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, and 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 plans.

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 - Functions that need to be restored ASAP not to exceed 24 hours**

Required for health, safety and general voice and data communications activities for the campus

<table>
<thead>
<tr>
<th><strong>• On campus network services</strong></th>
<th><strong>• Removed for Security</strong></th>
<th>*<em>• <em>UA web page (UAINFO)</em></em></th>
</tr>
</thead>
<tbody>
<tr>
<td>*<em>• <em>on campus voice communication</em></em></td>
<td>*<em>• <em>Voicemail including information and broadcast mailboxes</em></em></td>
<td><strong>• Email and Listserv systems</strong></td>
</tr>
<tr>
<td><strong>• Off campus voice communication</strong></td>
<td></td>
<td>*<em>• <em>Network authentication service (NETID &amp; CatNet)</em></em></td>
</tr>
</tbody>
</table>

**PRIORITY 2 - Functions that should be restored within 72 hours**

Critical to the operation of the university for business and academic activities.

<table>
<thead>
<tr>
<th><strong>UAccess</strong></th>
<th><strong>• Financial Records System (FRS)</strong></th>
<th><strong>• Off campus Internet connectivity</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>• Employee</strong></td>
<td><strong>• D2L</strong></td>
<td><strong>• High speed Internet connectivity (Internet 2)</strong></td>
</tr>
<tr>
<td><strong>• Student</strong></td>
<td><strong>• Enterprise Directory Services (EDS)</strong></td>
<td><strong>• UITS Department file service (OSMO)</strong></td>
</tr>
<tr>
<td></td>
<td><strong>• Matrix, including SEVIS</strong></td>
<td><strong>• Central IT printing capability</strong></td>
</tr>
</tbody>
</table>

The voice and data networks are used for many infrastructure, facility and processing activities.

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.

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**

Telephone lists have been created employee rosters for each department, these rosters contain:

<table>
<thead>
<tr>
<th>Employee</th>
<th>Essential Personnel</th>
<th>Disaster Recovery Team</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Name</td>
<td>• Software vendors and contact information</td>
<td></td>
</tr>
<tr>
<td>• Telephone numbers</td>
<td>• Distributed to Coordinators, Computer Ops, Alternate sites &amp; key personnel</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Names</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Phone Numbers</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Other key contact information</td>
<td></td>
</tr>
</tbody>
</table>

**UITS maintains three (3) plans for disaster and emergency situations**

<table>
<thead>
<tr>
<th>1. Disaster Recovery Plan</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Removed for Security Reasons</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>2. System Recovery Plan</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Removed for Security Reasons</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>3. UA LDRPS Documents</th>
<th></th>
</tr>
</thead>
</table>

For security purposes these sections have been omitted from this document.
INFORMATION WAREHOUSE

The Information Warehouse provides a backup data system in the event a disaster renders UA primary data systems as inoperable or destroyed.

SYSTEM COMPONENTS AND OPERATIONAL CONCEPT

The Information Warehouse Office (IWO) maintains hot off-site cloned servers. The IIW web server and both the IWO and UIS data warehouse clusters are backed up (Removed for Security). Should something happen to any of the main servers (Removed for Security) in the UITS equipment room, users would be redirected to the other site by changing the address reference for the affected site(s) to point to the alternative site(s). This would be done on the UITS domain name servers. At most, one day of work would be lost by such an accident and any files that existed, such as a new census file, would still be available from the source for that file during that day. Such source files could be retrieved and loaded on the alternate server.

BACKUP SYSTEMS/OPERATION

IWO data warehouse machines are backed up (removed for security reasons). In addition, some backup tapes are kept for a longer period to permit restoration of older data if need be; it is unlikely that this would apply to census files since they are used and backed up so regularly.

The result is that IWO has (removed for security reasons). The physical servers (removed for security reasons.) Tapes are rotated off the site on a regular basis and are systematically retained for varying lengths of time based on the risks involved. (See UITS Disaster Recovery Plan for recovery plans and facilities for the alternative location – Removed for security reasons.)