TEXAS A&M
UNIVERSITY
CENTRAL TEXAS

INFORMATION TECHNOLOGY

DISASTER RECOVERY PLAN

Public Version

August 31, 2012

TABLE OF CONTENTS

INTRODUCTION

Texas Administrative Code 202, subsection C, rule 202.74 requires Texas institutions of higher education to maintain a written disaster recovery plan that addresses information resources so that the effects of a disaster will be minimized and the institution of higher education will be able to either maintain or quickly resume mission-critical functions. This disaster recovery plan fulfills that requirement and serves as the guide for Texas A&M University – Central Texas (TAMUCT) Information Technology Services (ITS) management and staff in the recovery and restoration of the information technology systems operated by ITS in the event that a disaster destroys all or part of the those systems.

HISTORY

Located in Killeen and serving the Central Texas region, Texas A&M University-Central Texas became a stand-alone, upper-level (junior, senior, and graduate level coursework leading to baccalaureate and master's degrees) state university when Governor Rick Perry signed Senate Bill 629 on May 27, 2009. However, the path to stand-alone status actually began for TAMUCT in 1999 when the University of Central Texas, a private university, transitioned to become a System Center under Tarleton State University (TSU), a member of The Texas A&M University System (TAMUS). The System Center expanded access to affordable, upper-level undergraduate and graduate education in Central Texas previously offered only by private institutions in Killeen, Belton, and Waco.

During the 2008-2009 Academic Year, the System Center reached an enrollment of 1,000 full-time student equivalents, the threshold level required by the State for stand-alone status, and TAMUCT was authorized to begin operations in Fall 2009, housed in facilities leased from both Central Texas College and the Killeen Independent School District. Immediately following the legislative approval of TAMUCT as a stand-alone university, The Texas A&M University System received the transfer of 672 acres of land from the U.S. Department of the Army as the designated site in Killeen upon which to build a permanent TAMUCT campus. A master plan for the new campus was completed in the following months, and construction of the first building, Founders Hall, began in Fall 2010 and was completed in June 2012. This building houses the TAMUCT data center.

TAMUCT is now completing the third year of a coordinated transition from TSU, its parent institution during its operation as a System Center. Email and digital telephony (i.e., voice-over-IP) are provided by TAMUS. Blackboard, the software platform used for online educational program delivery, is hosted by the vendor. With the exception of the Banner student information system, most other software is hosted by TAMUCT. The last major step in the information technology transition is to transfer the Banner system, currently shared with and hosted by TSU, to a separate instance of Banner that is under TAMUCT control. TAMUS has approved the TAMUCT's request to contract with Ellucian (formerly SunGard) for the full transition of Banner to a vendor-hosted facility by Fall 2014.

PLAN OVERVIEW

The disaster recovery plan is composed of a number of sections that document resources and procedures to be used in the event that a disaster occurs at the Information Technology Services data center located in Founders Hall. Each supported application or platform has a section containing specific recovery procedures. There are also sections that document the personnel that will be needed to perform the recovery tasks and an organizational structure for the recovery process. This plan will be updated on a regular basis as changes to the computing and networking systems are made. Due to the very sensitive nature of the information contained in the plan, the plan should be treated as a confidential document.

SPECIAL NOTE: Two versions have been prepared of the TAMUCT IT Disaster Recovery Plan: a "Confidential, Internal Use Only" version (181 pages) which contains confidential staffing and technical information necessary for recovery activities and a "Public" version (69 pages) which does not contain this confidential information. This document is the "Public" version of the IT Disaster Recovery Plan.

PLAN APPROVAL

Texas A&M University - Central Texas, Version 1.0, dated August 31, 2012 has been reviewed and approved.

_____ _____

Todd Lutz, Chief Information Officer Date

DISASTER DECLARATION

PERSONNEL AUTHORIZED TO DECLARE A DISASTER OR RESUME NORMAL OPERATIONS

The following employees of Texas A&M University - Central Texas are authorized to declare an Information Technology Systems Disaster and also signal a resumption of normal processing:

Name	Title
Marc A Nigliazzo	President
Gaylene Nunn	Vice President, Finance and Administration
Todd Lutz	Chief Information Officer

PLAN ACTIVATION

This plan will be activated in response to internal or external threats to the Information Technology Systems of TAMUCT. Internal threats could include fire, bomb threat, loss of power or other utility or other incidents that threaten the staff and/or the facility. External threats include events that put the facility in danger. Examples might include severe weather or a disruptive incident in the community. Once a threat has been confirmed, the plan management team will assess the situation and initiate the plan if necessary.

RESUMPTION OF NORMAL OPERATIONS

Once the threat has passed, equipment has been repaired or replaced or a new data center has been built and stocked, the disaster recovery team will assess the situation, declare the disaster over and resume normal operations.

PLAN OVERVIEW, OBJECTIVES, AND DECISIONS

PLAN OVERVIEW

The primary focus of this document is to provide a plan to respond to a disaster that destroys or severely cripples the university's central computer systems operated by the Information Technology Services Department. The intent is to restore operations as quickly as possible with the latest and most up-to-date data available. This plan is designed to reduce the number of decisions which must be made when, and if, a disaster occurs.

This plan is a "living document." It is the responsibility of everyone involved in TAMUCT's disaster recovery efforts to ensure that the plan remains current. When you are aware of any changes to personnel, hardware, software, vendors or any other item documented in the plan, please bring them to the attention of the plan administrator.

PLAN OBJECTIVES

The overall objectives of this plan are to protect TAMUCT's computing resources and employees, to safeguard the vital records of which Information Technology Systems is the custodian, and to guarantee the continued availability of essential IT services. The role of this plan is to document the pre-agreed decisions and to design and implement a sufficient set of procedures for responding to a disaster that involves the data center and its services.

A disaster is defined as the occurrence of any event that causes a significant disruption in IT capabilities. This plan assumes the most severe disaster, the kind that requires moving computing resources to another location. Less severe disasters are controlled at the appropriate management level as a part of the total plan.

The basic approach, general assumptions, and possible sequence of events that need to be followed are stated in the plan. It will outline specific preparations prior to a disaster and emergency procedures immediately after a disaster. The plan is a roadmap from disaster to recovery. Due to the nature of the disaster, the steps outlined may be skipped or performed in a different sequence. The general approach is to make the plan as threat-independent as possible. This means that it should be functional regardless of what type of disaster occurs.

For the recovery process to be effective, the plan is organized around a team concept. Each team has specific duties and responsibilities once the decision is made to invoke the disaster recovery mode. The leader of each team and their alternates are key ITS and other university personnel. With such a small IT staff, the use of distinct teams with separate responsibilities is not practical as would be in larger organizations. Rather, IT staff will be assigned to multiple teams with specific assignments made according to knowledge, experience and availability. It is also assumed vendors and knowledgeable personnel from TAMUS will be actively enlisted to help during a recovery situation.

The plan represents a dynamic process that will be kept current through updates, testing, and reviews. As recommendations are completed or as new areas of concern are recognized, the plan will be revised to reflect the current IT environment.

DISASTER RECOVERY PHASES

The disaster recovery process consists of four phases. They are:

Phase 1: Disaster Assessment
Phase 2: Disaster Recovery Activation
Phase 3: Alternate Site/Data Center Rebuild
Phase 4: Return Home

DISASTER ASSESSMENT

The disaster assessment phase lasts from the inception of the disaster until it is under control and the extent of the damage can be assessed. Cooperation with Bell County emergency services personnel is critical.

DISASTER RECOVERY ACTIVATION

When the decision is made to move primary processing to another location, this phase begins. The Disaster Recovery Management Team will assemble at the command center and call upon team members to perform their assigned tasks. The most important function is to fully restore operations at a suitable location and resume normal functions. Once normal operations are established at the alternate location, Phase 2 is complete.

ALTERNATE SITE OPERATION/DATA CENTER REBUILD

This phase involves continuing operations at the alternate location. In addition, the process of restoring the primary site will be performed.

