Guidelines for Generating a Disaster Recovery Plan

University of Arizona
NetManagers/NetVision Disaster Recovery sub-committee 2002
Guidelines for Generating a Disaster Recovery Plan

Table of Contents

1. INTRODUCTION ......................................................................................................................1
   1.1. Background ..................................................................................................................... 1

2. SCOPE ....................................................................................................................................... 1
   2.1. Purpose ........................................................................................................................ 1
   2.2. Objectives .................................................................................................................... 1
   2.3. Assumptions .................................................................................................................. 2
   2.4. Plans and Goals ............................................................................................................ 2

3. DISASTER RECOVERY POLICY .................................................................................. 3
   3.1. Policy Statement ............................................................................................................... 3
       3.1.1. Purpose .................................................................................................................. 3

4. CONTINGENCY PLANNING ........................................................................................... 3
   4.1. Disaster Planning Strategy and Process ........................................................................... 3
       4.1.1. Initial Short-term, High-impact Strategy ................................................................. 3
       4.1.2. Long-term, Extended Strategy ............................................................................... 4
   4.2. Planning Considerations ................................................................................................ 5
       4.2.1. Types of disaster to consider ................................................................................. 5
       4.2.2. Most Probable Disaster Occurrences .................................................................. 5

5. DISASTER RECOVERY TEAMS .................................................................................. 5
   5.1. Recovery Team Plans ....................................................................................................... 5
   5.2. Disaster Management Team .......................................................................................... 6
   5.3. University Crisis Management Team ............................................................................. 6
   5.4. Executive Director ......................................................................................................... 6
   5.5. Facilities Management .................................................................................................. 6
   5.6. Communications ........................................................................................................... 7
   5.7. Support Teams ................................................................................................................ 8
       5.7.1. Administrative/Business Function Support ............................................................ 8
       5.7.2. User Support ........................................................................................................... 8
       5.7.3. Other potential teams may include: ........................................................................ 9
   5.8. Team Detail Description ................................................................................................10
       5.8.1. Team Coordinator/Leader ...................................................................................... 10
       5.8.2. Definition of Team ................................................................................................ 10
       5.8.3. Roles Required ....................................................................................................... 10
       5.8.4. Assignment of Members (Team Members) ............................................................ 10
       5.8.5. Responsibilities ...................................................................................................... 10
       5.8.6. Task Assignment .................................................................................................. 11
Appendix C
Page (2)

5.8.7. Alternate Assignments ................................................................. 11
5.9. Disaster Recovery Coordinator ....................................................... 11

6. OPERATIONS IMPACT ANALYSIS ..................................................... 12
6.1. What is an Operations Impact Analysis (OIA)? ............................ 12
6.2. The Importance of an OIA ............................................................. 12

7. ASSESSMENT OF RESOURCE REQUIREMENTS ................................. 12
7.1. Audit Control Requirements ........................................................ 12
  7.1.1. Data Requirements ................................................................ 13
7.2. Software Requirements ............................................................... 13
7.3. Hardware Requirements ............................................................... 13

8. RISK ANALYSIS ............................................................................... 14
8.1. Overview ...................................................................................... 14
8.2. Environmental Risk Identification ................................................ 14
  8.2.1. Departmental organization risks checklist ............................. 14
8.3. Physical Site Risk Identification ................................................... 14

9. RISK REDUCTION ............................................................................. 15
9.1. Computer Data Protection ............................................................ 15
9.2. Cyber-Terrorism and Cyber-Crime Protection ............................... 15
9.3. Physical Security .......................................................................... 15
  9.3.1. Building, Computer and Switch Room Access ...................... 15
  9.3.2. Fire Risk .............................................................................. 15
  9.3.3. Water Damage Risk ............................................................... 16
  9.3.4. Lightning Damage Risk .......................................................... 16
  9.3.5. Risk of Sabotage .................................................................. 16
  9.3.6. Power Failure ........................................................................ 17
  9.3.7. Air Conditioning Failure ......................................................... 17
  9.3.8. Particulates Contamination ...................................................... 17
  9.3.9. Floor/Roof/Wall Collapse ...................................................... 18
  9.3.10. Major Equipment Failure ...................................................... 18
9.4. Access to Computing Systems ...................................................... 18
  9.4.1. Data Access and Ownership Policy ........................................ 18
  9.4.2. System Administration .......................................................... 18
9.5. Computer Operations ................................................................. 19
9.6. Insurance .................................................................................... 19
9.7. Backup Procedures and Schedule ............................................... 19
  9.7.1. Equipment Operations Backup Procedures ........................... 19
  9.7.2. Storage Procedures ............................................................... 19

