

**INFORMATION TECHNOLOGY**

**DISASTER RECOVERY PLAN**

**Public Version**

**August 31, 2012**

Page 0 of 69 Information Technology Disaster Recovery Plan – Public Version August 31, 2012

**TABLE OF CONTENTS**

****

[TABLE OF CONTENTS](#page2) [i](#page2)

[INTRODUCTION](#page6) [1](#page6)

[HISTORY](#page6) [1](#page6)

[PLAN OVERVIEW](#page7) [2](#page7)

[PLAN APPROVAL](#page7) [2](#page7)

[DISASTER DECLARATION](#page8) [3](#page8)

[PERSONNEL AUTHORIZED TO DECLARE A DISASTER OR RESUME NORMAL OPERATIONS](#page8) [3](#page8)

[PLAN ACTIVATION](#page8) [3](#page8)

[RESUMPTION OF NORMAL OPERATIONS](#page8) [3](#page8)

[PLAN OVERVIEW, OBJECTIVES, AND DECISIONS](#page8) [3](#page8)

[PLAN OVERVIEW](#page8) [3](#page8)

[PLAN OBJECTIVES](#page9) [4](#page9)

[DISASTER RECOVERY PHASES](#page9) [4](#page9)

[DISASTER ASSESSMENT](#page9) [4](#page9)

[DISASTER RECOVERY ACTIVATION](#page10) [5](#page10)

[ALTERNATE SITE OPERATION/DATA CENTER REBUILD](#page10) [5](#page10)

[RETURN HOME](#page10) [5](#page10)

[KEY DISASTER RECOVERY ACTIVITIES](#page10) [5](#page10)

[DISASTER DECISION TREE](#page11) [6](#page11)

[DECISION MAKING FOR A DATA CENTER DISASTER](#page12) [7](#page12)

[RECOVERY TIME OBJECTIVES (RTO)](#page13) [8](#page13)

[RECOVERY POINT OBJECTIVES (RPO)](#page14) [9](#page14)

[THE DISASTER RECOVERY COORDINATOR](#page15) [10](#page15)

[THE COMMAND CENTER & VITAL RECORDS](#page16) [11](#page16)

[COMMAND CENTER LOCATIONS](#page17) [12](#page17)

[PRIMARY LOCATION](#page17) [12](#page17)

[SECONDARY LOCATION](#page17) [12](#page17)

[VITAL RECORDS RETRIEVAL](#page17) [12](#page17)

[VITAL RECORDS FACILITY ADDRESS AND CONTACTS](#page17) [12](#page17)

Page 1 of 69 Information Technology Disaster Recovery Plan – Public Version August 31, 2012

[OVERVIEW OF WHAT IS STORED OFFSITE](#page17) [12](#page17)

[DISASTER RECOVERY TEAM](#page18) [13](#page18)

[DISASTER RECOVERY MANAGEMENT TEAM (MGMT)](#page18) [13](#page18)

[GENERAL RESPONSIBILITIES](#page18) [13](#page18)

[ADMINISTRATIVE RESPONSIBILITIES (ADMN)](#page19) [14](#page19)

[SUPPLY RESPONSIBILITIES (SUPP)](#page20) [15](#page20)

[PUBLIC RELATIONS RESPONSIBILITIES (PUB)](#page21) [16](#page21)

[MANAGEMENT TEAM CALL CHECKLIST](#page22) [17](#page22)

[TECH SUPPORT TEAM (TECH)](#page23) [18](#page23)

[HARDWARE RESPONSIBILITIES (HARD)](#page23) [18](#page23)

[SOFTWARE RESPONSIBILITIES (SOFT)](#page24) [19](#page24)

[NETWORK RESPONSIBILITIES (NET)](#page25) [20](#page25)

[OPERATIONS RESPONSIBILITIES (OPS)](#page26) [21](#page26)

[TECH SUPPORT TEAM CALL CHECKLIST](#page27) [22](#page27)

[FACILITY TEAM (FACL)](#page28) [23](#page28)

[SALVAGE RESPONSIBILITIES (SALV)](#page28) [23](#page28)

[NEW DATA CENTER RESPONSIBILITIES (DCTR)](#page29) [24](#page29)

[NEW HARDWARE RESPONSIBILITIES (HARD)](#page30) [25](#page30)

[FACILITY TEAM CALL CHECKLIST](#page31) [26](#page31)

[SEQUENTIAL LIST OF DISASTER RECOVERY TASKS](#page32) [27](#page32)

[DISASTER ASSESSMENT PHASE](#page33) [28](#page33)

[DISASTER RECOVERY ACTIVATION PHASE](#page34) [29](#page34)

[ALTERNATE SITE OPERATION / DATA CENTER REBUILD PHASE](#page37) [32](#page37)

[RETURN HOME PHASE](#page38) [33](#page38)

[APPLICATION RECOVERY](#page39) [34](#page39)

[APPLICATION RECOVERY PRIORITIES](#page39) [34](#page39)

[Tier 0 Applications (Hosted Applications - No special Disaster Recovery Plan Needed)](#page39) [34](#page39)

[Tier 1 Applications (5 days after LAN/WAN restore)](#page39) [34](#page39)

[Tier 2 Applications (10 days after LAN/WAN restore)](#page39) [34](#page39)

[Tier 3 Applications (15 days after LAN/WAN restore)](#page40) [35](#page40)

[Tier 4 Applications (When Possible)](#page40) [35](#page40)

Page 2 of 69 Information Technology Disaster Recovery Plan – Public Version August 31, 2012

[SOFTWARE LICENSE KEYS/ACTIVATION CODES](#page41) [36](#page41)

[APPLICATION DETAILS](#page42) [37](#page42)

[APPLICATION SOFTWARE PROFILE](#page42) [37](#page42)

[SERVER RECOVERY](#page44) [39](#page44)

[SERVER RACK LAYOUT](#page44) [39](#page44)

[SERVER DETAILS](#page45) [40](#page45)

[SERVER PROFILE](#page45) [40](#page45)

[SERVER RECOVERY GENERAL INFORMATION](#page47) [42](#page47)

[SERVER RECOVERY GENERAL TASK CHART](#page48) [43](#page48)

[NETWORK RECOVERY](#page49) [44](#page49)

[NETWORK RECOVERY PROCEDURES](#page49) [44](#page49)

[NETWORK DIAGRAM](#page50) [45](#page50)

[VOICE RECOVERY AT FOUNDERS HALL](#page51) [46](#page51)

[PBX EQUIPMENT LISTING](#page52) [47](#page52)

[PROCEDURES FOR FORWARDING CALLS TO ANOTHER LOCATION](#page53) [48](#page53)

[VOICE DISASTER DECISION TREE](#page54) [49](#page54)

[DISASTER RECOVERY PLAN MAINTENANCE](#page55) [50](#page55)

[DISASTER RECOVERY PLAN RECOMMENDED MAINTENANCE](#page56) [51](#page56)

[DISASTER RECOVERY PLAN UPDATE LOG](#page57) [52](#page57)

[DISASTER RECOVERY PLAN DISTRIBUTION LIST](#page58) [53](#page58)

[TRAINING THE DISASTER RECOVERY TEAM](#page59) [54](#page59)

[DISASTER RECOVERY TRAINING LOG](#page60) [55](#page60)

[TESTING THE DISASTER RECOVERY PLAN](#page61) [56](#page61)

[SAMPLE RECOVERY TEST AGENDA](#page61) [56](#page61)

[RECOVERY TEST HISTORY](#page62) [57](#page62)

[SAMPLE RECOVERY TEST PLAN](#page63) [58](#page63)

[DISASTER RECOVERY PLAN TESTING FORMS](#page65) [60](#page65)

[TEST EVALUATION](#page66) [61](#page66)

[PERSONNEL LISTING](#page68) [63](#page68)

[VENDOR LISTING](#page69) [64](#page69)

[DAMAGE ASSESSMENT AND SALVAGE ACTIVITIES](#page70) [65](#page70)

Page 3 of 69 Information Technology Disaster Recovery Plan – Public Version August 31, 2012

[DAMAGE ASSESSMENT AND SALVAGE CHECKLIST](#page70) [65](#page70)

[DAMAGE ASSESSMENT AND SALVAGE LOG](#page73) [68](#page73)

[EMERGENCY TELEPHONE NUMBERS](#page74) [69](#page74)

Page 4 of 69 Information Technology Disaster Recovery Plan – Public Version August 31, 2012

**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.

Page 1 of 69 Information Technology Disaster Recovery Plan – Public Version August 31, 2012

**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

Page 2 of 69 Information Technology Disaster Recovery Plan – Public Version August 31, 2012

**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.

Page 3 of 69 Information Technology Disaster Recovery Plan – Public Version August 31, 2012

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.



Page 4 of 69 Information Technology Disaster Recovery Plan – Public Version August 31, 2012

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

Page 5 of 69 Information Technology Disaster Recovery Plan – Public Version August 31, 2012

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 |

Page 6 of 69 Information Technology Disaster Recovery Plan – Public Version August 31, 2012

DECISION MAKING FOR A DATA CENTER DISASTER



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

Page 7 of 69 Information Technology Disaster Recovery Plan – Public Version August 31, 2012

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.

Page 8 of 69 Information Technology Disaster Recovery Plan – Public Version August 31, 2012

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 |
|  |  |

Page 9 of 69 Information Technology Disaster Recovery Plan – Public Version August 31, 2012

**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 o Technical staff

o Business staff o Vendors

o University Management

o 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.

Page 10 of 69 Information Technology Disaster Recovery Plan – Public Version August 31, 2012

**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.

Page 11 of 69 Information Technology Disaster Recovery Plan – Public Version August 31, 2012

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.