RETURN HOME

This phase involves the reactivation of the primary data center at either the original or possibly a new location. The activation of this site does not have to be as rushed as the activation of the alternate recovery center. At the end of this phase, a thorough review of the disaster recovery process should be taken. Any deficiencies in this plan can be corrected by updating the plan.

KEY DISASTER RECOVERY ACTIVITIES

Declaring a disaster means:

1. Activating the recovery plan
2. Notifying team leaders
3. Notifying key management contacts
4. Redirecting voice service to an alternate location
5. Securing a new location for the data center
6. Ordering and configuring replacement equipment
7. Reconfiguring the network
8. Reinstalling software and data
9. Keeping management informed
10. Keeping users informed
11. Keeping the public informed

DISASTER DECISION TREE

EVENT	DECISION
Data Center destroyed	Activate disaster recovery plan
Data Center unusable for MORE than 2 days	Activate disaster recovery plan
Data Center unusable for 2 days or LESS	Management Team and Facilities Team perform an assessment
Data Center unusable for 2 days or LESS	Management Team and Tech Support Team perform an assessment
Network down	Management Team and Tech Support Team perform an assessment
Central telephone company office down	Management Team and Tech Support Team perform an assessment
Environmental problems (A/C, power, etc.)	Management Team and Facilities Team perform an assessment

DECISION MAKING FOR A DATA CENTER DISASTER

DECISION POINT	ACTIONS				CATEGORY
1. Incident occurs	2. Alarm sounds	3. Begin evacuation	4. Ensure all employees evacuated	5. Meet in designated area	Initiation
7. Determine if incident is real	8. If no, then	9. Recovery plan is not activated	10. Return to normal operations	12. Evaluate evacuation	Determination
7. Determine if incident is real	8. If yes, then	9. Switch call handling to an alternate location			Determination
10. Determine scope of incident and assess damage after building access is allowed	11. If small scope with no to minimal damage, then	12. Return and begin clean up and minor repairs	13. Return calls	14. Return to normal operations	Short Evacuation Required
10. Determine scope of incident and assess damage after building access is allowed	11. If moderate to large scope or moderate to severe damage, then	12. Activate alternate computer processing site	13. Activate recovery team	14. Notify management and employees of situation	Moderate to Severe Damage to Data Center or Infrastructure
16. Assess damage	17. If damage is moderate and will be able to return in 30 days or less	18. Complete repairs as necessary while operating at alternate site	19. Return to data center	20. Return to normal operations	Moderate Severe Damage to Data Center or Infrastructure
16. Assess damage	17. If more than 30 days, locate to new facility	18. Order supplies and equipment	19. Set up and operate at new facility while completing repairs	20. Return to normal operations	Severe Damage to Data Center or Infrastructure

RECOVERY TIME OBJECTIVES (RTO)

The Recovery Time Objectives reflect the estimated recovery times based on current configurations and operations. While a detailed listing of applications and their associated Recovery Tiers is listed later in this document, here is a general overview of the RTO's.

NETWORK SERVICE	RECOVERY GOAL
LAN (Local Area Network)	7-10 days estimate
WAN (Wide Area Network)	30 days estimate
Internet	30 days estimate

APPLICATION RECOVERY TIER	RECOVERY GOAL
Tier 0 Applications	Immediately after WAN/Internet restore
Tier 1 Applications	5 days after LAN/WAN restore
Tier 2 Applications	10 days after LAN/WAN restore
Tier 3 Applications	15 days after LAN/WAN restore
Tier 4 Applications	When Possible

These RTO's should be considered best-case estimates. Currently, TAMUCT does not have computer hardware available for recovery nor contracts or agreements in place to obtain hardware on a priority basis. In the event of a disaster, hardware would have to be located, purchased, shipped, installed, and configured before any software or data could be installed or restored. The availability of the relevant equipment and shipping times could vary greatly depending on the timing and scope of the disaster.

The network services and application recovery times are additive in case of a disaster that affects servers and the LAN. However, a WAN disaster takes significantly longer to recover from due to the installation schedules of telecommunications providers. During this delay, server and LAN recovery could be completed so the WAN recovery time would be the only time applicable to the RTO.

RECOVERY POINT OBJECTIVES (RPO)

Recovery Point Objective (RPO) reflects the estimated point in time to which recovery would be made based on current configurations and operations. The exact recovery point for each server will vary due to the time when backup takes place and when the disaster occurs. Below are general guidelines for the different types of DR data protection.

DATA PROTECTION TYPE	RECOVERY POINT (AGE OF DATA)
Replication	Under development, RPO to be determined following the deployment of the remote Storage Area Network (SAN) unit at an offsite location such as Tarleton's IT server room
Backup	Up to 7 Days from disaster period

THE DISASTER RECOVERY COORDINATOR

The function of the Disaster Recovery Coordinator is vitally important to maintaining the plan in a consistent state of readiness. The Recovery Coordinator's role is multifaceted. Not only does the Coordinator assume a lead position in the ongoing life of the plan, but the Coordinator is a member of the Continuity Management Team in the event of a computer disaster.

The primary responsibilities of the Disaster Recovery Plan Coordinator are as follows:

- Distribution of the Disaster Recovery Plan
- Training the Disaster Recovery Teams
- Testing of the Disaster Recovery Plan
- Evaluation of the Disaster Recovery Plan Tests
- Review, change and update the Disaster Recovery Plan

In a disaster situation, the Disaster Recovery Plan Coordinator will:

- Facilitate communication between technical and non-technical staff
- Act as a Project Manager to coordinate the efforts of
  - Technical staff
  - Business staff
  - Vendors
  - University Management
  - Other personnel as needed

The Information Technology Disaster Recovery Coordinator for Texas A&M University - Central Texas is Todd Lutz, Chief Information Officer. The alternate Information Technology Disaster Recovery Coordinator is Steve Blum.

THE COMMAND CENTER & VITAL RECORDS

A Command Center must be established when a disaster is declared. The Command Center serves as a focal point for all recovery operations. It also provides temporary office space for team members.

The Command Center should be stocked with adequate supplies including:

- Paper
- Pens
- Pencils
- Trash can(s)
- Post-it notes
- White boards
- Markers
- Erasers
- Telephones
- Fax machine(s)
- Copier(s)
- PCs
- A small tool kit
- Coffee pot
- Coffee
- Cups
- Other items that the team leaders might need to head the recovery effort

COMPANIES THAT HAVE SUCCESSFULLY RECOVERED FROM A DISASTER HAVE STATED THAT THE EXISTENCE OF A COMMAND CENTER WAS A KEY INGREDIENT IN THEIR RECOVERY EFFORTS.

COMMAND CENTER LOCATIONS

PRIMARY LOCATION

If the disaster event permits the location of the Command Center in Founders Hall, then the computer lab or other available classroom or office space will be utilized. If the evacuation from Founders Hall is required, the Command Center will be located in the computer lab or other available classroom or office space at the North Campus of Texas A&M University – Central Texas located at 701 Whitlow Drive, Killeen, Texas.

SECONDARY LOCATION

If evacuation from Founders Hall is required, the Command Center will be located in the computer lab or other available classroom or office space at the North Campus of Texas A&M University – Central Texas.

VITAL RECORDS RETRIEVAL

VITAL RECORDS FACILITY ADDRESS AND CONTACTS

Offsite Storage Location for disaster recovery plans, software licenses and server installation media:
TAMUCT North Campus
CONTACT: Police Dept.
701 Whitlow Dr.
Killeen, Texas
254-519-5777 (office/mobile)

OVERVIEW OF WHAT IS STORED OFFSITE

1. A current copy of this disaster recovery plan.
2. Copies of install disks for all relevant software and critical software/operating system licenses. These should be stored electronically rather than relying on Internet-downloadable versions. When the software is needed the same version of the software used may not be available on the Internet, or there may be Internet issues that could negatively affect large downloads or may significantly slow down the recovery process.

