



**Volume 2 - APPENDIX 7
(UITS – BUSINESS SYSTEMS SUPPORT)
TO
ANNEX E (PLANNED RESPONSE ACTIVITIES-UA OPERATIONAL SUPPORT)**

OBJECTIVES

The primary objectives of the UITS Business Continuity and Disaster Recovery (BCDR) Plan are to make sufficient agreements about preparations, and to design and implement sufficient procedures for responding to a disaster of any size in the UITS area of responsibility.

The purpose of these procedures is to minimize the effect of a disaster upon the operations of the organization. The emphasis is on safeguarding the vital assets of the University and ensuring the continued availability of critical UITS services.

Other objectives of the plan are as follows:

- Risk reduction and prevention to help avert any interruption in computing system, application, network or voice systems and services.
- Reduce confusion during any chaotic period by having a clearly defined course of action that will reestablish services as soon as possible.
- Identify critical functions with consideration of priority scheduling.
- Identify alternate sites of operation that provide the same or compatible equipment. Conclude formal backup arrangements with such sites as identified. Specify steps necessary to relocate to the alternate site.
- Identify key personnel for each application, database or service so that they can be summoned without delay when needed.
- Identify users of UITS services to be notified of delays and to be involved in the recovery process. Establish the personnel responsible for all phases of Disaster Recovery.
- Provide sufficient documentation for use by the Disaster Management Team in its evaluation of the Disaster Recovery Plan.

PLAN ORGANIZATION

The content of the Information Technology and Telecommunications plan covers disaster procedures, responsibilities, identification of essential software applications and hardware, general procedures for potential interruptions, policies for reducing risk,

contingency planning parameters, disaster response, and testing & maintenance of the disaster recovery plan. The document is divided into component sections each of which describes its objective and relationship to the plan. The paragraphs which follow provide a brief description of a very comprehensive and detailed UITS Business Continuity and Disaster Recovery Plan.

CONTINGENCY PLANNING

This section describes the disaster recovery planning process by describing the planning strategies considered, defining responsibilities of the Disaster Coordinator, identifying a number of disaster recovery teams and describing disaster planning considerations.

DISASTER RECOVERY TEAMS

Included are each team's description, responsibilities and roles at the Disaster Management Team (DMT) level. The definition of the individual recovery teams, their assignment of members, responsibilities and tasks are described in Appendix A – Disaster Recovery Team Detail.

BUSINESS IMPACT ANALYSIS

This section includes a brief definition of the business impact analysis process, describes the importance of the BIA and summarizes the BIA process previously used here at the University of Arizona for critical computing and telecommunication systems.

ASSESSMENT OF RESOURCE REQUIREMENTS

This section addresses resource requirements through an evaluation of applications systems summaries, and the establishment of application priority by the applicable disaster team and users of UITS services. Resource requirements cover Risk Analysis, Application System Requirements, Minimum Recovery Requirements, Hardware, Communications, Software and Data Requirements.

RISK ANALYSIS

The risk analysis section describes the process of identifying and estimating expected losses as a consequence of undesired things happening to the resource requirements considered in the section “Assessment of Resource Requirements”.

RISK REDUCTION

Policies, procedures and considerations for reducing risk are covered. General topics include: protection of computer data, virus and network intrusion, physical security of the data center operation, access to computers and applications, and systems management.

DISASTER RECOVERY STRATEGIES

Detailed in this section is an analysis of alternatives that deal with service level agreements, vendor policies and agreements, and contingency site preparations including a discussion on hot-site and cold-site planning.

GENERAL DISASTER PROCEDURES

This section covers general procedures for potential interruptions of service due to: fires, electrical power outages, telecommunication infrastructure failures, flooding, hardware failures, software failures, application failures, cyber-terrorism and cyber-crime, and major disasters.

DISASTER RECOVERY PLAN ACTIVATION

This section details the recovery procedures that have been put into place to handle an emergency from initial response until a return to normal service.