Page 12 of 69 Information Technology Disaster Recovery Plan – Public Version August 31, 2012

**DISASTER RECOVERY TEAM**

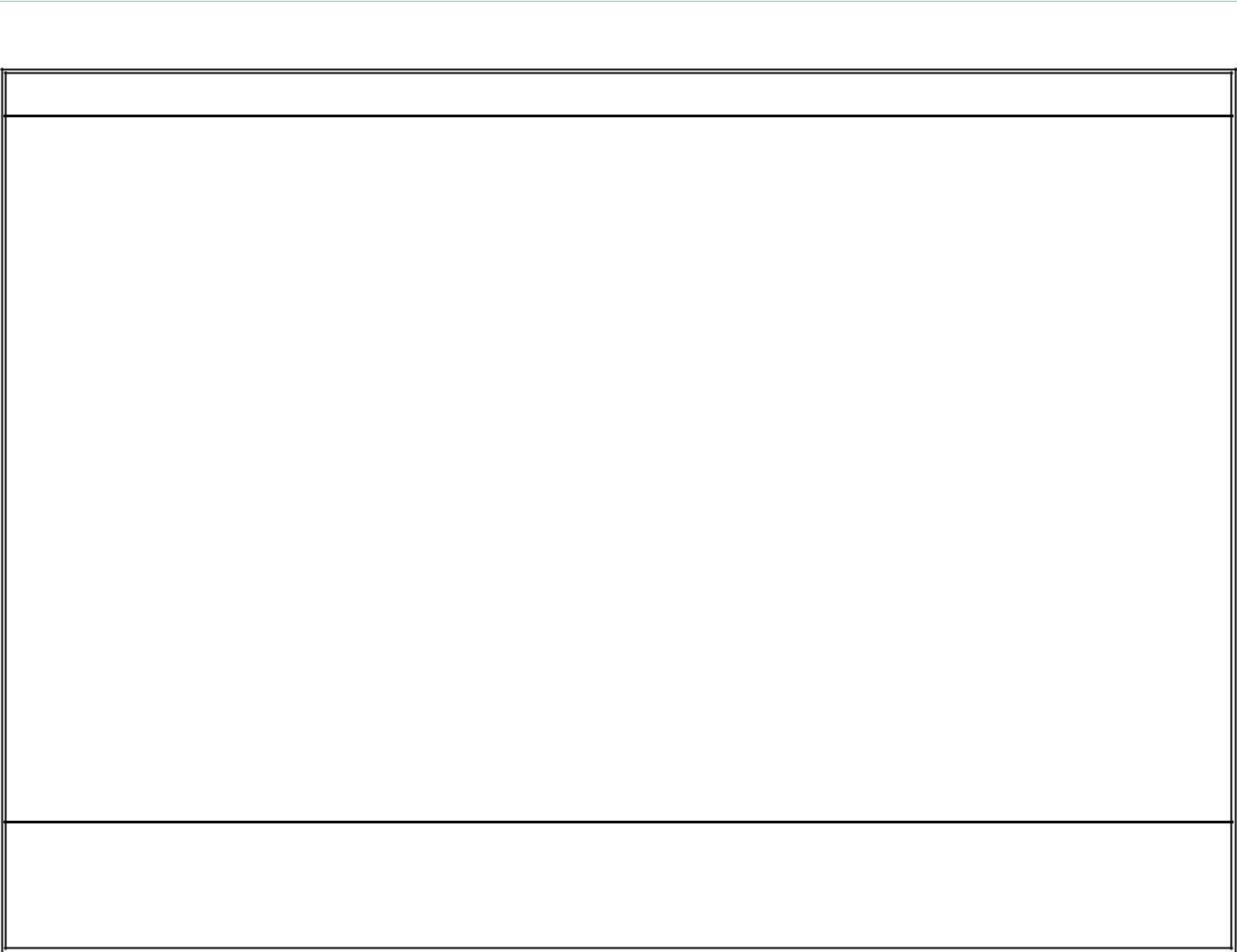
****

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

Page 13 of 69 Information Technology Disaster Recovery Plan – Public Version August 31, 2012

ADMINISTRATIVE RESPONSIBILITIES (ADMN)



**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

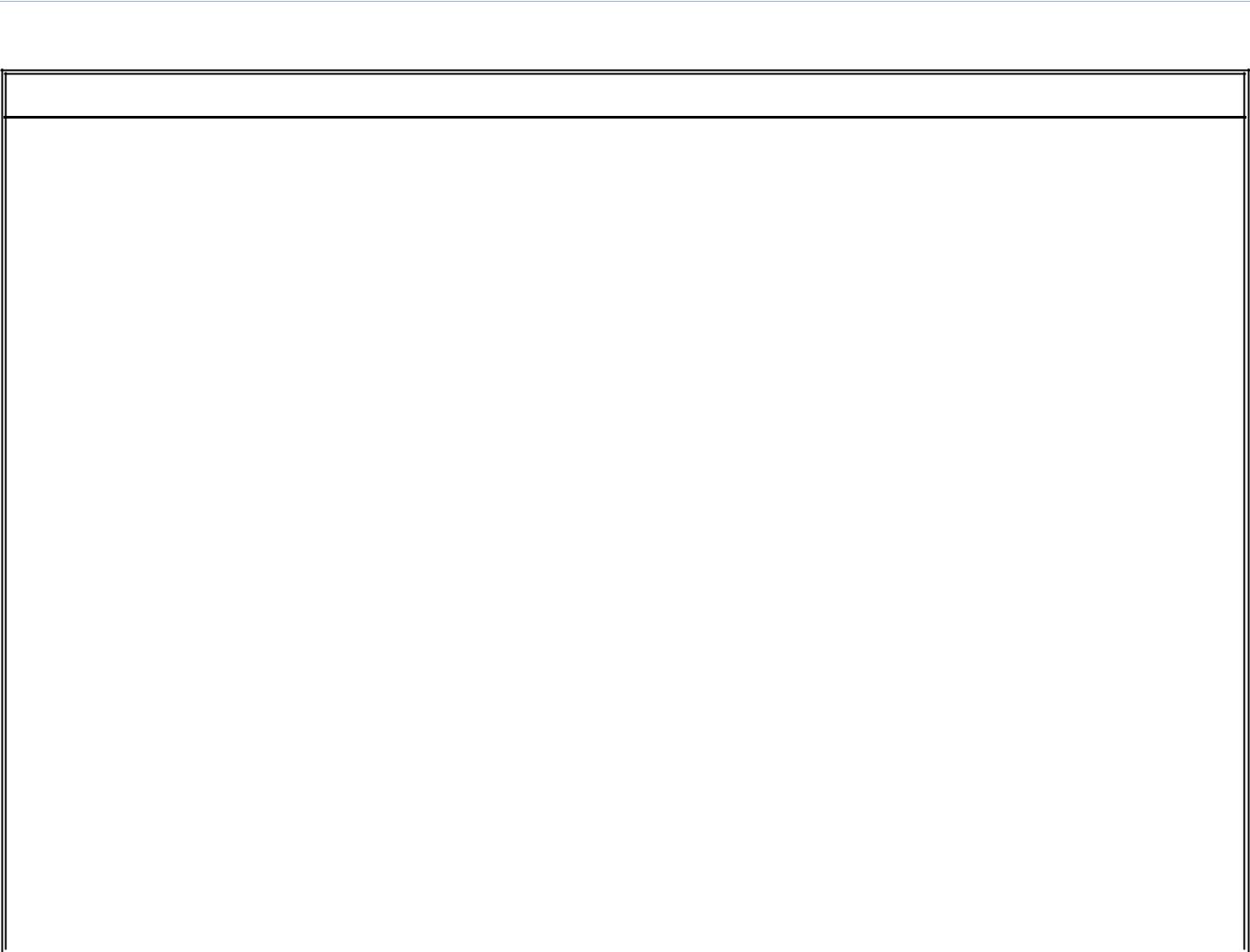
* Process expense reports
* Account for the recovery costs
* Handle personnel problems

AFTER THE DISASTER

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

Page 14 of 69 Information Technology Disaster Recovery Plan – Public Version August 31, 2012

SUPPLY RESPONSIBILITIES (SUPP)