DISASTER RECOVERY TEAM

DISASTER RECOVERY MANAGEMENT TEAM (MGMT)

Sub-teams: Administration, Supplies and Public Relations

GENERAL RESPONSIBILITIES

TEAM OVERVIEW

The IT Disaster Recovery Management Team (MGMT) is responsible for the overall coordination of the disaster recovery process from an Information Technology Systems perspective. The other team leaders report to this team during a disaster. In addition to their management activities, members of this team will have administrative, supply, transportation, and public relations responsibilities during a disaster. Each of these responsibilities should be headed by a member of the MGMT team.

GENERAL ACTIVITIES

- Assess the damage and if necessary, declare a disaster (damage assessment
- forms are included in this plan)
- Coordinate efforts of all teams
- Secure financial backing for the recovery effort
- Approve all actions that were not preplanned
- Give strategic direction
- Be the liaison to upper management
- Expedite matters through all bureaucracy
- Provide counseling to those employees that request or require it

AFTER THE DISASTER

- Make recommendations on how the disaster recovery plan can be improved

ADMINISTRATIVE OVERVIEW

The administrative function provides administrative support services to any team requiring this support. This includes the hiring of temporary help or the reassignment of other clerical personnel.

ACTIVITIES BY PHASE

PROCEDURES DURING DISASTER RECOVERY ACTIVATION PHASE

- Notify all vendors and delivery services of change of address

PROCEDURES DURING ALL PHASES

- Process expense reports
- Account for the recovery costs
- Handle personnel problems

AFTER THE DISASTER

- Make recommendations on how the disaster recovery plan can be improved

SUPPLY OVERVIEW

The supply function is responsible for coordinating the purchase of all needed supplies during the disaster recovery period. Supplies include all computing equipment and supplies, office supplies such as paper and pencils, and office furnishings.

ACTIVITIES BY PHASE

PROCEDURES DURING DISASTER RECOVERY ACTIVATION PHASE

- Purchase supplies required by the teams at the alternate site.

PROCEDURES DURING REMOTE OPERATION/DATA CENTER REBUILD PHASE

- Work with university Purchasing to order replacement supplies and expedite shipments
- Ongoing distribution of supplies

PROCEDURES DURING RETURN HOME PHASE

- Restock supplies at the restored site

AFTER THE DISASTER

- Make recommendations on how the disaster recovery plan can be improved

PUBLIC RELATIONS OVERVIEW

The public relations function will pass appropriate information about the disaster and associated recovery process to the public and to employees. Every effort should be made to give these groups reason to believe that TAMUCT is doing everything possible to minimize losses and to ensure a quick return to normalcy.

ACTIVITIES BY PHASE

ALL PHASES

- Ensure that employees do not talk to the media
- Control information released to the public and to employees
- Interface with university Public Relations or defer to Senior Management
- Publish internal newsletters
- Keep everyone aware of recovery progress

AFTER THE DISASTER

- Make recommendations on how the disaster recovery plan can be improved

TEAM LEADER INFORMATION

CALLER	NAME	TELEPHONE
Primary	INFORMATION ON FILE	
Alternate		

TEAM MEMBER INFORMATION

NAME	TELEPHONE	FUNCTIONAL ASSIGNMENT
		Infrastructure
		Networks
INFORMATION ON FILE		University Administration
		Internal Communications
		Facilities
		Police & Security system
		Telephone system
		External Communications

TECH SUPPORT TEAM (TECH)

Sub-Teams: Hardware, Software, Network, Operations

HARDWARE RESPONSIBILITIES (HARD)

TEAM OVERVIEW

The responsibility of the Hardware Team is to acquire (along with the Facilities Team), configure and install servers and workstations for TAMUCT users.

ACTIVITIES BY PHASE

PROCEDURES DURING DISASTER RECOVERY ACTIVATION PHASE

- Determine scope of damage for servers and workstations
- Order appropriate equipment and supplies (coordinate and work with the Facilities Team for this activity)

PROCEDURES DURING REMOTE OPERATION/DATA CENTER REBUILD PHASE

- Set up servers and workstations
- Install software as necessary
- Restore data
- Install additional workstations as they arrive

PROCEDURES DURING RETURN HOME PHASE

- Notify users
- Ensure data is backed up
- Relocate equipment

AFTER THE DISASTER

- Make recommendations on how the disaster recovery plan can be improved

TEAM OVERVIEW

The responsibility of the Software Team is to maintain the systems software at the alternate site and reconstruct the system software upon returning to the primary site. In addition, the Software Team will provide technical support to the other teams.

ACTIVITIES BY PHASE

PROCEDURES DURING DISASTER RECOVERY ACTIVATION PHASE

- Provide technical support to the other teams
- Build servers and workstations
- Reinstall and configure systems at the primary site
- Test the hardware and software
- Work with appropriate vendors to assist in recovery
- Verify that the systems are performing as expected

PROCEDURES DURING REMOTE OPERATION/DATA CENTER REBUILD PHASE

- Provide technical support to the other teams
- Build servers and workstations
- Reinstall and configure systems at the primary site
- Test the hardware and software
- Work with appropriate vendors to assist in recovery
- Verify that the systems are performing as expected

PROCEDURES DURING RETURN HOME PHASE

- Provide technical support to the other teams
- Verify that the system is performing as expected

AFTER THE DISASTER

- Make recommendations on how the disaster recovery plan can be improved

TEAM OVERVIEW

The Network Team is responsible for preparing for voice and data communications to the alternate location data center and restoring voice and data communications at the primary site.

ACTIVITIES BY PHASE

PROCEDURES DURING DISASTER RECOVERY ACTIVATION PHASE

- Determine the requirements for voice and data communications
- Install the network including lines, routers, switches, controllers and other communications equipment at the alternate location data center
- Test the network

PROCEDURES DURING REMOTE OPERATION/DATA CENTER REBUILD PHASE

- Operate the backup network
- When the replacement equipment arrives at the primary site, install it

PROCEDURES DURING RELOCATION HOME PHASE

- Support the primary site network
- Dismantle the alternate location data center network

AFTER THE DISASTER

- Make recommendations on how the disaster recovery plan can be improved

OPERATIONS OVERVIEW

The Operations responsibilities include the daily operation of computer services and management of all backup tapes. When a disaster is declared, the team must secure the correct tapes for transport to the alternate location. Once operations are established at the alternate location, arrangements must be made with an offsite storage service.

ACTIVITIES BY PHASE

PROCEDURES DURING DISASTER RECOVERY ACTIVATION PHASE

- Inventory and select the correct backup tapes
- Transport the tapes to the alternate data center
- Assist all teams in restoring the production environment at the alternate data center

PROCEDURES DURING REMOTE OPERATION/DATA CENTER REBUILD PHASE

- Establish a production schedule at the alternate location
- Run the daily schedule at the alternate location
- Perform system and production backups at the alternate location
- Assist other teams in preparing the primary site
- Establish offsite storage at the alternate location

PROCEDURES DURING RETURN HOME PHASE

- Perform system and production backups
- Inventory all tapes at the alternate data center
- Transport all tapes from the alternate data center to the primary site

AFTER THE DISASTER

- Make recommendations on how the disaster recovery plan can be improved

TEAM LEADER INFORMATION

CALLER	NAME	TELEPHONE
PRIMARY	INFORMATION ON FILE	
ALTERNATE		

TEAM MEMBER INFORMATION

NAME	TELEPHONE	TIME CALLED/ COMMENTS
	INFORMATION ON FILE	

FACILITY TEAM (FACL)

Sub-teams: Salvage Team, New Data Center and New Hardware Team

SALVAGE RESPONSIBILITIES (SALV)

SALVAGE OVERVIEW

The Salvage Team is responsible for minimizing the damage at the primary site and to work with the insurance company for settlement of all claims. This depends on a quick determination of what equipment is salvageable and what is not. Repair and replacement orders will be filed for what is not in working condition. This team is also responsible for securing the disaster recovery data center.