REVIEW, MAINTENANCE & TESTING

In support of recommendations for a long-term planning strategy, a summary is presented in outline format for the project phases, objectives and implementation strategy decisions for follow-up consideration during the review process and testing phases.

DISASTER RECOVERY SOFTWARE

UITS uses a Business Continuity Software package called LDRPS that requires populating "Dictionaries" with all of the essential information needed to set a disaster recovery plan into action. The Dictionaries are divided into four groups: Responsibilities, People, Materials, and Miscellaneous. Using this software enhances our Disaster Recovery Plan by utilizing and keeping current the above-mentioned dictionaries, which allows for easy point and click operation and individual plan development.

STAFFING REQUIREMENTS

UITS has created a reporting structure for all critical areas. The Disaster Recovery Structure (see attached) identifies all of these areas within UITS and has assigned Team Coordinators and Team Leaders to each critical function within our computing environment. Depending on the severity of the situation each identified individual would be contacted and the proper staff would be assembled.

CRITICAL EQUIPMENT AND NECESSARY SUPPLIES

The Hardware inventory list is listed as "Appendix C: Hardware Inventory List" All vital equipment is listed in this appendix. LDRPS also has a supply dictionary which lists all

essential supplies that may be needed in any emergency. Additionally the Support Teams Coordinator, depending on the severity of the situation, has been tasked with providing human essential support such as food, water and other comfort accommodations.

Our alternate site has been set up to house critical servers in the event that we lose all or part of our main computing site. We also have negotiated and signed contractual agreements that obligate vendors to provide hardware that is the same, equal to, or better than that which is required in the event of a disaster. We provide these vendors with our inventory list, which defines all of UITS's hardware.

CRITICAL FUNCTIONS

UITs has identified those functions that are deemed critical to the ongoing operations of university functions. Listed below are Priority 1 and Priority 2 functions. Priority 1 identifies those functions that need to be restored as soon as possible and not to exceed 24 hours. Priority 2 identifies those functions that should be restored within 72 hours.

Priority 1

These priority 1 functions are required for health, safety and general voice and data communications activities for the campus.

- On campus network services.
- On campus voice communication.
- Off campus voice communication.
- Special circuits (911, Police Dispatch, etc.).
- Voicemail including information and broadcast mailboxes.
- UA web page (UAINFO).
- Email and Listserv systems.
- Network authentication service (NETID).

The voice and data networks are used for many infrastructure, facility and processing activities. While these systems are extremely critical the replication of them for redundancy and backup to achieve the desired recovery time is cost prohibitive. The \$25 million investment and years of implementation into the building, facilities, PBX system, inside and outside cable plant, and supporting infrastructure present a significant challenge to preparing a response and recovery plan for these items. Included in the UITS continuity and recovery plan is the recognition that attending to risk reduction and functional resiliency, dependence on business unit interim plans and emergency support units like FEMA, and identifying other solutions are critical to the plan.

Priority 2

These priority 2 functions are critical to the operation of university for business and academic activities.

- Personnel Services Operating System (PSOS).

- Financial Records System (FRS).
- Student Information System (SIS).
- Student and Advisor Link.
- Employee Link.
- Cosmos System.
- Student & Extended Visitor Information System (SEVIS).
- University Information System (UIS).
- Off campus Internet connectivity.
- High speed Internet connectivity (Internet 2).
- Dial up modems for external network connection.
- UITS Department file services (OSMO).
- Central IT printing capability.

Many of these functions have redundant services housed in our off-campus recovery facility. The most important of this list, FRS and SIS, require expensive mainframe hardware that is not duplicated at this time. UITS recovery plans include vendor contracts for this equipment delivery in the event of a significant loss to the UITS central site and our off-site recovery facility has been prepared for their installation. The time required to deliver, install and prepare an alternate system for FRS and SIS is about 30 days. Therefore the campus needs to prepare for a minimum of 30 days without these systems. Business and academic units should have manual procedures in place for dealing with the functions they require of these application systems.

