UIW Technology Disaster Preparedness & Recovery Plan

Written: May 2011
Last updated: May 2011

Acknowledgments

We acknowledge the ideas taken from the following disaster recovery plans:

Abilene Christian University Disaster Preparedness and Recovery Plan, February 2007, http://www.acu.edu/technology/Technologydocuments/cio/UIW_Technology_Disas.pdf

Baylor University Center for Computing and Information Systems Disaster Recovery Plan, CSD0247, CAUSE, Baylor University, May 25, 1988.

Purpose and Scope

Introduction

The University of the Incarnate Word (UIW) has set up a highly computerized operational environment. This includes the use of microcomputers in offices as well as servers that provide much of the operational support for the administrative and academic units. A campus-wide network ties these various systems together and provides communications to other computer networks, universities, and the computer diagnostic facilities of selected computer vendors involved. In addition, the operation of the campus network provides a vital support component of the university system, including the operation of local and long distance telephone services and cable TV.

The reliability of computers and computer-based systems has increased dramatically. Computer failures that do occur can normally be diagnosed automatically and repaired promptly using both local and remote diagnostic facilities. Many computer systems contain redundant parts, which improve their reliability and provide continual operation when some failures occur.
In years past, most computer operations were predominantly batch-oriented. Disaster plans were comprised primarily of reciprocal agreements made between users of similar systems for job processing (usually at night and/or weekends). This has become less feasible with the very complicated on-line and diverse network systems most institutions now have installed. Although institutions may have similar equipment and operating systems, they generally do not have the capacity to add a large number of users from another on-line environment to their systems even if the technical problems could be solved.

Another possibility is to find alternate sites near the local systems where any additional equipment needed can be shipped in rapidly, and critical on-line operations for the organization can be resumed in a reasonable time. Redundancy in the communications network and a tie-in to the alternate site, or the ability to rapidly tie-in, is an important part of the disaster plan. This type of site is called a cold backup site, as opposed to a hot backup site which contains all equipment necessary to start immediate operations.

For the most part, the major problems that can cause a computing system to be inoperable for a length of time result from environmental problems related to the computing systems. The various situations or incidents that can disable, partially or completely, or impair support of UIW's computing facilities are identified. A working plan for how to deal with each situation is provided.

Almost any disaster will require special funding from the university in order to allow the affected systems to be repaired or replaced. This report assumes that these funds will be made available as needed. Proper approval will be obtained before any funds are committed for recovery.

Objectives/Constraints

A major objective of this document is to define procedures for a contingency plan for recovery from disruption of computer and/or network services. This disruption may come from total destruction of the central site or from minor disruptive incidents. There is a great deal of similarity in the procedures to deal with the different types of incidents affecting different departments in UIW's technology areas. However, special attention and emphasis is given to an orderly recovery and resumption of those operations that concern the critical business of running the university, including providing support to academic departments relying on computing. Consideration is given to recovery within a reasonable time and within cost constraints.

The objectives of this plan are limited to the computing support given to UIW clients from academic and administrative systems under the stewardship of UIW technology areas. The elements that concern microcomputers are addressed; however, client-related functions not directly tied to computer and telephone support by UIW technology areas are not addressed. Also, offices at UIW should develop their own plan to deal with manual operations within their offices should computer and/or network services be disrupted. Due to cost factors and benefit considerations at this time, the alternatives of hot sites and contracts with disaster recovery companies are considered infeasible and unnecessary for UIW.

All major computing systems vital for the daily operation of the University and under the stewardship of UIW technology areas are maintained under service contracts with the equipment vendors. This ensures that routine maintenance problems will be addressed in a timely manner with adequate resources. These contracts range from telephone support only to full hardware replacement.

Assumptions

This section contains some general assumptions, but does not include all special situations that can occur. Any special decisions for situations not covered in this plan needed at the time of an incident will be made by senior technology staff members on site.

This plan will be invoked upon the occurrence of an incident. The senior staff member on site at the time of the incident or the first one on site following an incident will contact the CIO for a determination of the need to declare an incident. The CIO will determine who else needs to be notified including when to notify the Vice President for Finance & Technology.

The senior technology staff member on site at the time of the incident will assume immediate responsibility. The first responsibility will be to see that people are evacuated as needed. If injuries have occurred as a result of the incident, immediate attention will be given to those persons injured. The UIW Campus Police, Facilities Management, and Risk and Safety Office staff will be notified if necessary. If the situation allows, attention will be focused on shutting down systems, turning off power, etc., *but* evacuation is the highest priority. For more emergency information, reference the Emergency Response & Evacuation Plan (http://www.uiw.edu/safety/documents/EmergencyPlanIIUIW6-7-10final.pdf) and the Risk & Safety Office web page (www.uiw.edu/emergency/).

Once an incident which is covered by this plan has been declared, the plan, duties, and responsibilities will remain in effect until the incident is resolved and proper university authorities are notified. Invoking this plan implies that a recovery operation has begun and will continue with top priority until workable technology and/or telephone support to the university has been reestablished.