ACTIVITIES BY PHASE

PROCEDURES DURING DISASTER RECOVERY ACTIVATION PHASE

- Establish the command center
- Assist in the immediate salvage operations
- Contact TAMUCT Insurance representatives
- Inventory all equipment in the data center. If necessary, involve the vendors.

PROCEDURES DURING REMOTE OPERATION/DATA CENTER REBUILD PHASE

- Salvage equipment and supplies
- Settle property claims with the insurance company
- Provide for security at the data center

AFTER THE DISASTER

- Make recommendations on how the disaster recovery plan can be improved

NEW DATA CENTER TEAM OVERVIEW

The New Data Center Team is responsible for locating the proper location for a new data center and overseeing the construction of it. This includes the environmental and security controls for the room.

ACTIVITIES BY PHASE

PROCEDURES DURING REMOTE OPERATION/DATA CENTER REBUILD PHASE

- Determine the requirements for a new data center
- Work with contractors and university staff on the details
- Oversee the construction of the new data center

PROCEDURES DURING RETURN HOME PHASE

- Ensure that all controls are working as designed

AFTER THE DISASTER

- Make recommendations on how the disaster recovery plan can be improved

NEW HARDWARE TEAM OVERVIEW

The New Hardware Team is responsible for ordering replacement hardware for equipment damaged in the disaster and installing it in the new or rebuilt data center. Depending on the age of the damaged hardware, replacement may not be one-for-one. All types of hardware are to be handled, including:

- Servers
- Printers
- Routers, Hubs, Switches
- Workstations
- Environmental systems
- UPS equipment

ACTIVITIES BY PHASE

PROCEDURES DURING DISASTER RECOVERY ACTIVATION PHASE

- Obtain a list of damaged and destroyed equipment

PROCEDURES DURING REMOTE OPERATION/DATA CENTER REBUILD PHASE

- Determine what new hardware should be ordered
- Order new hardware
- Arrange for installation and testing of the new hardware

AFTER THE DISASTER

- Make recommendations on how the disaster recovery plan can be improved

TEAM LEADER INFORMATION

CALLER	NAME	TELEPHONE
PRIMARY	INFORMATION ON FILE	
ALTERNATE		

TEAM MEMBER INFORMATION

NAME	TELEPHONE	TIME CALLED/ COMMENTS
	INFORMATION ON FILE	

SEQUENTIAL LIST OF DISASTER RECOVERY TASKS

This section presents a sequential list of tasks to be performed during the four phases of a disaster. The list suggests a recommended order. In an actual disaster, some tasks could very well be performed before this list suggests they be performed.

The tasks are numbered as follows. Tasks for phase one begin with an A, phase two tasks begin with a B, phase three with a C and phase four with a D. Task numbers are sequenced by 10. In the team column, the primary team is listed along with the sub-team function. In some instances, multiple teams are responsible for the performance of a task. All teams/sub-teams will be listed in these cases. When a task has been completed, put a check in the X column.

Sometimes, the sequence may change depending on the type of disaster or circumstances at the time. Some tasks are ongoing, that is they span the entire phase or disaster. An example of this is task B180, which states that the Management Team coordinates activities of all teams. Some tasks are contiguous with others in that they can all be performed simultaneously.

TASK NUMBER	PRIOR TASK	DESCRIPTION	TEAMS/ SUB-TEAMS	X
A010		Disaster Recovery Coordinator receives notification	MGMT/MGMT	
A020		Ensure that those affected by the problem are receiving emergency care	MGMT/MGMT	
A030	A010	Assemble the Management Team	MGMT/MGMT	
A040	A030	Assess damage and determine length of outage	MGMT/MGMT TECH/HARD	
A050	A040	Declare Disaster	MGMT/MGMT	
A060	A040	Make arrangements with Police/Security Firm to secure the damaged area.	MGMT/MGMT	
A070	A050	Advise upper management of decision	MGMT/MGMT	

TASK NUMBER	PRIOR TASK	DESCRIPTION	TEAMS/ SUB-TEAMS	X
B010	A050	Assemble Disaster Recovery Teams	MGMT/MGMT	
B020	B010	Activate the Command Center	FACL/SALV	
B030	B020	Notify all TAMUCT Personnel	MGMT/ADMN	
B040	B020	Gather offsite storage materials and tapes from offsite.	TECH/OPS	
B050	B020	Application leaders will notify Key Users. Provide them with the help desk number	TECH/SOFT	
B060	B020	Notify Hardware & Supply Vendors	MGMT/ADMN	
B070	B020	Notify Software Vendors	MGMT/ADMN	
B080	B020	Notify Insurance / Risk Manager	MGMT/ADMN	
B090	B020	Reassess the situation	MGMT/ADMN	
B100	B030	Work with executive management to prepare statements for the media	MGMT/PUB	
B110	B100	Determine where to operate an alternate data center	MGMT/MGMT	
B120	B110	Arrange for vendors to deliver equipment to the alternate data center	FACIL/SALV	
B130	B120	Secure the alternate data center	FACIL/SALV	
B140	B130	Coordinate arrival of equipment to the alternate data center	TECH/HARD	
B150	B130	If necessary, acquire temporary office space	MGMT/MGMT	
B160	B150	Gather and distribute supplies at the Command Center	MGMT/SUPP	
B170	B150	Begin assessment of salvageable equipment and supplies	FACL/SALV	
B180	B150	Coordinate activities of all teams	MGMT/MGMT	
B190	B180	Set up a central information desk at the Command Center	TECH/SOFT	
B200	B170	Pack and bring off-site materials to the alternate data center	TECH/OPS	
B210	B200	Reassess the situation	MGMT/MGMT	

TASK NUMBER	PRIOR TASK	DESCRIPTION	TEAMS/ SUB-TEAMS	X
B220	B200	Notify the Post Office of new address to deliver the mail	MGMT/ADMN	
B230	B210	Determine what the recovery point will be	TECH/OPS TECH/SOFT	
B240	B230	Notify Key Users of where the recovery point will be.	TECH/SOFT	
B250	B240	Make arrangements to process expenses during the disaster	MGMT/ADMN	
B260	B250	Prepare to receive shipped equipment	TECH/NET	
B280	B270	Restore the TAMUCT Servers	TECH/OPS TECH/SOFT	
B290	B280	Boot the TAMUCT servers	TECH/OPS	
B300	B290	Determine what information remote users will need to dial in to the alternate data center	TECH/NET	
B310	B300	Establish Communications from alternate data center to alternate work area	TECH/NET	
B330	B320	Test operating system	TECH/SOFT	
B340	B330	Test communications network	TECH/NET	
B350	B340	Test remote dial in	TECH/NET	
B360	B350	Begin restoration of application and user data	TECH/OPS TECH/SOFT TECH/SOFT	
B370	B360	Test applications	TECH/SOFT	
B380	B370	Provide reports to appropriate users	TECH/PROD	
B390	B380	Determine what other information users require	TECH/SOFT	
B400	B390	Reassess the situation	MGMT/MGMT	
B410	B400	Establish an operating schedule	TECH/SOFT MGMT/MGMT	
B420	B410	Notify users of system availability	TECH/SOFT	
B430	B420	Begin processing	TECH/OPS	
B440	B430	Determine who else needs to go to the alternate data center	MGMT/MGMT	
B450	B250	Take a complete inventory of the damaged facility	FACL/SALV	

TASK NUMBER	PRIOR TASK	DESCRIPTION	TEAMS/ SUB-TEAMS	X
B460	Ongoing	Provide counseling to employees that require or request it	MGMT/MGMT	