TELEPHONE LISTS

We have created Employee Rosters for each department, these rosters have the employee name, and all telephone numbers by which to contact the individual. We maintain an Emergency Phone list which list all essential personnel, including all software and hardware vendors and their appropriate contacts, this list is distributed to Coordinators, Computer Operations, Alternate Site, and several key personnel.

Included in this document are the Disaster Recovery management team and their respective contact information.

UITS PLAN APPENDIXES (Attachments Omitted for Security Reasons)

Appendix A - Disaster Recovery Team Detail

Detailed disaster recovery plans for each team is included in this appendix. Included in each team's description are (1) Team Coordinator/Leader, (2) Definition of Team, (3) Roles Required, (4) Assignment of Members, (5) Responsibilities, (6) Task Assignments, (7) Alternate Assignments, (8) Key Management Liaisons and (9) Pre-Planning Required.

Appendix B - Emergency Phone List

This is the emergency phone list maintained by the Computer Recovery Coordinator Team. It contains numbers for UITS software support, vendor

software support, vendor hardware, accounting, physical resources, peripheral hardware, remote computing sites, and personnel.

Appendix B1 – Emergency Forms

This appendix contains forms needed to make the proper assessment of situations which may need further clarification or information.

Appendix C - Hardware Inventory

This is the computer hardware inventory for UITS. This list is provided to appropriate vendors on the contracted scheduled basis.

Appendix C-1 Hardware Inventory – Backup Systems Located at the Disaster Recovery Site

This is a list of backup servers and workstations located at the Disaster Recovery Site.

Appendix D - Software Inventory

This appendix contains a list of all systems software products installed on UITS systems. The list includes operating system, administrative application software, utilities, database management, and third party software products.

Appendix E – Business Impact Analysis Checklist

In conducting the administrative and academic risk analysis described in the section “Assessment of Resource Requirements” each team has available to them the checklist which are reproduced in this appendix.

Appendix F – Campus-wide Protection & Recovery (CPR)

A campus-wide team was assembled to provide an assessment of potential risks and resource requirements by application. This team produced a Business Impact Analysis (BIA) that describes financial and processing implications that would be a result of system outages. These implications are used by the Computer Recovery Coordinator Team to identify priority recovery and processing needs if a disaster event should occur.

Appendix G - Data Access & Ownership Policy

The Policy that is reproduced in this Appendix establishes responsibilities associated with the granting of access to University administrative data and the use thereof.

Appendix H - Backup Schedule and Facilities

Current backup schedule and locations are contained in this document.

Appendix I - UITS Organization Chart and Recovery Team Structure

The UITS Organization Chart and this plan Recovery Team Structure diagrams are provided in this appendix.

Appendix J - Disaster Plan Distribution List

The list of Disaster Recovery Plan recipients is contained in this Appendix.

Appendix K – Application Summaries

Application summaries for each system in the disaster recovery process are contained in this appendix.

Appendix M - Vendor Agreements

This document contains vendor contract and agreement information. The actual contract and agreements are located in the Disaster Management Office vital records book.

Appendix O - Building Monitor List

The building monitor list contains the contact names and numbers for each building on campus as maintained by Facilities Management.

Appendix P - Power Grid Information

Diagrams depict the power substations and their connected buildings. UAWEST Substation identifies the two feeders that provide primary and secondary power support to the Computer Center Buildings 73 and 73A.

Appendix R – Policies

This is a collection of policies that are used for development, reference and execution of this disaster recovery plan.

Appendix R-1- Individual Assistance

This is the list of Individual Assistance Programs Available from FEMA.

Appendix R-2 Emergency P.O. and PCARD Policy

The policy for using the Emergency P.O. numbers and for Catering services using a PCARD.