Incidents Requiring Action

This disaster recovery plan for UIW will be invoked under any of the following circumstances:

- An incident which has disabled or will disable, partially or completely, the central computing facilities, and/or the communications network for a period of 24 hours.
- An incident which has impaired the use of computers and networks managed by UIW technology areas due to circumstances which fall beyond the normal processing of day-to-day operations. This includes all academic and administrative systems which UIW technology areas manage. This includes, but is not limited to, hardware failure, internet attacks, virus attacks, and spam attacks.
- An incident which was caused by problems with computers and/or networks managed by UIW technology areas and has resulted in the injury of one or more persons at UIW.

Contingencies

General situations that can destroy or interrupt technology and telephone services usually occur under the following major categories:

- Power/Air Conditioning Interruption
- Fire
- Water

- Weather and Natural Phenomenon
- Sabotage and Interdiction

There are different levels of severity of these contingencies necessitating different strategies and different types and levels of recovery. This plan covers strategies for:

- Partial recovery - operating at an alternate site on campus and/or other client areas on campus.
- Full recovery - operating at the current central site and client areas, possibly with a degraded level of service for a period of time.

Physical Safeguards

Administration Building

The Administration Building has manual locks on all exterior entrances. Campus Police are the only personnel with keys to external entrances. There is a card swipe on the west side, basement level doors of the Administration Building.

AD 19-30 comprise the server room, the telecommunications room, and infrastructure support services offices. AD 19-30 is protected by an electronic door lock from the interior hallway. (AD-30 also has a combination lock on the door). Only technology and facilities services employees who need regular access have the combination and/or card access. The card access permissions are regularly audited to ensure that only appropriate individuals have access to the server room. See *Appendix One* for a current server room card access list.

AD – 26 – Telecommunications Equipment Room

This room houses the telephone switch, voice mail system, and data communications equipment. It is the hub for each of these campus-wide data, voice, and video networks. There is no protection against water damage.

The telephone equipment is connected to a 5000 VA UPS with three battery backs. This will maintain the telephone switch for approximately 14 hours in the event of a power outage. Other equipment in this room is connected to individual or clustered UPS equipment. There is no fire suppression system installed.

AD-30 – Server Room

AD-30 houses centralized computing equipment for Infrastructure Support Services and Enterprise Systems. There is no protection against water damage and there is no fire suppression system.

All computer equipment in AD-30 is powered by individual or clustered UPS units. Each UPS provides approximately 60 minutes of power during a power interruption. A Caterpillar “Olympian” Natural Gas Generator (Model G100F3) is located down the hall from AD-30 and will power the server room in the event of a power outage. It is exercised weekly on Friday mornings but live cutovers have not been tested.

AD 30 also houses the main DMARC for the campus and the primary distribution point for fiber and copper for the campus.

Network Security Safeguards

All network traffic originating from and destined to the campus passes through a firewall. This firewall is setup with pass and block rules are based on source and destination IP addresses and ports. The firewall is powered by an individual UPS unit, and in the event of a power failure, the firewall is set block all traffic.

Types of Computer Service Disruptions

This document includes hardware and software information, emergency information, and personnel information that will assist in faster recovery from most types and levels of disruptive incidents that may involve UIW's computing facilities. Additional information that may be needed is provided in the appendices of this document. Supporting documents contain additional hardware, software and vendor information.

Normal computer system problems

Most of the major hardware and software vendors represented on campus have some kind of remote diagnostic testing for routine problems. UIW maintains a maintenance contract for these systems that includes 8x5 next business day response for network equipment and four hours for server hardware problems.

Some minor hardware problems do not disrupt service and maintenance is scheduled when convenient for these problems. Most hardware problems disrupting the total operation of the computers are fixed within a few hours.

Major computer and communications system problems

Generally, we have test servers that could be used in case of emergency on our primary systems until repairs can be accomplished or the system replaced. Users would be inconvenienced for some amount of time while systems and parameters are adjusted.

Environmental problems (air conditioning, electrical, fire)

Air Conditioning Outage

The air conditioning is provided by four different units: (1) Day & Light ceiling mount unit; (2) York ceiling mount unit; (3) Armstrong unit; and (4) Ducone unit. The units will keep the room cool enough to avoid hardware damage for a short period of time in case of failure of a single unit.

Electrical

In the event of an electrical outage all servers and other critical equipment are protected from damage by Uninterruptible Power Supplies (UPSs). These units will maintain electrical service to

UIW servers long enough for them to be shut down gracefully. Once electrical power is restored the servers will remain “powered down” until the UPSs are recharged a sufficient amount to ensure the servers could be gracefully shut down in the event of a second power failure.

Fire

UIW does not employ a fire protection system. A centralized fire detection system was installed in 2011 and smoke alarms are also present in the server room.

Major computer and communications system problems

In the event of a catastrophic fire involving the entire building, we would most likely have to replace all hardware.

Humidity factors are a consideration in San Antonio, however they are not as critical as they once were to computing equipment. UIW does not employ a de-humidifying solution in the server room.

Attacks on servers & campus network

In the event of a disruption of service originating by an attack whether malicious or viral, the first response is to determine the destination of the attack. If the destination is local to the administrative servers, the link to these servers would be disconnected to limit information compromises. If the attack is widespread, then the next step is to determine if the attack originated from within the campus or off-campus. If the attack originated within the campus, this portion of the network would be disconnected. If the attack originated off campus, the Internet connection would be disconnected. The extent of the damage would then be assessed, and the nature of the attack would be investigated so that appropriate preventive measures can be taken before services would be restored.