TASK NUMBER	PRIOR TASK	DESCRIPTION	TEAMS/ SUB-TEAMS	X
C010	ON-GOING	Maintain control over disaster recovery expenses	MGMT/ADMN	
C020	B450	Establish system and application backup procedures	TECH/OPS TECH/SOFT	
C030	B450	Establish report distribution procedures	TECH/OPS	
C040	C020	Arrange for an offsite storage facility at the alternate data center	TECH/OPS	
C050	C040	Order communications equipment and hardware	FACL/HARD	
C060	C050	Determine if a new permanent operating site is required	FACL/SALV MGMT/MGMT	
C070	B450	If necessary, establish a schedule to process all applications	TECH/SOFT MGMT/MGMT	
C080	C070	If necessary, notify users of processing schedule	TECH/SOFT	
C090	C080	If necessary, begin processing all applications	TECH/OPS	
C100	C060	Construct or repair data center	FACL/DCTR	
C110	C100	Install equipment as it arrives	FACL/HARD TECH/NET	
C120	Ongoing	Provide counseling to employees that require or request it	MGMT/MGMT	

TASK NUMBER	PRIOR TASK	DESCRIPTION	TEAMS/ SUB-TEAMS	X
D010	C110	Determine appropriate date to resume processing at permanent data center	MGMT/MGMT	
D020	D010	Complete processing and take final backups (make two copies)	TECH/SOFT	
D030	D020	Shut systems down	TECH/SOFT	
D040	D030	Move all equipment to permanent data center	ALL	
D050	D040	Install equipment	ALL	
D060	D050	Test Operating systems and applications	TECH/SOFT	
D070	D060	Switch communications from the alternate site to permanent data center	TECH/NET	
D080	D060	Arrange to have the rest of the tapes and documentation shipped	TECH/OPS	
D090	D060	Notify Users	TECH/SOFT	
D100	D080	Resume normal processing	TECH/OPS	
D110	D100	Prepare media statements	MGMT/PUB	
D120	D100	Complete final disaster expense reports	MGMT/ADMN	
D130	Ongoing	Provide counseling to employees that require or request it	MGMT/MGMT	
D140	D120	Update Disaster Recovery Plan based on lessons learned	MGMT/MGMT	

APPLICATION RECOVERY

APPLICATION RECOVERY PRIORITIES

TAMUCT's applications are identified and classified below in priority order.

Depending on when the disaster takes place, these priorities may change.

Tier 0 Applications (Hosted Applications - No special Disaster Recovery Plan Needed)

Application	Host Location	Disaster Recovery Restore Method
Public Web server	TAMU-CIS at College Station, TX	Restore will not be necessary since data and applications are stored at the host's data center
Public DNS	TAMU-CIS at College Station, TX	
Zimbra E-mail	TAMU-CIS at College Station, TX	
Banner Student information	Tarleton State University	
Blackboard LMS	Hosted by Blackboard	

Tier 1 Applications (5 days after LAN/WAN restore)

Application	Data Communication Method to Disaster Recovery Site	Disaster Recovery Restore Method
Active Directory (Faculty and Staff), DNS, DHCP	Backups stored at Tarleton	Restore from Backup
Active Directory (Students), DNS	Backups stored at Tarleton	Restore from Backup
File Server	Backups stored at Tarleton	Restore from Backup
Hyper-V Hosts	Backups stored at Tarleton	Restore from Backup
Print Server, Print Manager Pus	Backups stored at Tarleton	Restore from Backup
Gene6FTP	Backups stored at Tarleton	Restore from Backup

Tier 2 Applications (10 days after LAN/WAN restore)

Application	Data Communication Method to Disaster Recovery Site	Disaster Recovery Restore Method
NetID Provisioner	Backups stored at Tarleton	Restore from Backup
Wireless Controller	Backups stored at Tarleton	Restore from Backup

Tier 3 Applications (15 days after LAN/WAN restore)

Application	Data Communication Method to Disaster Recovery Site	Disaster Recovery Restore Method
Titanium	Backups stored at Tarleton	Restore from Backup
Minitab	Backups stored at Tarleton	Restore from Backup
WSUS	Backups stored at Tarleton	Restore from Backup
ManageEngine	Backups stored at Tarleton	Restore from Backup
Sysaid Help Desk	Backups stored at Tarleton	Restore from Backup

Tier 4 Applications (When Possible)

Application	Data Communication Method to Disaster Recovery Site	Disaster Recovery Restore Method
Ghost Servers	Backups stored at Tarleton	Restore from Backup
EZProxy	Backups stored at Tarleton	Restore from Backup
ILLiad	Backups stored at Tarleton	Restore from Backup
Evergreen	Backups stored at Tarleton	Restore from Backup
Symantec Enterprise Protection Manager	Backups stored at Tarleton	Restore from Backup
Academic servers for individual professors	None	None
Solarwinds	Backups stored at Tarleton	Restore from Backup

SOFTWARE LICENSE KEYS/ACTIVATION CODES

Software	Install Key	Notes
Microsoft Windows 7		
Microsoft Windows Server 2008	**INFORMATION ON FILE**	
Microsoft Office 2010		

APPLICATION DETAILS

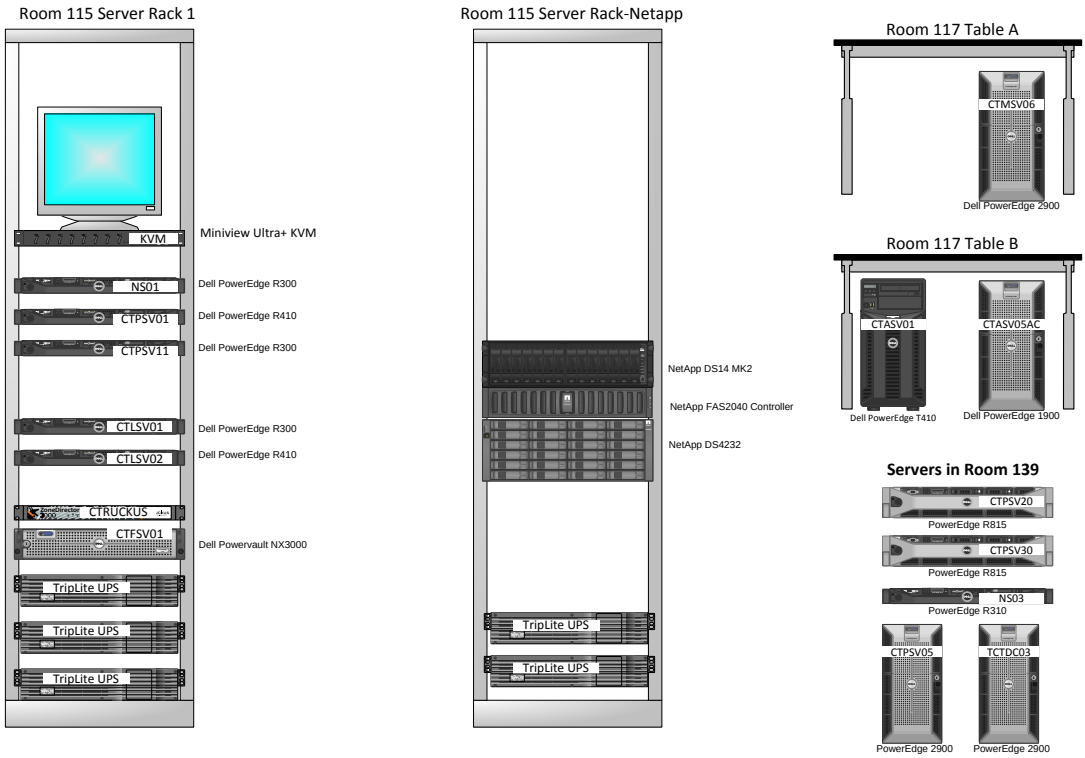
APPLICATION SOFTWARE PROFILE

Date Updated	**An Application Software Profile has been completed and is on file for each application system.**
Unique Application ID	
Application Name	
Owner (e.g., Department, Business Unit, Center, Professor, etc.)	
Custodian (e.g., departmental IT staff, college IT staff, CIS, vendor)	
Description	
User Base/Scope (e.g., Departmental employees, general public, students)	
Business Function	
Data Classification	
Criticality	
Date of Last Business Impact Analysis (BIA)	
Operating System	
Asset Tag	
Serial Number	
Licensing Information	
Vendor (or, internally developed)	
Maintenance Contract Expires	
Maintenance Contact	
Current Instances (e.g., production and test, test only, production only)	
Program Language(s)	
Internet Accessible	
Requires own server	
Desktop Data Storage (e.g., what files/configuration is required if app allows or requires storage of data on desktops)	
External File Requirements	
Domain Information	
Service Account(s)	
Storage Requirements	
Seats/Units	
Load Balancing	
License Requirements	
Protocol Requirements	
Port Requirements	
Network Requirements	
IP Address/Range	