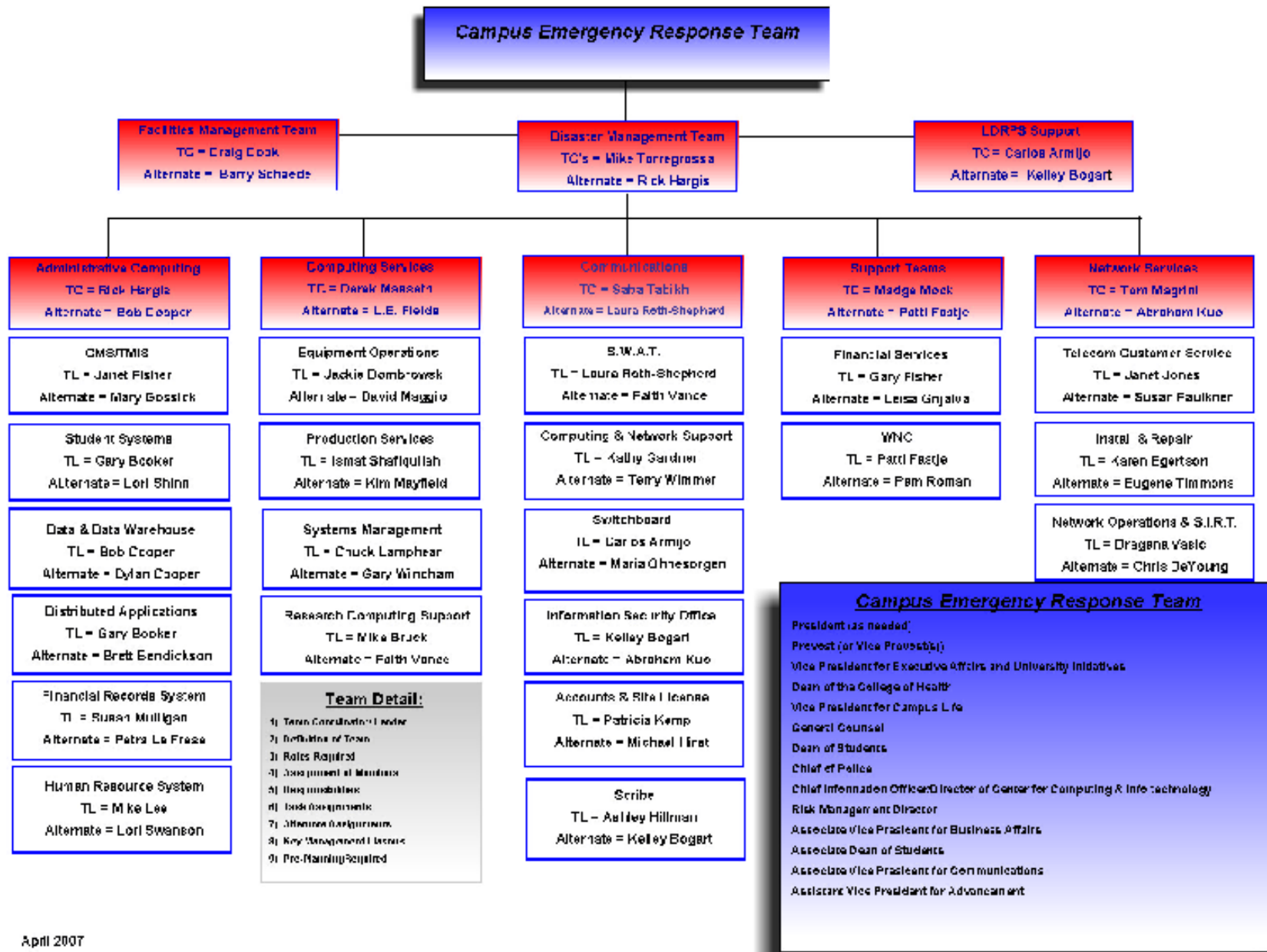
Appendix U – Campus Emergency Response Plan

Initiative on Preparedness and Emergency Response for the University of Arizona. Refer to Appendix 7 to Annex E for UITS's Business Systems Support section.

Appendix X - Glossary of Terminology

The glossary of terms provides some basic information to insure a common understanding of Disaster Recovery concepts and definitions.

CCIT Recovery Team Structure Diagram



Information in this document is **confidential and for internal use only**.
Do not release any information from this document without specific authorization from
the Information Security Office.