Insurance Considerations

All major hardware is covered under UIW's standard property and casualty insurance for the University with a $5,000 deductible.

Recovery Teams

In case of a disaster, the team will use the emergency call list. General duties of the disaster recovery coordinator are discussed. Recovery team leaders have been assigned in each major area and general duties given. Assignment of personnel in the major areas to specific tasks during the recovery stage will be made by the team leader over that area.

Organization of the Disaster/Recovery Teams

Disaster Recovery Coordinator - Chief Information Officer

Campus-wide Recovery Team
Chief Information Officer
Director, Infrastructure Support Services
Director, Technology Support Services

Director, Enterprise Systems
Director, Instructional Technology

Academic Systems/Operations Recovery Team
Director, Instructional Technology (team leader)
Director, Infrastructure Support Services
Director, Technology Support Services
Bb System Administrator
Audiovisual Coordinator

Administrative Systems/Operations Recovery Team
Director, Enterprise Systems (team leader)
Director, Infrastructure Support Services
System Administrator
DBAs

Network Communications Recover Team
Director, Infrastructure Support Services (team leader)
Network Administrators
Telecommunications Coordinator

Campus Communications Team
Director, Technology Support Services (team leader)
Director, Instructional Technology
Helpdesk/Desktop Support Technicians
IT Administrative Assistant

Disaster/Recovery Team Headquarters

- If the Administration Building is usable, the recovery team will meet in The IT Conference Room in AD-1.
- If the garden level of the Administration Building is not usable but other floors are, the team will meet in AD-155 (Conference Room).
- If the Administration Building is hazardous or not usable, the team will meet in Library G-16 (Training Room).
- If none of the campus facilities are usable, the recovery team will meet at St. Mary's University [pending execution of 'mutual assistance agreement'].

Disaster Recovery Coordinator

The CIO will serve as Disaster Recovery Coordinator. The major responsibilities include:

- Determining, through consultation with appropriate IT Directors, Campus Policies, Facilities Management, and/or Risk & Safety Office personnel, the extent and seriousness of the disaster, notifying the Vice President for Finance & Technology, and keeping him or her informed of the activities and recovery progress. The Vice President for Finance & Technology will in turn keep the President, the Provost and other Vice Presidents informed as appropriate.

- Invoking the Disaster Recovery Plan.
- Supervising the recovery activities.
- Ensure funding issues are resolved.
- Coordinating with the Vice President for Finance & Technology on priorities for clients while going from partial to full recovery.
- Naming replacements, when needed, to fill in for any disabled or absent disaster recovery members. Any members who are out of town and are needed will be notified to return.
- The Director, Technology Support Services will keep clients informed of the recovery activities, and will work with other university constituencies, e.g., Webmaster, as appropriate to do so.

Academic Systems Recovery Team Leader Responsibilities

The Director, Instructional Technology will serve as Academic Systems Recovery Team Leader. The responsibilities in this area include recovery in case of complete or partial disruption of services from the central academic systems. Further, with the Media Center and academic labs around campus, this group will be responsible for providing services for any disabled academic lab using Technology Support Services and Instructional Technology resources as appropriate.

Responsibilities include:

- Coordinating hardware and software replacement with the academic hardware and software vendors.
- Coordinating the activities of moving backup media and materials as appropriate and using these for recovery when needed.
- Coordinating recovery with client departments, those using the academic computers and/or those using labs.
- Coordinating appropriate computer and communications recovery with the Network Communications Recovery Team Leader.
- Keeping the Disaster Recovery Coordinator informed of the extent of damage and recovery procedures being implemented.

Administrative Systems/Operations Recovery Team Leader Responsibilities

The Director, Enterprise Systems will serve as Administrative Systems/Operations Recovery Team Leader.

Responsibilities include:

- Coordinating hardware and software replacement with the administrative hardware and software vendors.
- Supervising retrieval of backup media and materials as appropriate and using these for recovery when needed.
- Coordinating recovery with client departments.

- Coordinating appropriate computer and communications recovery with the Network Communications Recovery Team Leader.
- Coordinating recovery of administrative software with client departments.
- Coordinating schedules for administrative programming, production services, and computer job processing.
- Keeping the Disaster Recovery Coordinator informed of the extent of damage and recovery procedures being implemented.

Network Communications Recovery Team Leader Responsibilities

The Director, Infrastructure Support Services will serve as the Network Communications Recovery Leader.

Responsibilities include:

- Coordinating hardware and software replacement with the communications hardware and software vendors.
- Supervising recovery of the computer communications and telephone system (Note: Facilities Services is responsible for Cable TV).
- Assigning personnel duties from telecom analysts to project leaders of disaster recovery tasks as needed.
- Coordinating activities of computer and communications recovery with the other Recovery Team Leaders.
- Keeping the Disaster Recovery Coordinator informed of the extent of damage and recovery procedures being implemented.

Campus Communications Team Leader Responsibilities

The Director, Technology Support Services will serve as the Campus Communications Leader.