Minimum Client Requirements	**An Application Software Profile has been completed and is on file for each application system.**
Encryption Requirements	
Third Party Requirements (e.g., applications or software required)	
Code Libraries	
Known Bottlenecks	
Batch Processing Details (e.g., scheduled tasks, duration, subtasks, etc.)	
Backup Software	
Backup Type	
Backup Frequency/Schedule	
Media	
Offsite Storage Location	
Generations Offsite	
Source Code Backed Up?	
Additional Details	
Maintenance Window Details	
Vendor /Internal contact information	
Recovery Point Objective (RPO)	
Recovery Time Objective (RTO)	
Priority	
Additional Details	
Supporting Documentation Location	
Additional Details	
Application is dependent on the following hardware resources:	
Business Processes dependent on this application:	
Applications/services etc. dependent on this resource:	
Applications/services etc. this resource is dependent on:	

SERVER RACK LAYOUT

Texas A&M University – Central Texas
Data Rack Layout



SERVER DETAILS

SERVER PROFILE

Date Updated	**A Server Profile has been completed and is on file for each server.**
Unique Hardware ID	
Hardware Name	
Owner (e.g., Department, Business Unit, Center, Professor, etc.)	
Custodian (e.g., departmental IT staff, college IT staff, CIS, vendor)	
User Base/Scope (e.g., Departmental employees, general public, students)	
Description	
Hardware Make/Model (e.g., Dell PowerEdge R200)	
Hardware Type	
Data Classification	
Criticality	
Recovery Time Objective (RTO)	
Date of Last Business Impact Analysis (BIA)	
Location (e.g., building & room)	
Rack ID (if applicable)	
Asset Tag	
Serial Number	
Model Number	
Vendor	
Warranty Expires	
Maintenance Contact	
BTU (cooling requirements)	
KVA (power consumption rate)	
Processor (# and type)	
Processor Speed	
Memory	
Storage Capacity	
RAID Level	
NIC(s)	
IP Address	
DNS Name	
Backup Location	
Replication Details	
Supporting Documentation Location	
Additional Details	

Applications Hosted	**A Server Profile has been completed and is on file for each server.**
Services Hosted	
Virtual Servers Hosted	
Business Processes	
Hardware/applications/services etc. dependent on this resource:	
Hardware/applications/services etc. this resource is dependent on:	

SERVER RECOVERY GENERAL INFORMATION

These procedures outline the steps required to restore any of TAMUCT's servers. Recovery for the servers assumes that:

- Good backup data exists and can be retrieved from offsite storage
- Replacement servers will be procured with equal or greater capacity
- Network connectivity will be re-established

A decision must be made as to where the recovery will take place (alternate site, primary location). This decision is not made ahead of time since the specifics of the incident requiring recovery is not known.

SERVER RECOVERY GENERAL TASK CHART

This section is designed to be used to recover any TAMUCT Server. Some steps are not applicable to all disaster situations.

TASK NUMBER	TASK DESCRIPTION	COMPLETED
S010	Assess the damage	
S020	Prioritize servers to recover	
S030	Order replacements for damaged equipment from vendors	
S040	Order appropriate cables, wires and network devices	
S050	Configure hardware as it arrives	
S060	Retrieve the backup hard drive from offsite storage	
S070	Test Server hardware	
S080	Install appropriate operating system on the server. Refer to the server info sheets to install the correct releases	
S090	Install network cards	
S100	Install cables on the server	
S110	Restore backed up data to the available disk drives using Windows Backup	
S120	Connect the servers to the network	
S130	Start applications for user verification	
S140	Contact users and coordinate verification	
S150	Verify user access to network	
S160	Resume normal processing	

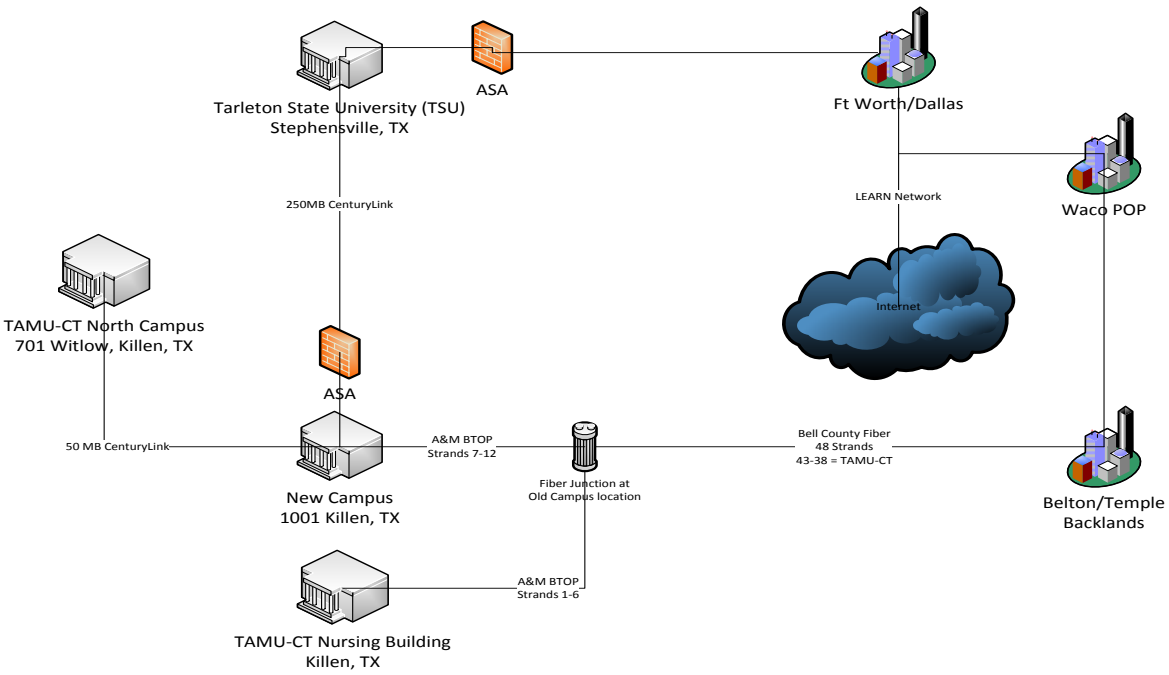
NETWORK RECOVERY

NETWORK RECOVERY PROCEDURES

Currently there is no direct communications path from any remote office sites to the DR data center at North Campus. The Nursing site and North Campus rely on connections through the primary MDF (room 105, Founders Hall). In the case of a disaster involving Founders Hall, it would be possible to reconfigure the existing WAN circuit (with the Centurylink and Tarleton assistance) at North Campus to connect to the Internet via Tarleton State.

For other locations such as the Nursing site, new WAN circuits will have to be installed which could take up to 30 days. Orders would be placed with Telecommunications providers as needed to establish connectivity between remaining offices and the DR data center. Firewalls, routers, and switches will need to be configured or settings changed to reflect the changes in the LAN and WAN.