**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

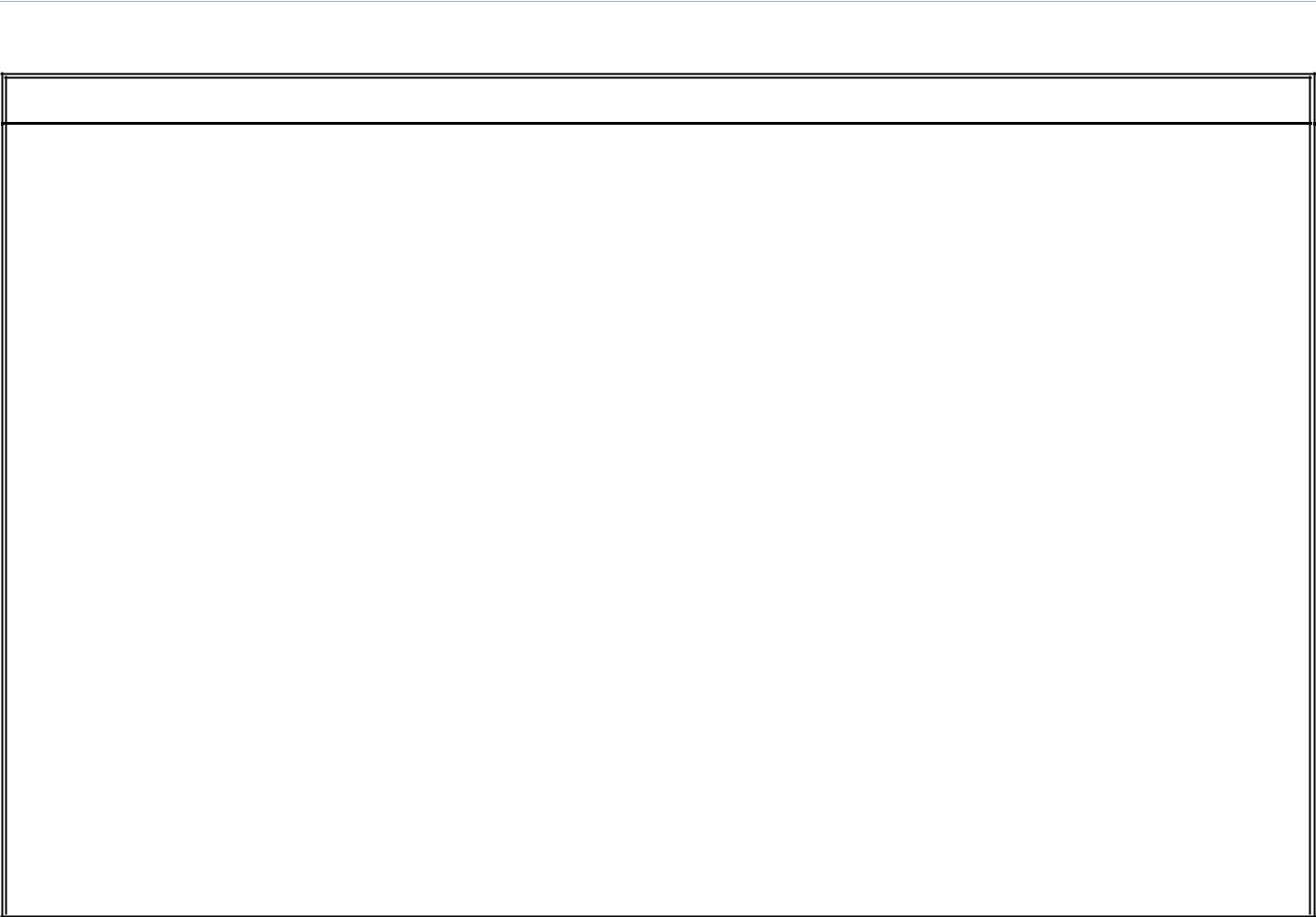
PROCEDURES DURING RETURN HOME PHASE  Restock supplies at the restored site

AFTER THE DISASTER

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

Page 15 of 69 Information Technology Disaster Recovery Plan – Public Version August 31, 2012

PUBLIC RELATIONS RESPONSIBILITIES (PUB)



**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

Page 16 of 69 Information Technology Disaster Recovery Plan – Public Version August 31, 2012

MANAGEMENT TEAM CALL CHECKLIST



**TEAM LEADER INFORMATION**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |
| **CALLER** |  | **NAME** |  |  | **TELEPHONE** | |
|  |  |  |  |  |  |  |
| Primary |  |  |  |  |  |  |
|  |  |  | **INFORMATION ON FILE** | |  |
|  |  |  |  |  |
| Alternate |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |  |
| **TEAM MEMBER INFORMATION** | | |  |  |  |  |
|  |  |  |  |  |  |  |
| **NAME** |  | **TELEPHONE** |  |  | **FUNCTIONAL ASSIGNMENT** | |
|  |  |  |  |  |  |  |
|  |  |  |  |  | Infrastructure | |
|  |  |  |  |  |  |  |
|  |  |  |  |  | Networks | |
|  |  |  |  |  |  |  |
|  |  |  |  |  | University Administration | |
|  | **INFORMATION ON FILE** | |  |  |
|  |  |  |  |  |
|  |  |  | Internal Communications | |
|  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  | Facilities | |
|  |  |  |  |  |  |  |
|  |  |  |  |  | Police & Security system | |
|  |  |  |  |  |  |  |
|  |  |  |  |  | Telephone system | |
|  |  |  |  |  |  |  |
|  |  |  |  |  | External Communications | |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |

Page 17 of 69 Information Technology Disaster Recovery Plan – Public Version August 31, 2012

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

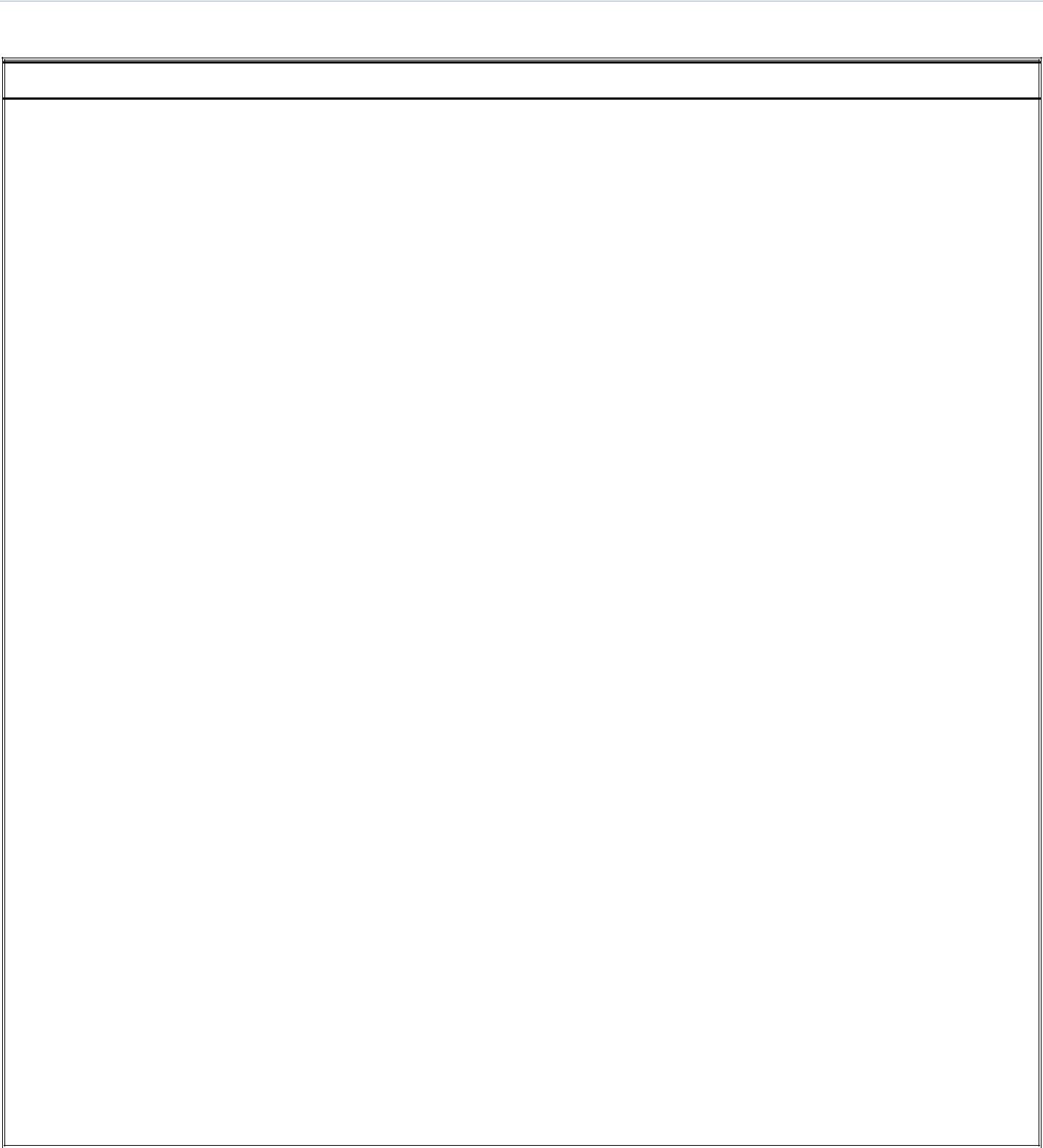
* Notify users
* Ensure data is backed up
* Relocate equipment

AFTER THE DISASTER

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

Page 18 of 69 Information Technology Disaster Recovery Plan – Public Version August 31, 2012

SOFTWARE RESPONSIBILITIES (SOFT)



**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

Page 19 of 69 Information Technology Disaster Recovery Plan – Public Version August 31, 2012

NETWORK RESPONSIBILITIES (NET)