Responsibilities include:

- Contact VIP list to begin communication about incident (See Appendix Two for VIP list.)
- Produce regular status reports regarding incident
- Facilitate meetings between team leaders
- Ensure food and other hospitality items are covered for other teams

Preparing for a Disaster

This section contains the minimum steps necessary to prepare for a possible disaster and as preparation for implementing the recovery procedures. An important part of these procedures is ensuring that the off-site storage facility contains adequate and timely computer backup tapes and documentation for applications systems, operating systems, support packages, and operating procedures.

General Procedures

Responsibilities have been given for ensuring each of following actions have been taken and that any updating needed is continued.

- Maintaining and updating the disaster recovery plan. (CIO)
- Ensuring that all UIW technology area personnel are aware of their responsibilities in case of a disaster. (CIO)
- Ensuring that periodic scheduled rotation of backup media is being followed for the offsite storage facilities. (Director, Infrastructure Support Services)
- Maintaining and periodically updating disaster recovery materials, specifically documentation and systems information, stored in the off-site areas. (Director, Infrastructure Support Services)
- Maintaining a current status of equipment in the main equipment rooms in AD-30. (Director, Infrastructure Support Services)
- Informing all technology personnel of the appropriate emergency and evacuation procedures from Administration Building. (Director, Technical Support Services, in consultation with Risk & Safety Office)
- Ensuring that all security warning systems and emergency lighting systems are functioning properly and are periodically checked by operations personnel. (Director, Technical Support Services, in consultation with Risk & Safety Office)
- Ensuring that fire protection systems (if applicable) are functioning properly and that they are checked periodically. (Director, Infrastructure Support Services)
- Ensuring that UPS systems are functioning properly and that they are being checked periodically. (Director, Infrastructure Support Services)
- Ensuring that the client community is aware of appropriate disaster recovery procedures and any potential problems and consequences that could affect their operations. (Director, Technology Support Services)
- Ensuring that the operations procedure manual for backups is kept current. (Director, Infrastructure Support Services)
- Ensuring that proper temperatures are maintained in equipment areas. (Director, Infrastructure Support Services)

Backup schemes

For Windows Servers: We use Symantec's Backup Exec version 12.5. We schedule full backups once a week and then do incremental backups. Some of the backups are so large that we back them up to disk and then do a tape backup. We use a 3-week rotation. We send tapes to Iron Mountain on Monday morning and we rotate tapes.

For Unix Servers: We use HP Data protector. We run full backups each night and incremental backups at 12p.m. and 6p.m. each night. We use a 3-week rotation. We send tapes to Iron Mountain on Monday morning and we rotate tapes.

At DataPoint in Support of Optometry: Optometry uses the Avamar backup tool for the DNS and DHCP servers and the Active Directory domain controller, as well as EMC Celerra (Storage Area Network) solution. A backup of the Active Directory domain controller and the EMC SAN is housed off-site via point-to-point connection and contract with Bridgehead Networks.

Recovery Procedures

Central Facilities Recovery Plan

An incident at the central computing/networking facilities in AD-30 may place this plan into action. An incident may be of the magnitude that the facilities are not usable and alternate site plans are required. In this case, the alternate site portions of this plan must be implemented. It is obvious that all major support sections in UIW technology areas will need to function together in a disaster, although a specific plan of action is written for each section.

Systems & Operations

This portion of the disaster/recovery plan will be set into motion when an incident has occurred that requires use of the alternate site, or the damage is such that operations can be restored, but only in a degraded mode at the central site in a reasonable time.

It is assumed a disaster has occurred and the administrative recovery plan is to be put in effect. This decision will be made by the Vice President, Finance & Technology upon advice from the CIO.

In case of either a move to an alternate site, or a plan to continue operations at the main site, the following general steps must be taken:

- Determine the extent of the damage and if additional equipment and supplies are needed.
- Obtain approval for expenditure of funds to bring in any needed equipment and supplies.
- Notify local vendor marketing and/or service representatives if there is a need of immediate delivery of components to bring the computer systems to an operational level even in a degraded mode.
- If it is judged advisable, check with third-party vendors to see if a faster delivery schedule can be obtained.
- Notify vendor hardware support personnel that a priority should be placed on assistance to add and/or replace any additional components.
- Notify vendor systems support personnel that help is needed immediately to begin procedures to restore systems software at UIW.
- Rush order any supplies, forms, electrical cables or media that may be needed.

In addition to the general steps listed at the beginning of this section, the following additional major tasks must be followed in use of the alternate site:

- Notify officials that an alternate site will be needed for an alternate facility.
- Coordinate moving of equipment and support personnel into the alternate site with appropriate personnel.

- Bring the recovery materials from the off-site storage to the alternate site.
- As soon as the hardware is up to specifications to run the operating system, load software and run necessary tests.
- Determine the priorities of the client software that needs to be available and load these packages in order. These priorities often are a factor of the time of the month and semester when the disaster occurs.
- Prepare backup materials and return these to the off-site storage area.
- Set up operations in the alternate site.
- Coordinate client activities to ensure the most critical jobs are being supported as needed.
- As production begins, ensure that periodic backup procedures are being followed and materials are being placed in off-site storage periodically.
- Work out plans to ensure all critical support will be phased in.
- Keep administration and clients informed of the status, progress, and problems.
- Coordinate the longer range plans with the administration, the alternate site officials, and staff for time of continuing support and ultimately restoring the Systems & Operations section.