Texas A&M of Central Texas WAN Diagram (After Move)



VOICE RECOVERY AT FOUNDERS HALL

In a disaster situation at Founders Hall involving the telephone system, support personnel from TAMU-Telecom will assist with recovering the VOIP system services and coordinate with the system vendor (Aastra). In the event of a complete system failure or major damage, the TAMU-Telecom site in College Station will serve as the temporary recovery point for TAMUCT's VOIP services for the headquarters at Founders Hall. Note that this requires network connectivity between the DR recovery site (at North Campus) and the TAMU network in College Station and reconfiguration of DID routing by the vendor.

If the entire VOIP system is lost at Founders Hall for an extended period of time, all phones services can be rerouted through the local carrier, CenturyLink, to the DR site at the TAMUCT North Campus which has a standalone NEC telephone system. Details are included in this section.

A disk containing the PBX configuration is stored offsite. Back up of the PBX and voice-mail is made once every two weeks and sent back offsite this is to insure up to date information.

Aastra/Clearspan VOIP system
Core equipment (including VM) Element Management Server IBM BladeCenter HT Package (DC Power) Application Blade Server Network Blade Server Media Blade Server Web Blade Server SIP Session Manager Blade Server UM Blade Server SurgeMail UM Software RHEL Basic Subscription (1 year) SIP Session Manager, up to 150 Concurrent Sessions AudioCodes 2PRI VoIP Gateway 48 V DC power plant and batteries 24 T1 channels (connected to CenturyLink for outside calls) 250 Digital telephone licenses 175 Unified communications licenses (voice mail) 24 Analog telephone ports 20 SIP trunk licenses
LOCATION: MDF, Room 105, Founders Hall
INITIAL RECOVERY: Initial recovery will be accomplished by routing VOIP services to the existing Texas A&M University VOIP system in College Station. When a new VOIP server is shipped, data and configuration backups will be used to restore the system at Founders Hall.

Place a call to [CONTACT NAME ON FILE] at CenturyLink Repair Center, at [TELEPHONE NUMBER ON FILE] and ask to have the lines and associated DID numbers forwarded to the circuit at North Campus:

Circuit ID# [ON FILE}

If additional circuits/lines are needed, contact [CONTACT NAME ON FILE] at [TELEPHONE NUMBER ON FILE] and make him/her aware that we have notified the repair center.

VOICE DISASTER DECISION TREE

SITUATION	PRIMARY RECOVERY OPTION
VOIP server is damaged, repairs will take more than 3 days.	1. Alert TAMU-Telecom Dept. (Telephone Number On File) of problem and request assistance. 2. With TAMU-Telecom support, redirect VOIP telephone sets to utilize the VOIP servers in College Station. 3. Temporarily route local PRI trunk(s) to College Station VOIP servers using the PRI gateway device at North Campus. (CenturyLink will need to assist with re-routing DID numbers) 4. After VOIP server is repaired, redirect PRI trunk(s) from the backup location back to Founders Hall.
VOIP server is destroyed, recover at DR site at North Campus, same central office	1. Alert TAMU-Telecom Dept. (Telephone Number On File) of problem and request vendor (Aastra) support. 2. With TAMU-Telecom support, redirect VOIP telephone sets to utilize the VOIP servers in College Station while recovery takes place at North Campus. (for outbound and long distance calling) 3. Route local DID numbers to North Campus NEC switch via existing PRI circuit. (CenturyLink will need to assist with re-routing DID numbers) 4. Work with Folkerson Comm. technicians to effect programming changes at North Campus on the NEC switch, install new NEC phones sets as required.
PBX destroyed, recover in new location, different central office (i.e. not in Killeen area)	1. Alert TAMU-Telecom Dept. (Telephone Number On File) of problem and request vendor (Aastra) support. 2. With TAMU-Telecom support, redirect VOIP telephone sets to utilize the VOIP servers in College Station while recovery takes place at recovery site. 3. Temporarily route local PRI trunk(s) to College Station VOIP servers via CenturyLink and IP trunking. 4. When replacement VOIP servers are in place at the selected recovery site, redirect local PRI circuit(s) to TAMUCT recovery system via IP trunking. 5. Redirect VOIP services from College Station to the replacement servers at recovery site.
Software failure	1. Alert TAMU-Telecom (Telephone Number On File) of problem and request assistance. 2. TAMU-Telecom support will notify vendor (Aastra) to initiate repairs or reinstallation of server software
Loss of long distance service via VOIP to Level 3	Outbound long distance service can be temporarily adjusted by reprogramming the Founders Hall VOIP server to use local Centurylink PRI trunks. Contact TAMU-Telecom to reconfigure.

DISASTER RECOVERY PLAN MAINTENANCE

The disaster recovery plan is a "living" document. Failure to keep it current could severely impact TAMUCT's ability to successfully recover in the event of a disaster.

Some information contained in the plan is more dynamic than other information. A matrix of events and the recommended maintenance schedule is included in this section. It is important to document changes to the plan and ensure that all copies of the plan are updated. An update log and list of personnel who possess a log are also included in this section.

Changes to the plan could occur more frequently than the time frames listed in the following table. Major hardware upgrades might affect business recovery contracts as well as this plan. Software changes, personnel changes and other changes that affect the plan should be updated as soon as possible, not just when the recommended intervals occur.

DISASTER RECOVERY PLAN RECOMMENDED MAINTENANCE

PERIOD	ACTION
Quarterly	Review all job changes and update plan with new personnel assignments
Quarterly	Have any new applications been implemented? If so, have all disaster recovery implications been addressed?
Quarterly	Have there been any major changes to existing applications? If so, update the recovery plan accordingly
Quarterly	Has the hardware configuration changed? If the changes affect your ability to recover, make appropriate changes to the recovery configuration.
Quarterly	Update the Network Configuration Diagrams
Quarterly	Visit the off-site storage location and ensure documentation is available and current
Quarterly	Ensure all team assignments are still valid
Quarterly	Ensure that all telephone lists are current
Semiannually	Test the plan and update it based on the results of the test
Annually	Review the tape retention requirements
Annually	Review the insurance coverage

DISASTER RECOVERY PLAN UPDATE LOG

PAGE(S) & SECTIONS AFFECTED	DESCRIPTION OF CHANGE	DATE

DISASTER RECOVERY PLAN DISTRIBUTION LIST

NAME	ENTIRE BOOK OR CHAPTERS
Offsite Storage	Entire

TRAINING THE DISASTER RECOVERY TEAM

The Disaster Recovery Coordinator is responsible for the coordination of training relating to the disaster recovery plan. The purpose of this training is twofold:

- To train recovery ream participants who are required to execute plan segments in the event of a disaster.

- To train TAMUCT management and key employees in disaster prevention and awareness and the need for disaster recovery planning.

The training of TAMUCT user management in disaster recovery planning benefits and objectives is crucial. A Disaster Recovery Plan must have the continued support from TAMUCT's user management to ensure future effective participation in plan testing and updating. As discussed later, it is not solely the responsibility of the Disaster Recovery Coordinator to initiate updates to the disaster recovery plan. User management must be aware of the basic recovery strategy; how the plan provides for rapid recovery of their information technology systems support structure; and how the plans effectiveness may be compromised without notification to the Disaster Recovery Coordinator as their business operations evolve and expand significantly.

It is the responsibility of each recovery team participant to fully read and comprehend the entire plan, with specific emphasis on their role and responsibilities as part of the recovery team. On-going training of the recovery team participants will continue through plan tests and review of the plan contents and updates provided by the Disaster Recovery Coordinator.

DISASTER RECOVERY TRAINING LOG

NAME	SIGNATURE	DATE

TESTING THE DISASTER RECOVERY PLAN

The Disaster Recovery Coordinator is responsible for testing of the disaster recovery plan at least annually to ensure the viability of the plan. On an on-going basis this frequency appears to be adequate considering the systems involved. However, special tests are to be given consideration whenever there has been a major revision to the plan or significant changes in the software, hardware or data communications have occurred.