**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

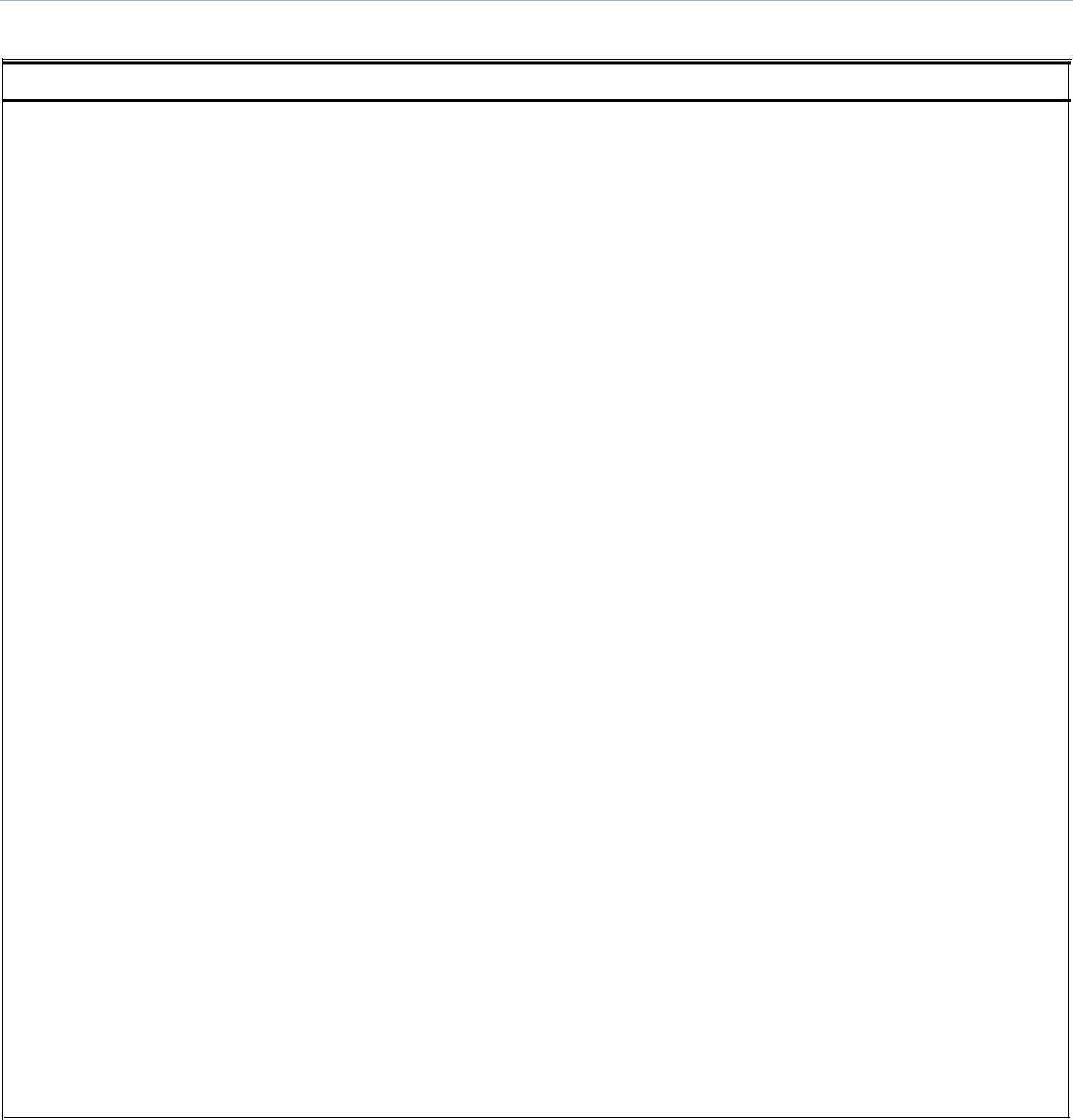
* Support the primary site network
* Dismantle the alternate location data center network

AFTER THE DISASTER

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

Page 20 of 69 Information Technology Disaster Recovery Plan – Public Version August 31, 2012

OPERATIONS RESPONSIBILITIES (OPS)



**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

Page 21 of 69 Information Technology Disaster Recovery Plan – Public Version August 31, 2012

TECH SUPPORT TEAM CALL CHECKLIST



**TEAM LEADER INFORMATION**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |
| **CALLER** | | **NAME** |  | **TELEPHONE** | | |
|  |  |  |  |  |  |  |
| PRIMARY | |  |  |  |  |  |
|  | **INFORMATION ON FILE** | | |  |
|  |  |  |  |
| ALTERNATE | |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
| **TEAM MEMBER INFORMATION** | |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
| **NAME** | | **TELEPHONE** |  | **TIME CALLED/ COMMENTS** | | |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |

**INFORMATION ON FILE**

Page 22 of 69 Information Technology Disaster Recovery Plan – Public Version August 31, 2012

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

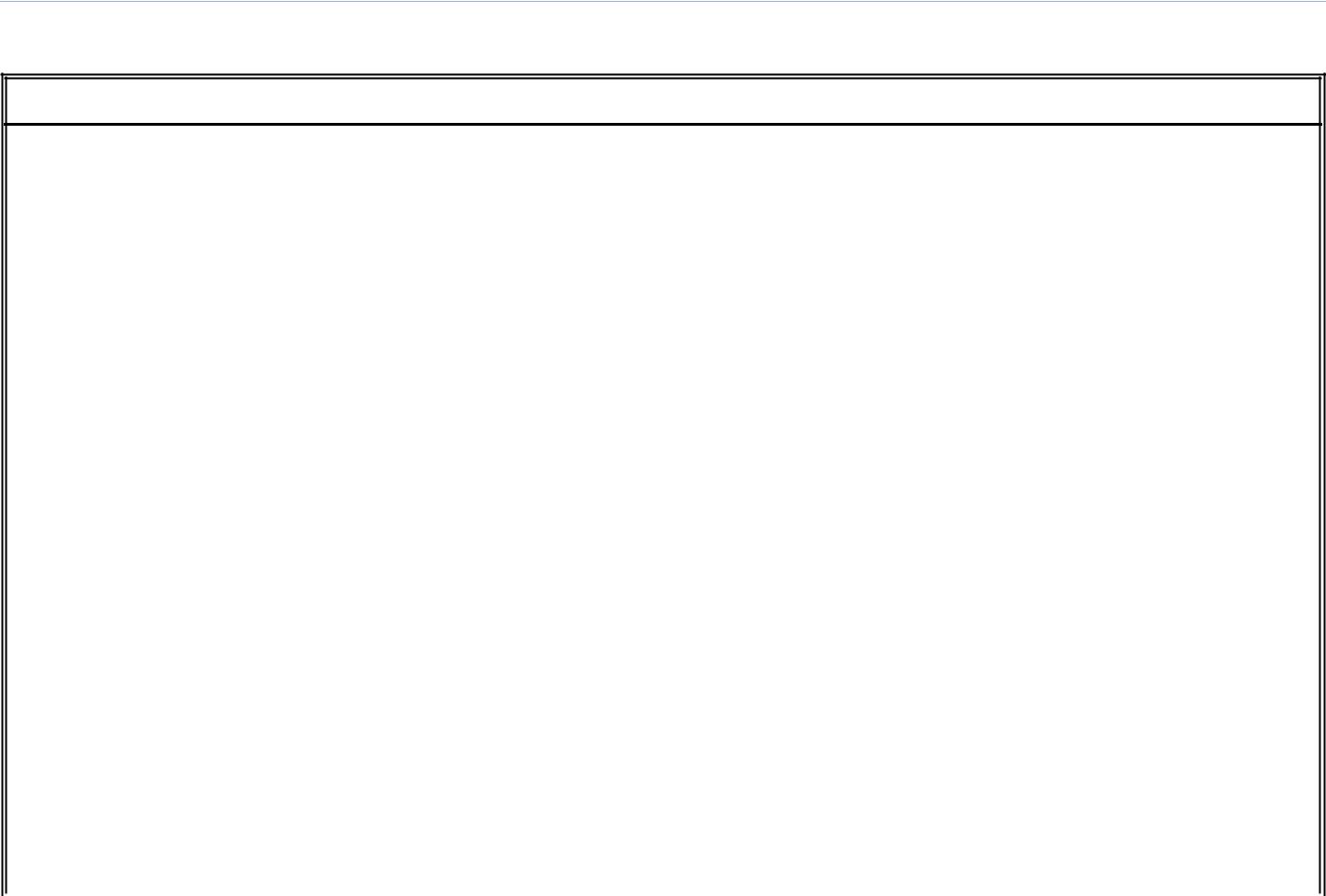
* Salvage equipment and supplies
* Settle property claims with the insurance company
* Provide for security at the data center

AFTER THE DISASTER

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

Page 23 of 69 Information Technology Disaster Recovery Plan – Public Version August 31, 2012

NEW DATA CENTER RESPONSIBILITIES (DCTR)



**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

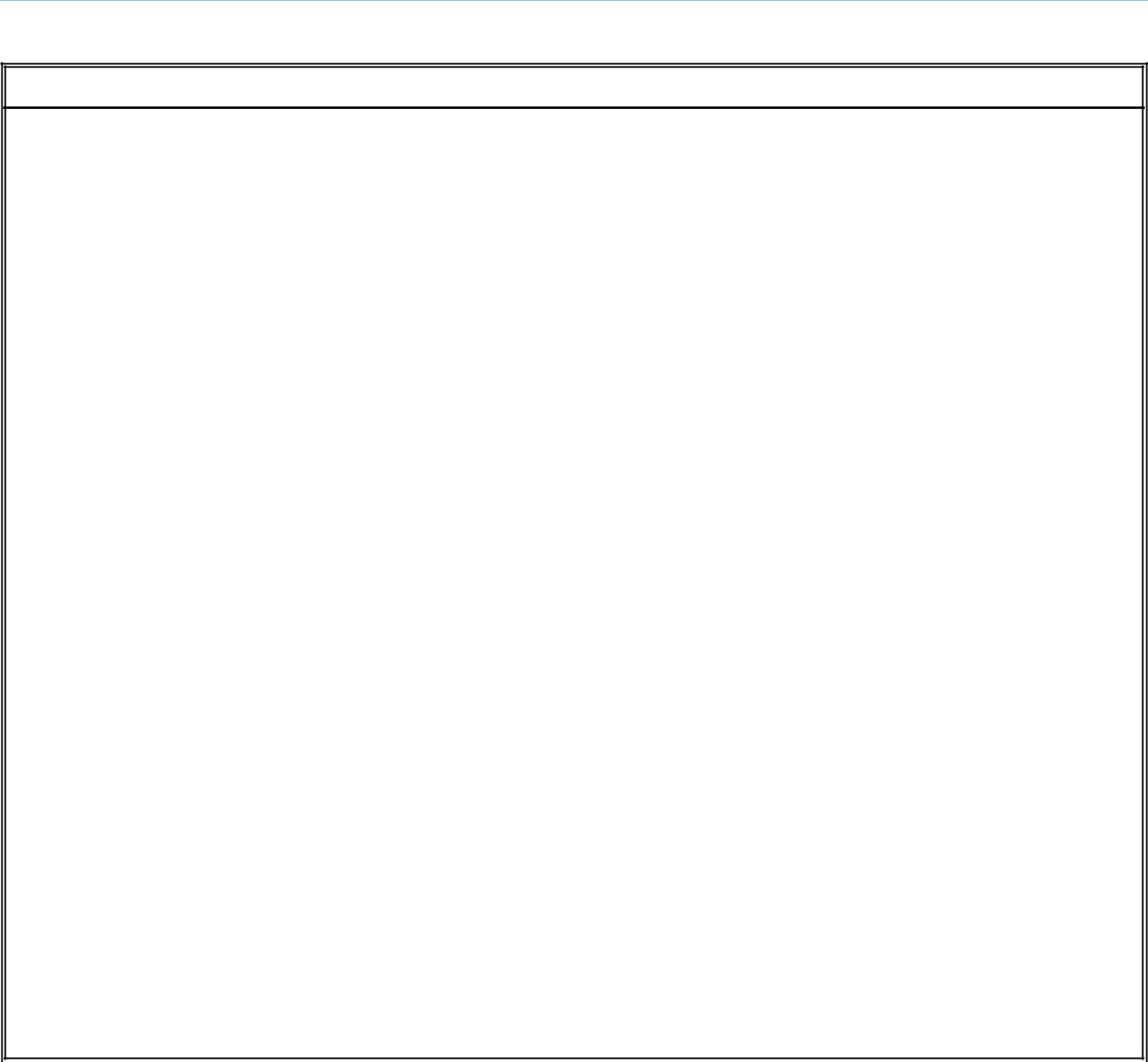
 Ensure that all controls are working as designed