Degraded Operations at Central Site

In this event, it is assumed that an incident has occurred but that degraded operations can be set up in the Administration Building. In addition to the general steps that are followed in either case, special steps need to be taken.

- Evaluate the extent of the damage, and if only degraded service can be obtained, determine how long it will be before full service can be restored.
- Replace hardware as needed to restore service to at least a degraded service.
- Perform system installation as needed to restore service. If backup files are needed and are not available from the on-site backup files, they will be transferred from the off-site storage.
- Work with the various vendors, as needed, to ensure support in restoring full service.
- Keep the administration and clients informed of the status, progress and problems.

Use of Alternate Sites

If the central site is destroyed, support of critical academic computing activities will be given from the alternate sites. Additional computer systems will be brought in as needed.
Some steps necessary in this process are listed.

- Determine the priorities of client needs and upgrade computers at the academic labs.
- Set up for operations support.
- Coordinate installing additional equipment and moving support personnel.
- When additional, needed equipment is available, move backup materials from the offsite storage area.
- Coordinate restoring any network communications with Infrastructure Support Services.
- Coordinate client computing support with clients.

- As production begins, ensure that backup procedures are followed and periodic backups are stored off site.
- Work with the Director, Instructional Technology for restoring full support to academic computing resources.

Network Communications

Redundancy is being built into the computer communications systems. We do not have complete redundancy, but most systems have backup equipment and/or cards. Email, DNS/DHCP, and Radius all have failover at Pharmacy. Two Banner servers are also housed in the Pharmacy IDF (Banner4 and Banner UIW8).

This plan does not, at this time, address the problem of a need for redundancy in the telephone switch system. Considerable funds will be needed for an alternate plan in this area in case of a major disaster in the university telephone switch. Providing adequate air conditioning and fire protection are the highest priority.

Since most of the telephone and computer communications lines are buried and in conduits across campus, connecting lines to alternate sites and to critical areas cannot be done rapidly. For example, it is estimated that if UIW technology areas had to move, it would take 72- 96 hours (depending on the disaster) to restore critical data and voice communications lines.

Some general steps that must be taken in case of a network communications disaster at the central site and/or other parts of the communications network are given.

- Assessment of the damage and an evaluation of steps needed to restore services.
- Assignment of personnel to disaster crews and assignment of tasks. The priority of repairs will be made by the Disaster Coordinator after an evaluation of the critical needs of the University following the disaster.
- If present supplies and equipment on hand are not adequate to restore service as needed, obtain approval for funds needed and contact vendors for priority shipment.
- Coordinate repairs of data communications disasters affecting specific areas of technology support with the recovery team leader of that area.
- Keep the Disaster Recovery Coordinator and team leaders of support areas informed of the extent of the communications damage and recovery procedures being implemented.

Computer Lab Recovery Plan

In case of an event affecting only a lab, this section of the disaster plan will be executed. For recovery purposes, labs by definition will mean a computer area supporting a number of clients as contrasted to an area containing only a few microcomputers. An event can occur in an area not defined as a lab; however, it is assumed recovery of services in this situation can be carried out in a routine manner. An area may be considered a lab even if it is in an administrative service area and there are a large number of microcomputers involved.

A disaster will be declared in a lab when a large portion of the units in the lab are affected to the extent that recovery in that area in a reasonable time with normal procedures is not possible.

General steps that will be followed in recovery of a lab are listed. The team leader of the computer area with support duties over the lab affected will assume prime responsibility in the recovery process.

- Determine the extent of the damage in the lab and whether alternate lab services will be needed while recovery is taking place.
- Obtain university approval for any funds needed to replace equipment and supplies.
- Determine whether adequate equipment is available on campus to restore even partial services in the lab affected.
- Coordinate recovery of the center with Infrastructure Support Services if communications lines are involved in the lab.
- If alternate services are to be provided for clients of the lab, coordinate activities between groups affected.
- Keep the Disaster Coordinator informed of the status of the lab and the recovery process.

Emergency Procedures

In case an incident has happened or is imminent that will drastically disrupt operations, the following steps should be taken to reduce the probability of personal injuries and/or limit the extent of the damage, if there is not a risk to employees. Similar steps should be followed, where appropriate, in incidents occurring in a satellite center.

- An announcement should be made to evacuate the building, if appropriate, or move to a safe location in the building. As a preparation for a potential disaster, all UIW technology area personnel should be aware of the exits available.
- If there are injured personnel, ensure their evacuations and call emergency assistance as needed.
- If the computers and air conditioning have not automatically powered down, initiate procedures to orderly shut down systems when possible.
- When possible and if time is available, set up damage-limiting measures.
- Designate available personnel to initiate lockup procedures normal to last shift procedures.