The objectives of testing the disaster recovery plan are as follows:

- Simulate the conditions of an ACTUAL Business Recovery situation.
- Determine the feasibility of the recovery process
- Identify deficiencies in the existing procedures
- Test the completeness of the business recovery information stored at the Offsite Storage Location.
- Train members of the disaster recovery teams

The initial test of the plan will be in the form of a structured walk-through and should occur within two months of the disaster recovery plan's acceptance. Subsequent tests should be to the extent determined by the Disaster Recovery Coordinator that are cost effective and meet the benefits and objectives desired.

SAMPLE RECOVERY TEST AGENDA

1. What is the PURPOSE of the test?
2. What are the test OBJECTIVES?
3. How will the successful achievement of these objectives be measured?
4. At the conclusion of the test, collect test measurements from all participants.
5. Evaluate the test results. Determine if the test was successful or not.
6. Determine the implications of the test results. Does success for this test imply success in all recovery scenarios?
7. Update the plan based on results of the test.

RECOVERY TEST HISTORY

DATE	TYPE	OBJECTIVE	RESULTS

TEST DATE _____ **TEST #** _____

TEST OBJECTIVES:

1. _____

2. _____

3. _____

TASK NUMBER	TASK DESCRIPTION	COMPLETED
T010	Determine appropriate test date	
T020	Schedule a test date	
T030	Meet and plan preliminary test criteria and goals	
T040	Determine who will be participating in the test	
T050	Meet with entire test team to discuss goals and objectives	
T060	Determine hardware requirements	
T070	Determine software requirements	
T080	Determine printing requirements	
T090	Determine network requirements.	
T100	Determine what tapes need to be used for the test	
T110	Determine what other documentation needs to be brought to the test location	
T120	Determine if blank tapes are needed for test and plan accordingly	
T130	If necessary, call vendors with licensing dependent products and get required information to run products on the test systems	
T140	Get network specific information	
T150	Final meeting to review plans	
T160	Pack tapes and other supplies for test	

TASK NUMBER	TASK DESCRIPTION	COMPLETED
T170	Perform test following procedures in the test script	
T180	Conduct post-test debriefing before leaving test site	
T190	Remove data from test system disk drives	
T200	Destroy confidential information	
T210	Pack tapes for return home	
T220	Gather documentation from all test teams	
T230	Complete documenting the test	
T240	Meet with test participants and analyze the test	
T250	Update disaster recovery manual based on test results	

TEST SCRIPT TEST DATE: _ _/_ _/_ _ TEST #____

ESTIMATED START	ACTUAL START	FINISH	STEP DESCRIPTION

TEST EVALUATION

TEST DATE _____ TEST # ____

The Disaster Recovery Coordinator is responsible for coordinating the review and analysis of the test results and updating the plan accordingly.

The test participants should document the test results immediately after the plan test. The Disaster Recovery Coordinator reviews the test results with the teams during a postmortem meeting to discuss weaknesses and resolve problem areas. The Disaster Recovery Coordinator makes changes and updates to the plan accordingly.

1. Were the test objectives met?

---

2. What problems were encountered?

---

3. During the test, were there any deviations from the plan?

---

4. Were all of the materials used during the test retrieved from an offsite source? If not, what items from the data center or on-site offices were used?

PERSONNEL LISTING

This list should contain the contact information for all TAMUCT employees who are involved in the disaster recovery activities. The list should employees from several departments including ITS, Administration, Security, Maintenance, etc.

Similar information is contained in each team's section. This listing provides all of the contact information on one page.

LAST NAME	FIRST NAME	TEAM(S)	HOME PHONE	CELL PHONE

INFORMATION ON FILE

VENDOR LISTING

COMPANY NAME	CONTACT	PHONE NUMBERS	EMAIL ADDRESS	SUPPLY / RESOURCE

INFORMATION ON FILE

DAMAGE ASSESSMENT AND SALVAGE ACTIVITIES

DAMAGE ASSESSMENT AND SALVAGE CHECKLIST

This section contains checklists to help the Facilities and Hardware teams assess the damage to the systems and data center. Once the assessment is complete, notify the Management Team of the results of the assessment, and coordinate salvage of equipment where possible.

A. Assess the requirement for physical security to minimize possible injury to unauthorized persons entering the facility of eliminate the potential for vandalism to TAMUCT assets.

Initials: _____ Date: _____ Time: _____

B. Utilizing the following checklist as a guideline, survey the systems and data center facilities to assess damage upon notification from the Management Team of the need for damage assessment.

1. Building
    a. Exterior
    b. Interior

2. Computer Room
    a. Walls
    b. Ceiling
    c. Floor

3. Environmental/Control
    a. Electrical
        i. UPS
        ii. Transformers
        iii. Emergency/Building
    b. HVAC
        i. Air Handling
        ii. Air Conditioning

4. Fire Suppression

5. Data Center Contents
    a. Servers
    b. External Disk Drives
    c. Tape Backup
    d. Network Cabling
    e. Communications
    f. Workstations
    g. Other Equipment
    h. Tape Media

i. Spare Parts
j. Documentation

The purpose of the above checklist is to provide a guide in the review and assessment of damage following a disaster to TAMUCT facilities, the network and/or the data center. In using the checklist, the Damage Assessment and Salvage Teams must consider:

1. Is the area safe for employees or vendors to work in?

2. Can the equipment under examination function, and if so, at what percent of normal capacity?

3. What must be done to recover damaged equipment?

4. How long will it take to repair or replace the damaged equipment?

Initials: _____ Date: _____ Time: _____

C. Using the damage assessment, determine the estimated time to recover based on the following guidelines.

Level I Minimal damage to facility and/or equipment. Estimated time to complete repairs is less than 4 hours.

Level II Moderate damage to facility and/or equipment. Estimated time to complete repairs is between 4 hours and 2 business days.

Level III Extensive damage to facility and/or equipment. Estimate time to complete repairs is greater than 2 business days.

Initials: _____ Date: _____ Time: _____

D. Identify equipment, documentation or spare parts which are immediately salvageable or in need of repair.

Initials: _____ Date: _____ Time: _____

E. Verbally notify the Management Team of survey, assessment of damage, estimated time to recover from damage and potentially salvageable equipment.

Initials: _____ Date: _____ Time: _____

F. Document findings from the survey and damage assessment.

Initials: _____ Date: _____ Time: _____

G. Attend the recovery briefing as scheduled by the Disaster Recovery Coordinator to apprise Recovery Team members of findings.

   Initials: _____ Date: _____ Time: _____

H. A log is prepared and maintained to record all salvageable equipment and is disposition and location.

   Initials: _____ Date: _____ Time: _____

UNDER NO CIRCUMSTANCES SHOULD THE DAMAGE ASSESSMENT OR SALVAGE TEAM MAKE ANY PUBLIC STATEMENTS REGARDING THE DISASTER, ITS CAUSE OR ITS EFFECT ON THE OPERATION AT TAMUCT.

DAMAGE ASSESSMENT AND SALVAGE LOG

AREA OR EQUIPMENT ASSESSED	TYPE OF DAMAGE	COMMENTS	DAYS TO REPAIR OR "SCRAP"	INITIALS

EMERGENCY TELEPHONE NUMBERS

PERSON OR ORGANIZATION	TELEPHONE
TAMUCT Police Dept.	INFORMATION ON FILE
Facilities	
Human Resources	
Legal - TAMUS Office of General Counsel	
Insurance	
FBI (San Antonio Division)	
Killeen Fire Department	
Killeen Police Department	
Bell County Sheriff	
Texas Dept. of Public Safety	
Ambulance	
Red Cross	
Emergency Management Agency (Bell County)	
Environmental Emergencies (Leaks, Spills, Etc.)	
Gas Company	
Electric Company – Champion Energy	
Water Company – City of Killeen Water/Waste Water	
Telephone Company – Local Engineering/Construction	
Telephone Company – TAMU Telecom	
Cable	
Post Office	