AFTER THE DISASTER

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

Page 24 of 69 Information Technology Disaster Recovery Plan – Public Version August 31, 2012

NEW HARDWARE RESPONSIBILITIES (HARD)



**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

Page 25 of 69 Information Technology Disaster Recovery Plan – Public Version August 31, 2012

FACILITY TEAM CALL CHECKLIST



**TEAM LEADER INFORMATION**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |
| **CALLER** | | **NAME** | | **TELEPHONE** | | |
|  |  |  |  |  |  |  |
| PRIMARY | |  |  |  |  |  |
|  | **INFORMATION ON FILE** | | |  |
|  |  |  |  |
| ALTERNATE | |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
| **TEAM MEMBER INFORMATION** | |  |  |  |  |  |
|  |  |  |  |  |  |  |
| **NAME** | | **TELEPHONE** | | **TIME CALLED/ COMMENTS** | | |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  | **INFORMATION ON FILE** | |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |

Page 26 of 69 Information Technology Disaster Recovery Plan – Public Version August 31, 2012

**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.

Page 27 of 69 Information Technology Disaster Recovery Plan – Public Version August 31, 2012

DISASTER ASSESSMENT PHASE



|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  |  |  |  |
| **TASK** | **PRIOR** | **DESCRIPTION** | **TEAMS/** | **X** |
| **NUMBER** | **TASK** |  | **SUB-TEAMS** |  |
|  |  |  |  |  |
| A010 |  | Disaster Recovery Coordinator receives notification | MGMT/MGMT |  |
|  |  |  |  |  |
| A020 |  | Ensure that those affected by the problem are | MGMT/MGMT |  |
|  |  | receiving emergency care |  |  |
|  |  |  |  |  |
| 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 | MGMT/MGMT |  |
|  |  | secure the damaged area. |  |  |
|  |  |  |  |  |
| A070 | A050 | Advise upper management of decision | MGMT/MGMT |  |
|  |  |  |  |  |
|  |  |  |  |  |

Page 28 of 69 Information Technology Disaster Recovery Plan – Public Version August 31, 2012

DISASTER RECOVERY ACTIVATION PHASE



|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |
| **TASK** |  | **PRIOR** |  | **DESCRIPTION** | **TEAMS/** | **X** |
| **NUMBER** |  | **TASK** |  |  | **SUB-TEAMS** |  |
|  |  |  |  |  |  |  |
| 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 | TECH/OPS |  |
|  |  |  |  | tapes from offsite. |  |  |
|  |  |  |  |  |  |  |
| B050 |  | B020 |  | Application leaders will notify Key Users. Provide | TECH/SOFT |  |
|  |  |  |  | them with the help desk number |  |  |
|  |  |  |  |  |  |  |
| 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 | MGMT/PUB |  |
|  |  |  |  | statements for the media |  |  |
|  |  |  |  |  |  |  |
| B110 |  | B100 |  | Determine where to operate an alternate data | MGMT/MGMT |  |
|  |  |  |  | center |  |  |
|  |  |  |  |  |  |  |
| B120 |  | B110 |  | Arrange for vendors to deliver equipment to the | FACIL/SALV |  |
|  |  |  |  | alternate data center |  |  |
|  |  |  |  |  |  |  |
| B130 |  | B120 |  | Secure the alternate data center | FACIL/SALV |  |
|  |  |  |  |  |  |  |
| B140 |  | B130 |  | Coordinate arrival of equipment to the alternate | TECH/HARD |  |
|  |  |  |  | data center |  |  |
|  |  |  |  |  |  |  |
| B150 |  | B130 |  | If necessary, acquire temporary office space | MGMT/MGMT |  |
|  |  |  |  |  |  |  |
| B160 |  | B150 |  | Gather and distribute supplies at the Command | MGMT/SUPP |  |
|  |  |  |  | Center |  |  |
|  |  |  |  |  |  |  |
| B170 |  | B150 |  | Begin assessment of salvageable equipment and | FACL/SALV |  |
|  |  |  |  | supplies |  |  |
|  |  |  |  |  |  |  |
| B180 |  | B150 |  | Coordinate activities of all teams | MGMT/MGMT |  |
|  |  |  |  |  |  |  |
| B190 |  | B180 |  | Set up a central information desk at the Command | TECH/SOFT |  |
|  |  |  |  | Center |  |  |
|  |  |  |  |  |  |  |
| B200 |  | B170 |  | Pack and bring off-site materials to the alternate | TECH/OPS |  |
|  |  |  |  | data center |  |  |
|  |  |  |  |  |  |  |
| B210 |  | B200 |  | Reassess the situation | MGMT/MGMT |  |
|  |  |  |  |  |  |  |
|  | |  |  | | | |
| Page 29 of 69 | |  | Information Technology Disaster Recovery Plan – Public Version August 31, 2012 | | | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  |  |  |  |
| **TASK** | **PRIOR** | **DESCRIPTION** | **TEAMS/** | **X** |
| **NUMBER** | **TASK** |  | **SUB-TEAMS** |  |
|  |  |  |  |  |
| B220 | B200 | Notify the Post Office of new address to deliver the | MGMT/ADMN |  |
|  |  | mail |  |  |
|  |  |  |  |  |
| 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 | MGMT/ADMN |  |
|  |  | disaster |  |  |
|  |  |  |  |  |
| 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 | TECH/NET |  |
|  |  | to dial in to the alternate data center |  |  |
|  |  |  |  |  |
| B310 | B300 | Establish Communications from alternate data | TECH/NET |  |
|  |  | center to alternate work area |  |  |
|  |  |  |  |  |
| 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 | MGMT/MGMT |  |
|  |  | data center |  |  |
|  |  |  |  |  |
| B450 | B250 | Take a complete inventory of the damaged facility | FACL/SALV |  |
|  |  |  |  |  |
|  |  |  |  |  |

Page 30 of 69 Information Technology Disaster Recovery Plan – Public Version August 31, 2012

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

Page 31 of 69 Information Technology Disaster Recovery Plan – Public Version August 31, 2012

ALTERNATE SITE OPERATION / DATA CENTER REBUILD PHASE



|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  |  |  |  |
| **TASK** | **PRIOR** | **DESCRIPTION** | **TEAMS/** | **X** |
| **NUMBER** | **TASK** |  | **SUB-TEAMS** |  |
|  |  |  |  |  |
| 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 | TECH/OPS |  |
|  |  | data center |  |  |
|  |  |  |  |  |
| C050 | C040 | Order communications equipment and hardware | FACL/HARD |  |
|  |  |  |  |  |
| C060 | C050 | Determine if a new permanent operating site is | FACL/SALV |  |
|  |  | required | MGMT/MGMT |  |
|  |  |  |  |  |
| C070 | B450 | If necessary, establish a schedule to process all | TECH/SOFT |  |
|  |  | applications | 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 | MGMT/MGMT |  |
|  |  | request it |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

Page 32 of 69 Information Technology Disaster Recovery Plan – Public Version August 31, 2012

RETURN HOME PHASE



|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  |  |  |  |
| **TASK** | **PRIOR** | **DESCRIPTION** | **TEAMS/** | **X** |
| **NUMBER** | **TASK** |  | **SUB-TEAMS** |  |
|  |  |  |  |  |
| D010 | C110 | Determine appropriate date to resume processing | MGMT/MGMT |  |
|  |  | at permanent data center |  |  |
|  |  |  |  |  |
| D020 | D010 | Complete processing and take final backups | TECH/SOFT |  |
|  |  | (make two copies) |  |  |
|  |  |  |  |  |
| 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 | TECH/NET |  |
|  |  | permanent data center |  |  |
|  |  |  |  |  |
| D080 | D060 | Arrange to have the rest of the tapes and | TECH/OPS |  |
|  |  | documentation shipped |  |  |
|  |  |  |  |  |
| 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 | MGMT/MGMT |  |
|  |  | request it |  |  |
|  |  |  |  |  |
| D140 | D120 | Update Disaster Recovery Plan based on lessons | MGMT/MGMT |  |
|  |  | learned |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

Page 33 of 69 Information Technology Disaster Recovery Plan – Public Version August 31, 2012

**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 |  |  |  |
|  |  |  |  |  |  |  |
| Public DNS |  |  | TAMU-CIS at College Station, TX |  |  | Restore will not be necessary |
|  |  |  |  |  |  |
|  |  |  |  |  |  |  |
| Zimbra E-mail |  |  | TAMU-CIS at College Station, TX |  |  | since data and applications are |
|  |  |  |  |  |  | stored at the host’s data center |
| Banner Student information |  |  | Tarleton State University |  |  |
|  |  |  |  |  |
|  |  |  |  |  |  |  |
| Blackboard LMS |  |  | Hosted by Blackboard |  |  |  |
|  |  |  |  |  |  |  |