Off-site Storage

All central file backups are made on magnetic tapes using an appropriate backup strategy and are stored off-site at:

Iron Mountain San Antonio
931 North Broadway
San Antonio, TX 78215
(210) 248-0037
(800) 899-4766

Other reference documents:

- After Hours and Emergency Call List for Information Services (See Appendix Two)
- Primary vendor contact information (See Appendix Three)
- Critical Services Index (See Appendix Four)

Appendix One: Card Access List for AD 19-30 Doors

CARDHOLDER LIST

(by Name)

4/26/2011
5:39:01PM

REPORT NAME: Access to IT Office Door

List #	*Cardholder*	*Code #*	*Access Level (s)*	*Loc #*	*Linking Level(s)*	*Company*
1	**AGNESE, LOUIS PRESIDENT**					**UIW Employees**
2	**Agnese, Michael**					**RDS Elec. Sec. a**
3	**Agnese, Michael**					**UIW Employees**
4	**Andrews, Carrie**					**UIW - Police**
5	**Arnell, Melvin**					**UIW Employees**
6	**Bhirdo, Alice**					**UIW - Police**
7	**Blancas, Carlos - HVAC**					**UIW Employees**
8	**Bostian, Cary**					**UIW - Police**
9	**Burrell, John**					**UIW Employees**
10	**Caffey, Robert**					**UIW - Police**
11	**Cantu, George**					**UIW Employees**
12	**Card, Test**					**UIW - Police**
13	**Carrillo, Roland**					**UIW Employees**
14	**Cavazos, Abel**					**UIW - Police**
15	**Colunga, Jacob**					**UIW - Police**
16	**Cook, Kevin**					**UIW - Police**
17	**Cordova, Vanessa**					**UIW Student**
18	**Cruz, Ed**					**UIW - Police**
19	**Dancause, Gabriel**					**UIW Employees**
20	**DOVER, ELEVATOR SERVICE**					**Contract Compan**
21	**DREXLER, JOHN**					**UIW Employees**
22	**Dunkley, Ken**					**UIW - Police**
23	**Dziuk, Thomas**					**UIW Employees**
24	**Eidson, Marshall**					**UIW Employees**
25	**FONSECA, DIANA**					**UIW Employees**
26	**Fuentes, Ana**					**UIW Employees**
27	**Garcia, Rene - Maint.**					**UIW Employees**
28	**Garcia, Sam**					**RDS Elec. Sec. a**
29	**Garza, Gerardo**					**UIW Employees**
30	**Garza, Veronica M.**					**UIW Employees**
31	**Gil, Arthur**					**UIW Employees**
32	**Givens, Sandy C.**					**Administration E**
33	**Gleason, Elijah**					**UIW Employees**
34	**Gonzalez, Ana**					**UIW Employees**
35	**Grau, Robert**					**UIW Employees**
36	**Guerrero, Albert**					**UIW Employees**
37	**HAYWOOD, CARL**					**UIW Employees**
38	**Hernandez, Manuel - Elect.**					**UIW Employees**
39	**Heying, Stephen**					**UIW Employees**
40	**Ireland, Joseph**					**UIW - Police**

CARDHOLDER LIST

4/26/2011
5:39:04PM

REPORT NAME: Access to IT Office Door

List #	*Cardholder*	*Code #*	*Access Level (s)*	*Loc #*	*Linking Level(s)*	*Company*
41	**Jimenez, Oscar**					**UIW - Police**
42	**Leon, Raymond - Paint Supervisor**					**UIW Employees**
43	**Logan, Robin**					**UIW Employees**
44	**Lopez, Rene**					**UIW Employees**
45	**Martinez, Ray**					**UIW Employees**
46	**Martinez, Robert**					**RDS Elec. Sec. a**
47	**McDaniel, Samuel**					**UIW Employees**
48	**Mesquias, Johnny**					**UIW Employees**
49	**Moreno, Michael A.**					**UIW Employees**
50	**Mouse, Mickey**					**Administration E**
51	**Ogden, Edward**					**UIW Employees**
52	**Ortega, Richard - HVAC**					**UIW Employees**
53	**Pena, Jorge - Elec.**					**UIW Employees**
54	**Ramos, Anthony**					**UIW Employees**
55	**Ramos, Joe**					**UIW - Police**
56	**Ramos, Stephen**					**UIW - Police**
57	**RDS, Rene**					**Contract Compan**
58	**Reininger, Peter - Supervisor**					**UIW Employees**
59	**Rivera, Samuel**					**UIW Employees**
60	**Rodriguez, Oscar**					**UIW Employees**
61	**Rogers, Jack**					**UIW Employees**
62	**Rogers, Kenneth**					**UIW Employees**
63	**Rohrbacher, Hwn**					**UIW - Police**
64	**Ruiz, Alejandro**					**UIW Employees**
65	**Saldana, Celedino**					**UIW Employees**
66	**Sanchez, Juan**					**UIW - Police**
67	**Schilousky, Terry - Information Syst**					**UIW Employees**
68	**Serbantes, Jessica**					**UIW - Police**
69	**Shiu, Chin (Stephen)**					**UIW Employees**
70	**Solcher, Iris**					**UIW Employees**
71	**Solis, Jorge**					**UIW Employees**
72	**Solis, Lizbeth**					**UIW - Police**
73	**Summers, Steven**					**UIW Employees**
74	**Tamez, Christopher**					**UIW - Police**
75	**Test, for Air**					**SPECIAL - LON**
76	**testing, test**					**Administration E**
77	**Tingwald, Chris**					**UIW - Police**
78	**Villarreal, Armando**					**UIW Employees**
79	**Villarreal, Javier "JV"**					**UIW Employees**
80	**Villarreal, Javier "JV" - Access Car**					**UIW Employees**
81	**White, Bruce**					**UIW Employees**
82	**Wilhite, Lorenzo**					**UIW - Police**

