the server room or ensure that those that do have access are properly educated about the security concerns. Better control of the "back room" by the front desk to ensure that visitors can not walk around Computing Services freely.		
44	7.8 Email	Possibly enable SpamAssassin by default for all employees. Look into additional black listing services.		
45	7.8 Email	Enable encrypted SMTP-AUTH to allow our users to send email from other networks, while preventing spammers from relaying through our network. Possibly block outgoing SMTP connections originating anywhere other than our mail servers to prevent workstations, particularly those in the dorms, from sending spam.		
46	7.8 Email	Possibly start using SquirrelMail CVS to get the most up-to-date code, limiting the potential duration a programming flaw can cause problems. Possibly look into further limiting the Safe Mode Exec Dir to a single directory containing only the specific programs required to be run by PHP.		
47	7.8 Email	Enable encrypted SMTP-AUTH to allow our users to send email via our network, even when they are connected via a different network. This is providing additional functionality, but ensuring the security of the new functionality.		
48	7.8 Email	Possibly move /tmp to a filesystem mounted noexec.		
49	7.8 Email	Consider using rsync for backups-to-disk on the student mail server. Determine a policy for retaining long term backups to allow restoration of data going further back in time than one week. This policy could also address maintaining a permanent archive of all messages sent and received by certain users.		

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.		

Appendix E
IT Disaster Recovery Plan
Action Items

AI #	Area	Action Item	Status	Comments
60	7.10 1-Card System	The Campus Card Office needs to be properly staffed or relocated to an area where staff consistently reside		
61	7.10 1-Card System	A redundant, perpetual backup of database would help lessen problem of any lost transactions that have occurred between an existing backup and loss of primary database.		
62	7.10 1-Card System	There needs to be a periodic review of Campus Card administrative accounts and administrative terminals, combined with a policy of password change requirements		
63	7.11 ResNet Services	Purchase additional Clean Access hardware to provide necessary system redundancy.		
64	7.11 ResNet Services	Send the CCA system administrator to vendor training.		
65	7.12 Tech Classrooms	Any academic area which has a unique IT service that is not addressed elsewhere in this document, must list the service with Computing Services to ensure it can be prioritized in the event of a disaster		
66	7.12 Tech Classrooms	For non-disastrous equipment failures or network outages, instructors should have alternative lesson plans and backup material available		