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



|  |  |  |  |
| --- | --- | --- | --- |
| **Application** | **Data Communication Method** | **Disaster Recovery** |  |
|  | **to Disaster Recovery Site** | **Restore Method** |  |
|  |  |
|  |  |  |  |
| Active Directory (Faculty and | Backups stored at Tarleton | Restore from Backup |  |
| Staff), DNS, DHCP |  |  |  |
|  |  |  |  |
| 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** | **Disaster Recovery** |  |
|  | **to Disaster Recovery Site** | **Restore Method** |  |
|  |  |
|  |  |  |  |
| NetID Provisioner | Backups stored at Tarleton | Restore from Backup |  |
|  |  |  |  |
| Wireless Controller | Backups stored at Tarleton | Restore from Backup |  |
|  |  |  |  |
|  |  |  |  |

Page 34 of 69 Information Technology Disaster Recovery Plan – Public Version August 31, 2012

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



|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Application** | **Data Communication Method** |  | **Disaster Recovery** |  |  |
|  | **to Disaster Recovery Site** |  | **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** |  |  |
|  | **Disaster Recovery Site** |  | **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 | Backups stored at Tarleton |  | Restore from Backup |  |  |
| Manager |  |  |  |  |  |
|  |  |  |  |  |  |
| Academic servers for individual | None |  | None |  |  |
| professors |  |  |  |  |  |
|  |  |  |  |  |  |
| Solarwinds | Backups stored at Tarleton |  | Restore from Backup |  |  |
|  |  |  |  |  |  |

Page 35 of 69 Information Technology Disaster Recovery Plan – Public Version August 31, 2012

SOFTWARE LICENSE KEYS/ACTIVATION CODES



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

Page 36 of 69 Information Technology Disaster Recovery Plan – Public Version August 31, 2012

APPLICATION DETAILS



APPLICATION SOFTWARE PROFILE



|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Date Updated |  |  |  |  |
|  |  |  |  |
| 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 |  | **An Application Software** | |  |
| Licensing Information | |  |
|  |  |  |
| Vendor |  | **Profile has been completed** | |  |
| (or, internally developed) | | **and is on file for each** | |  |
| Maintenance Contract Expires | | **application system.** | |  |
| 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 |  |  |  |  |
| Page 37 of 69 | Information Technology Disaster Recovery Plan – Public Version | | August 31, 2012 | |

|  |  |  |
| --- | --- | --- |
| Minimum Client Requirements |  |  |
|  |  |
| 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 | **An Application Software** |  |
| Generations Offsite | **Profile has been completed** |  |
| Source Code Backed Up? | **and is on file for each** |  |
| Additional Details | **application system.** |  |
| 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: |  |  |
|  |  |

Page 38 of 69 Information Technology Disaster Recovery Plan – Public Version August 31, 2012

**SERVER RECOVERY**

****

SERVER RACK LAYOUT

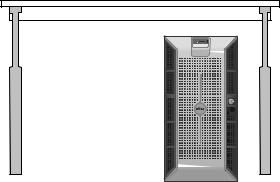
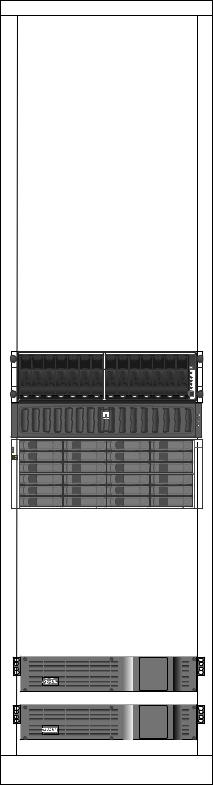
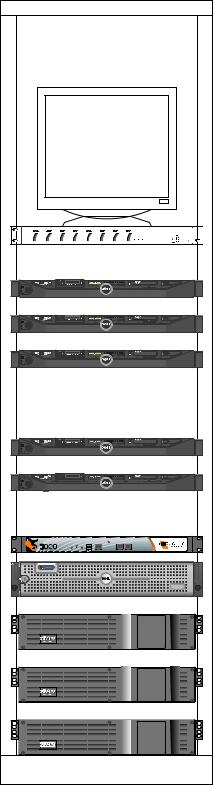


**Texas A&M University – Central Texas**

**Data Rack Layout**

Room 115 Server Rack 1 Room 115 Server Rack-Netapp

Room 117 Table A



CTMSV06

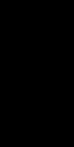
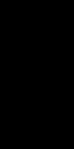
Dell PowerEdge 2900

KVM

|  |  |  |  |
| --- | --- | --- | --- |
| Miniview Ultra+ KVM |  | Room 117 Table B | |
|  |  |
|  |  |  |  |
|  |  |  |  |



|  |  |
| --- | --- |
| NS01 | Dell PowerEdge R300 |
|  |



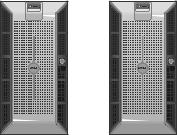
|  |  |  |
| --- | --- | --- |
| CTPSV01 | Dell PowerEdge R410 |  |
| CTASV01 | CTASV05AC |
|  |

|  |  |
| --- | --- |
| CTPSV11 | Dell PowerEdge R300 |
|  |

|  |  |  |
| --- | --- | --- |
|  | NetApp DS14 MK2 |  |
|  | NetApp FAS2040 Controller | Dell PowerEdge 1900 |
| CTLSV01 | Dell PowerEdge T410 |
| Dell PowerEdge R300 |  |

NetApp DS4232

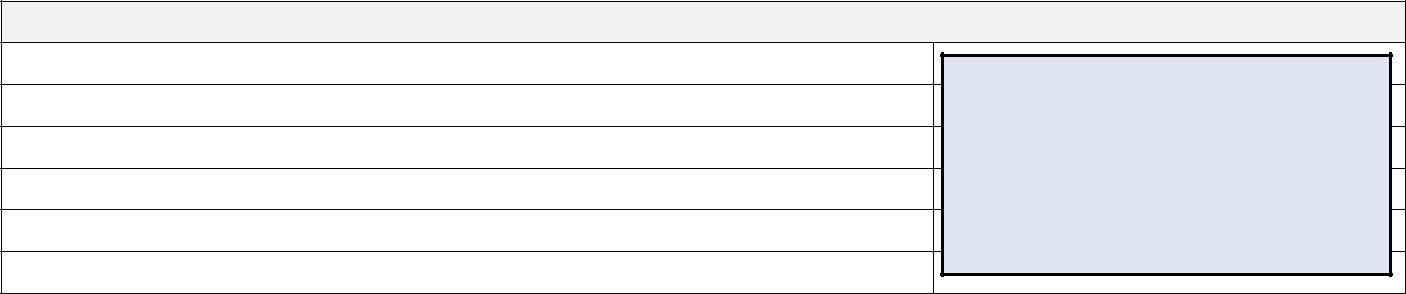
|  |  |  |  |
| --- | --- | --- | --- |
|  | CTLSV02 | Dell PowerEdge R410 |  |
|  | **Servers in Room 139** | |
|  |  |
| **ZoneDirector** | CTRUCKUS |  | CTPSV20 |
|  |  |
|  | CTFSV01 | PowerEdge R815 | |
|  | Dell Powervault NX3000 |  |
|  |  | CTPSV30 |
|  |  |  |
|  |  | PowerEdge R815 | |
| TripLite UPS | |  | NS03 |
|  |  |  |
|  |  | PowerEdge R310 | |
| TripLite UPS | | TripLite UPS |  |
|  |  |
|  |  | CTPSV05 | TCTDC03 |
| TripLite UPS | | TripLite UPS |  |
|  |  |



PowerEdge 2900 PowerEdge 2900

Page 39 of 69 Information Technology Disaster Recovery Plan – Public Version August 31, 2012

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| SERVER DETAILS |  |  |  |  |  |
|  |  |  |  |  |  |
| SERVER PROFILE |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
| Date Updated |  |  |  |  |  |
| 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) | | **A Server Profile has been** | |  |  |
| Rack ID (if applicable) | | **completed and is on file for** | |  |  |
| Asset Tag |  |  |  |
|  | **each server.** | |  |  |
| 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 |  |  |  |  |  |
|  |  |  |  |  |
| Page 40 of 69 | Information Technology Disaster Recovery Plan – Public Version | | August 31, 2012 | | |



Applications Hosted

Services Hosted

Virtual Servers Hosted

Business Processes

Hardware/applications/services etc. dependent on this resource:

Hardware/applications/services etc. this resource is dependent on:

**A Server Profile has been completed and is on file for each server.**

Page 41 of 69 Information Technology Disaster Recovery Plan – Public Version August 31, 2012

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.