End of Cardholder List. **Report List Total = 82**

Appendix Two: After Hours and Emergency Call List for Information Technology

	IT Contact List			
	Ext.	**Name**	**Title**	**Cell Phone**
		IT Directors		
	3866	**Eidson, Marshall**	**CIO**	**254-721-2869**
	3935	**Haywood, Carl**	**Director, Infrastructure Support**	**210-289-8581**
	1201	**Ramos, Anthony**	**Director, Technical Support Services**	**210-913-4607**
	3949	**Givens, Sandy**	**Director, Enterprise Systems**	**210-487-9734**
	3937	**Gonzalez, Ana**	**Director, Instructional Technology**	**210-473-0710**
	8680	**de los Santos Arturo**	**Director, NW Campus Tech Services**	210-861-0683
		Enterprise		
	3949	**Givens, Sandy**	**Director, Enterprise Systems**	**210-487-9734**
	3070	Dziuk, Thomas	Programmer/Analyst	210-667-3138
	283-6489	Grau, Robert F.	System Administrator	210-781-9533
	2150	Ruiz, Alejandro	DBA	210-884-1736
	3867	Schilousky, Terry	Sr. Programmer/Analyst	210-487-0448
	3018	Shiu, Stephen	Sr. Programmer/Analyst	210-415-1463
	2110	Solcher, Iris	Sr. Programmer/Analyst	210-308-8755
	7266	Villarreal, Armando	Programmer/Analyst	210-232-6665
		Vacant	Application Support Analyst	
		IR		
	3933	**Logan, Robin**	**Director, Institutional Research**	**210-865-0384**
	2185	Carrillo, Roland	IR Programmer/Analyst	210-722-5176
		Vacant	IR Programmer/Analyst	
		Infrastructure		
	3935	**Haywood, Carl**	**Director, Infrastructure Support**	**210-289-8581**
	6002	Cantu, George	Unix System Manager	210-213-8819
	6061	Garza, Veronica	Network Administrator III	210-723-9221
	3934	Moreno, Michael	Network Administrator II	210-415-1037
		Arnell, Melvin	Network Administrator I	210-240-8541
	2197	Rogers, Kenneth	Blackboard Administrator	210-415-6094
	3200	Summers, Steve	Telecommunications System Admin	210-621-4595
		Instructional		
	3937	**Gonzalez, Ana**	**Director, Instructional Technology**	**210-473-0710**
	5699	Evans, Rodney	AV Coordinator	210-323-9655
	5840	Garcia, Jose	AV Technician	210-380-3585
	3946	Gott, Adela	Multimedia Specialist	210-326-9627
	2156	Miller, John F.	Convergent Media Manager	210-218-6981
	3920	Peak, Terry	Training Coordinator	210-218-8795
	6067	Segovia, Gino	Convergent Media Specialist	210-845-4401
		TSS		
	1201	**Ramos, Anthony**	**Director, Technical Support Services**	**210-913-4607**
	5034	Vacant	PC Technician	210-240-8541
	2134	Elder, Earl	PC Techncian	210-214-7655
	1124	Palmeri, Brian	PC Techncian (Pharmacy)	210-260-3935
	3844	Rogers, Jack	IT Procurement	
		NW Campus		
	*Opt-8680	de los Santos Arturo	Director, NW Campus Tech Services	861-0683
	*Opt-8168	Jimenez, Roberto	Technical Support Services	315-6572
	*Opt-8164	Smith, Daniel	Technical Support Services	882-9518
	*Opt-5619	Plessinger, Christpher	Virtualization & Storage Specialist	464-8181