Page 42 of 69 Information Technology Disaster Recovery Plan – Public Version August 31, 2012

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** | **TASK DESCRIPTION** | **COMPLETED** |
| **NUMBER** |  |  |
|  |  |  |
| 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 |  |
|  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

Page 43 of 69 Information Technology Disaster Recovery Plan – Public Version August 31, 2012

**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.

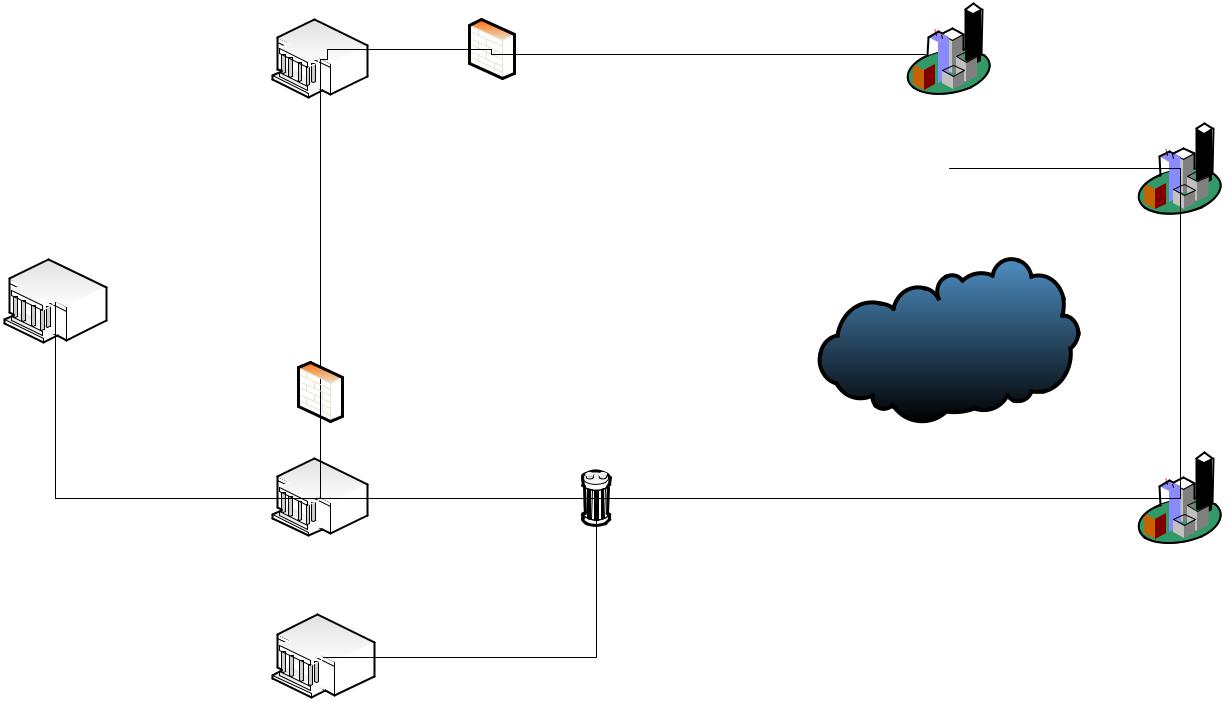
For other locations such as the Nursing site, new WAN circuits will have to be installed which could take up to 30 days. Orders would be placed with Telecommunications providers as needed to establish connectivity between remaining offices and the DR data center. Firewalls, routers, and switches will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

Page 44 of 69 Information Technology Disaster Recovery Plan – Public Version August 31, 2012

NETWORK DIAGRAM



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



|  |  |
| --- | --- |
|  | ASA |
| Tarleton State University (TSU) | Ft Worth/Dallas |
| Stephensville, TX |  |

250MB CenturyLink

LEARN Network

Waco POP

Internet

TAMU-CT North Campus

701 Witlow, Killen, TX

ASA

Bell County Fiber

A&M BTOP

50 MB CenturyLink 48 Strands

Strands 7-12

43-38 = TAMU-CT

Fiber Junction at

New Campus Old Campus location

1001 Killen, TX

Belton/Temple

Backlands

A&M BTOP

Strands 1-6

TAMU-CT Nursing Building

Killen, TX

Page 45 of 69 Information Technology Disaster Recovery Plan – Public Version August 31, 2012

**VOICE RECOVERY AT FOUNDERS HALL**

****

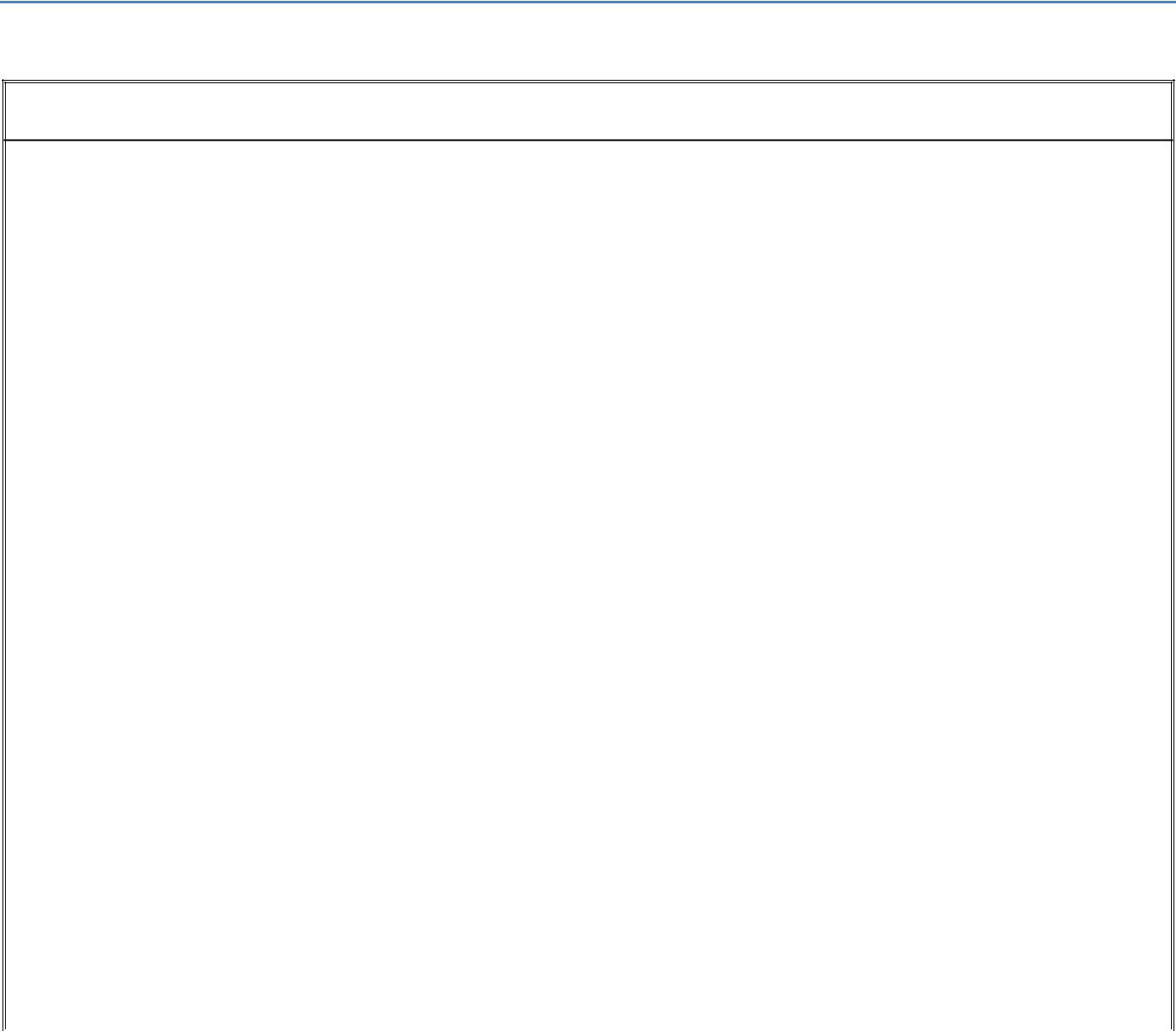
In a disaster situation at Founders Hall involving the telephone system, support personnel from TAMU-Telecom will assist with recovering the VOIP system services and coordinate with the system vendor (Aastra). In the event of a complete system failure or major damage, the TAMU-Telecom site in College 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.

Page 46 of 69 Information Technology Disaster Recovery Plan – Public Version August 31, 2012

PBX EQUIPMENT LISTING



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 existingTexas 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.

Page 47 of 69 Information Technology Disaster Recovery Plan – Public Version August 31, 2012

PROCEDURES FOR FORWARDING CALLS TO ANOTHER LOCATION



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.

Page 48 of 69 Information Technology Disaster Recovery Plan – Public Version August 31, 2012

VOICE DISASTER DECISION TREE



|  |  |  |  |
| --- | --- | --- | --- |
|  |  |  |  |
| **SITUATION** |  | **PRIMARY RECOVERY OPTION** |  |
|  | |  | |
| VOIP server is damaged, repairs will take | | 1. Alert TAMU-Telecom Dept. (Telephone Number On | |
| more than 3 days. |  | 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 | | 1. Alert TAMU-Telecom Dept. (Telephone Number On | |
| at North Campus, same central office | | 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, | | 1. Alert TAMU-Telecom Dept. (Telephone Number On | |
| different central office (i.e. not in Killeen | | File) of problem and request vendor (Aastra) support. | |
| area) |  | 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 | | Outbound long distance service can be temporarily | |
| Level 3 |  | adjusted by reprogramming the Founders Hall VOIP | |
|  |  | server to use local Centurylink PRI trunks. Contact | |
|  |  | TAMU-Telecom to reconfigure. |  |
| Page 49 of 69 | Information Technology Disaster Recovery Plan – Public Version | | August 31, 2012 |

**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.

Page 50 of 69 Information Technology Disaster Recovery Plan – Public Version August 31, 2012

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 |
|  |  |

Page 51 of 69 Information Technology Disaster Recovery Plan – Public Version August 31, 2012

DISASTER RECOVERY PLAN UPDATE LOG



|  |  |  |
| --- | --- | --- |
| **PAGE(S) & SECTIONS AFFECTED** | **DESCRIPTION OF CHANGE** | **DATE** |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

Page 52 of 69 Information Technology Disaster Recovery Plan – Public Version August 31, 2012

DISASTER RECOVERY PLAN DISTRIBUTION LIST



|  |  |
| --- | --- |
|  |  |
| **NAME** | **ENTIRE BOOK OR CHAPTERS** |
|  |  |
| Offsite Storage | Entire |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

Page 53 of 69 Information Technology Disaster Recovery Plan – Public Version August 31, 2012

**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.

Page 54 of 69 Information Technology Disaster Recovery Plan – Public Version August 31, 2012

DISASTER RECOVERY TRAINING LOG



|  |  |  |  |
| --- | --- | --- | --- |
|  | **NAME** | **SIGNATURE** | **DATE** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Page 55 of 69 Information Technology Disaster Recovery Plan – Public Version August 31, 2012

**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.

Page 56 of 69 Information Technology Disaster Recovery Plan – Public Version August 31, 2012

RECOVERY TEST HISTORY



|  |  |  |  |
| --- | --- | --- | --- |
| **DATE** | **TYPE** | **OBJECTIVE** | **RESULTS** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Page 57 of 69 Information Technology Disaster Recovery Plan – Public Version August 31, 2012

SAMPLE RECOVERY TEST PLAN



**TEST DATE \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_** **TEST # \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

TEST OBJECTIVES:

1. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
2. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
3. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

|  |  |  |
| --- | --- | --- |
|  |  |  |
| **TASK** | **TASK DESCRIPTION** | **COMPLETED** |
| **NUMBER** |  |  |
|  |  |  |
| 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 |  |
|  |  |  |
|  |  |  |
| Page 58 of 69 | Information Technology Disaster Recovery Plan – Public Version | August 31, 2012 |

|  |  |  |
| --- | --- | --- |
|  |  |  |
| **TASK** | **TASK DESCRIPTION** | **COMPLETED** |
| **NUMBER** |  |  |
|  |  |  |
| 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 |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

Page 59 of 69 Information Technology Disaster Recovery Plan – Public Version August 31, 2012

DISASTER RECOVERY PLAN TESTING FORMS



|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **TEST SCRIPT TEST DATE: \_** | | **\_/\_ \_/\_\_** | | **TEST # \_\_\_\_** | |
|  |  |  |  |  |  |
| **ESTIMATED** | **ACTUAL** |  | **FINISH** |  | **STEP DESCRIPTION** |
| **START** | **START** |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

Page 60 of 69 Information Technology Disaster Recovery Plan – Public Version August 31, 2012

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?

-------------------------------------------------------------------------------------------------------------------------

-------------------------------------------------------------------------------------------------------------------------

-------------------------------------------------------------------------------------------------------------------------

-------------------------------------------------------------------------------------------------------------------------

Page 61 of 69 Information Technology Disaster Recovery Plan – Public Version August 31, 2012

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?

-------------------------------------------------------------------------------------------------------------------------

-------------------------------------------------------------------------------------------------------------------------

-------------------------------------------------------------------------------------------------------------------------

-------------------------------------------------------------------------------------------------------------------------

Page 62 of 69 Information Technology Disaster Recovery Plan – Public Version August 31, 2012

**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**

Page 63 of 69 Information Technology Disaster Recovery Plan – Public Version August 31, 2012

**VENDOR LISTING**

****

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **COMPANY** | **CONTACT** | | **PHONE NUMBERS** | **EMAIL ADDRESS** | | **SUPPLY /** |
| **NAME** |  |  |  |  |  | **RESOURCE** |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |

**INFORMATION ON FILE**

Page 64 of 69 Information Technology Disaster Recovery Plan – Public Version August 31, 2012

**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.

1. 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: \_\_\_\_\_\_\_\_\_\_

1. 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
      1. Exterior
      2. Interior
   2. Computer Room
      1. Walls
      2. Ceiling
      3. Floor
   3. Environmental/Control
      1. Electrical
         1. UPS
         2. Transformers
         3. Emergency/Building
      2. HVAC
         1. Air Handling
         2. Air Conditioning
   4. Fire Suppression
   5. Data Center Contents
      1. Servers
      2. External Disk Drives
      3. Tape Backup
      4. Network Cabling
      5. Communications
      6. Workstations
      7. Other Equipment
      8. Tape Media

Page 65 of 69 Information Technology Disaster Recovery Plan – Public Version August 31, 2012

1. Spare Parts
2. 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: \_\_\_\_\_\_\_\_\_\_

1. 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: \_\_\_\_\_\_\_\_\_\_

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

Initials: \_\_\_\_\_\_\_\_\_\_ Date: \_\_\_\_\_\_\_\_\_\_ Time: \_\_\_\_\_\_\_\_\_\_

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

Initials: \_\_\_\_\_\_\_\_\_\_ Date: \_\_\_\_\_\_\_\_\_\_ Time: \_\_\_\_\_\_\_\_\_\_

1. Document findings from the survey and damage assessment. Initials: \_\_\_\_\_\_\_\_\_\_ Date: \_\_\_\_\_\_\_\_\_\_ Time: \_\_\_\_\_\_\_\_\_\_

Page 66 of 69 Information Technology Disaster Recovery Plan – Public Version August 31, 2012

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

Initials: \_\_\_\_\_\_\_\_\_\_ Date: \_\_\_\_\_\_\_\_\_\_ Time: \_\_\_\_\_\_\_\_\_\_

1. 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.**

Page 67 of 69 Information Technology Disaster Recovery Plan – Public Version August 31, 2012

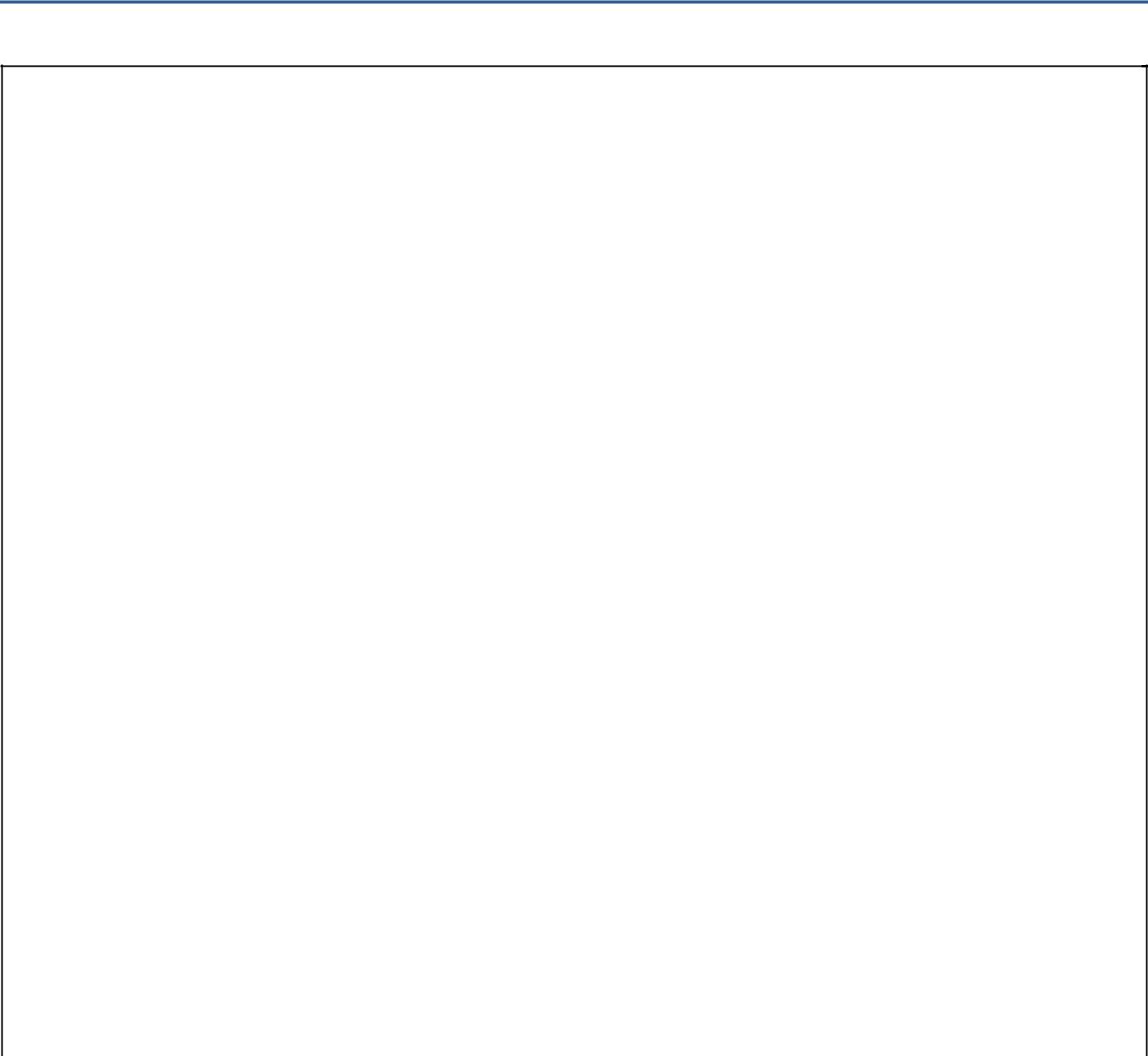
DAMAGE ASSESSMENT AND SALVAGE LOG



|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | **AREA OR** | **TYPE OF** | **COMMENTS** | **DAYS TO** | **INITIALS** |
|  | **EQUIPMENT** | **DAMAGE** |  | **REPAIR OR** |  |
|  | **ASSESSED** |  |  | **“SCRAP”** |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

Page 68 of 69 Information Technology Disaster Recovery Plan – Public Version August 31, 2012

**EMERGENCY TELEPHONE NUMBERS**

****

|  |  |
| --- | --- |
| **PERSON OR ORGANIZATION** | **TELEPHONE** |
|  |  |

TAMUCT Police Dept.

Facilities

Human Resources

Legal - TAMUS Office of General Counsel

Insurance

|  |  |
| --- | --- |
| FBI (San Antonio Division) |  |
|  |  |
| Killeen Fire Department |  |
|  |  |
| Killeen Police Department |  |
|  |  |
| Bell County Sheriff |  |
|  | **INFORMATION ON FILE** |
| 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 |  |

Page 69 of 69 Information Technology Disaster Recovery Plan – Public Version August 31, 2012