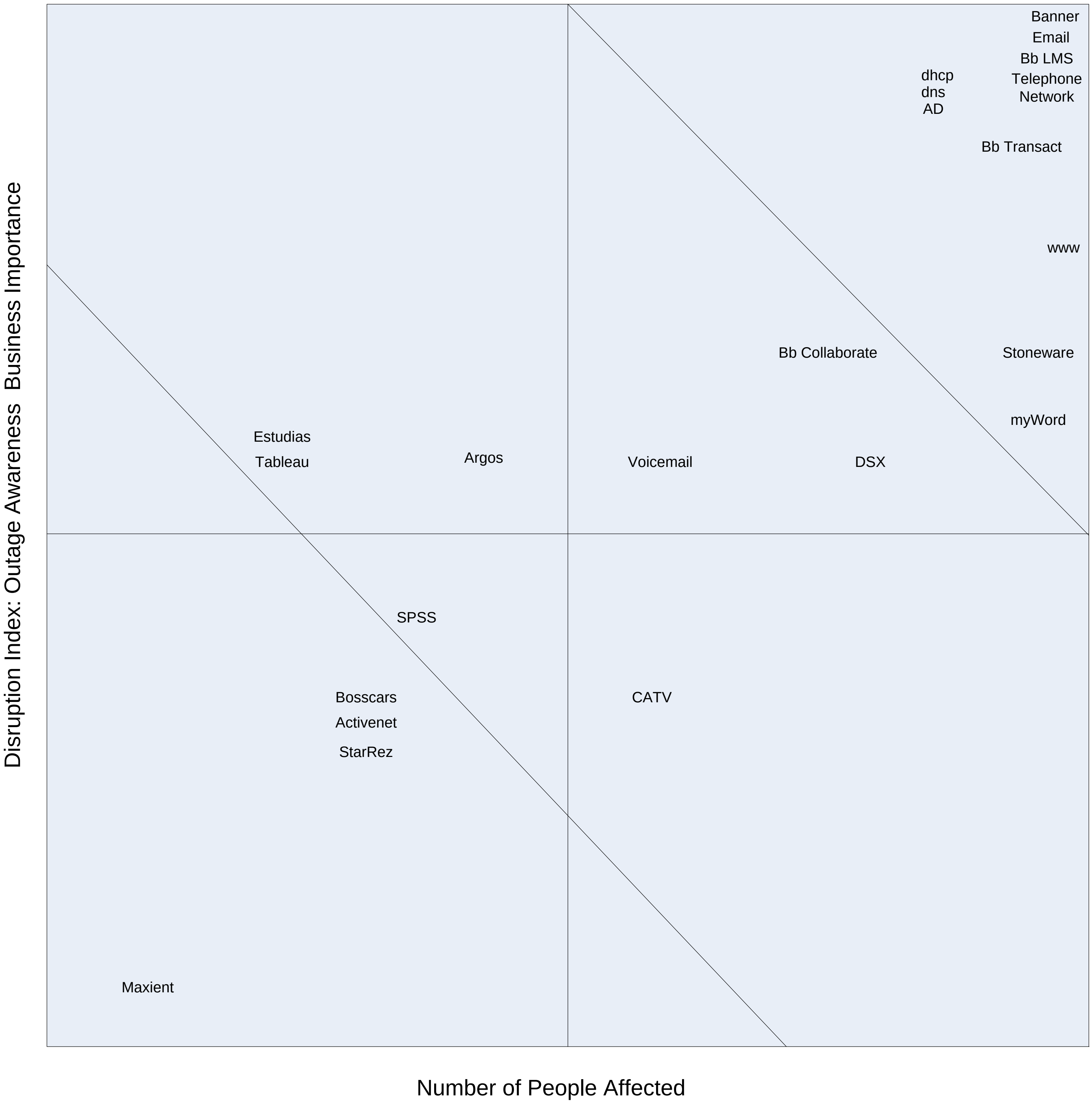
Appendix Three: Primary Vendor Contact Information

Vendor Contact List

Vendor	Product/ Service	Contact	Email	Phone	Alt Phone
Activenet	Wellness Membership		activenetsupport@active.com	1-800-663-4991	
AT&T	Internet	Tony Ramirez	tony.ramirezjr@att.com	210-633-5639	210-416-9449
Avaya	Telecom Equip	Tony Whitelow	tony.whitelow@att.com	972-828-6509	972-971-9269
Blackboard	LMS	John Floyd	jfloyd@blackboard.com	512-371-9557	512-762-7897
Bb Collaborate	Online Collaboration	**Mick de los Santos**	Mick.delossantos@blackboard.com	646.919.1540	
Bb Transaction	Transactions (Sodexo)		support@blackboard.com	1-888-788-5264	
Bosscars	Parking Permit	http://www.bosssoftware.com/support/login.php	support@boss-consulting-inc.com	877-489-7745	
Campus EAI	Portal		support@campuseai.org		
Cisco	Network Gear	Tim Hamilton	tihamilt@cisco.com	210-357-2539	
Dell	Computers Servers	Jody Cook	Joseph_cook@dell.com	512-423-4714	
DSX	ID Card				
I2	Internet	Helpdesk	trouble@the.net	512-471-8530	
Maxient	Judicial Software	Aaron Hark	ahark@maxient.com	(434) 295-1748	
Microsoft	Software			1-800-MICROSOFT	
Oracle	Database		support.oracle.com	800-633-0738	
StarRez	Housing	StarCare	starcare@starrez.com	(877) 812 7802	
Stoneware	Private Cloud	Patric Ainsworth	patric.ainsworth@stone-ware.com	317-669-8742	
Sungard HE	Banner	Use Support Portal https://connect.sungardhe.com	https://connect.sungardhe.com/customer_support/default.htmstart.swe?SWECmd=Start&SWEHo=connect.sungardhe.com	1-800-223-7036	
THE net	Internet	Helpdesk	trouble@the.net	512-471-8530	

Appendix Four: Critical Services Index

Critical Services Index


Banner
Email
Bb LMS
dhcp
Telephone
dns
Network
AD
Bb Transact
www
Bb Collaborate
Stoneware
myWord
Estudias
Argos
Tableau
Voicemail
DSX
SPSS
Bosscars
CATV
Activenet
StarRez
Maxient
Disruption Index: Outage Awareness Business Importance
Number of People Affected