10. DISASTER RECOVERY STRATEGIES ............................................. 20
10.1. Strategy Development ............................................................... 20
10.2. User Service Level Requirements .............................................. 20
10.3. Service Level Alternatives ......................................................... 20
  10.3.1. Service Degradation Strategies .......................................... 20
11. GENERAL DISASTER PROCEDURES ......................................................... 20

11.1. Emergency Calls .................................................................................. 21
11.2. Fires ...................................................................................................... 21
   11.2.1. Prevention ...................................................................................... 21
   11.2.2. Detection ...................................................................................... 21
   11.2.3. Fire Extinguisher locations ............................................................. 22
   11.2.4. Policy for Appropriate Action if a Fire or Alarm Occurs ................. 22
   11.2.5. Additional Building Evacuation Issues ............................................ 23
   11.2.6. Goals ........................................................................................... 23
11.3. Fire Extinguisher Procedures ................................................................. 23
11.4. Building Monitors ................................................................................ 24
11.5. Electrical Power Outages ...................................................................... 24
11.6. Flooding ................................................................................................ 24
   11.6.1. Prevention ...................................................................................... 24
   11.6.2. Detection ...................................................................................... 25
   11.6.3. Evacuation ..................................................................................... 25
11.7. Flooding Procedures ............................................................................. 25
   11.7.1. Goals ........................................................................................... 25
11.8. Hardware Failures ................................................................................ 26
   11.8.1. Hardware Inventory ....................................................................... 26
11.9. Systems Software Failures .................................................................... 26
11.10. Custom or third-party Application Failures ......................................... 26
11.11. Cyber-Terrorism and Cyber-Crime ...................................................... 26
11.12. Major Disasters .................................................................................. 26

12. DISASTER RECOVERY PLAN ACTIVATION ........................................ 26

12.1. Initial Response .................................................................................. 26
   12.1.1. Emergency Response Procedures ................................................ 26
   12.1.2. Disaster Management Team Notification ........................................ 27
   12.1.3. Initial Disaster Management Procedures ....................................... 27
   12.1.4. Activation of an Emergency Control Center .................................... 28
   12.1.5. Notification of Necessary Disaster Teams ...................................... 28
   12.1.6. Disaster Management Team Coordination ...................................... 29
   12.1.7. Preparation for use of Contingency Site(s) ....................................... 29
   12.1.8. Contingency Operations Procedures ............................................ 29
12.2. Initial Recovery at a Contingency Site ................................................ 30
   12.2.1. Initial Procedures at Contingency Site ............................................ 30
   12.2.2. Offsite Storage and Pickup of Backup Materials ................................ 30
12.3. Full Operation at a Contingency Site .................................................... 30
   12.3.1. Establishing Contingency Site Operations ...................................... 30
   12.3.2. Recovery of Lost Data .................................................................... 31
   12.3.3. Coordination with Application Users .............................................. 31
   12.3.4. Specific Application Procedures .................................................... 32
12.4. Restoring Original Operations ............................................................. 32
   12.4.1. Hardware Replacement ................................................................. 32
   12.4.2. Return to Normal Operations ........................................................ 32

13. MAINTENANCE & TESTING OF THE DISASTER PLAN .................... 32
13.1. Review & Maintenance of the Plan ................................................................. 33
13.2. Testing the Disaster Recovery Plan ............................................................. 34

14. DISASTER TEAM TEMPLATE ............................................................................. 1
   14.1. Team Coordinator/Leader ........................................................................... 1
   14.2. Definition of Team ..................................................................................... 1
   14.3. Roles Required ........................................................................................... 1
   14.4. Team Members ......................................................................................... 1
   14.5. Responsibilities ......................................................................................... 1
   14.6. Task Assignments ...................................................................................... 1

15. INFORMATION TECHNOLOGY CRISIS MANAGEMENT TEAM .......... 1

16. CONTACT LIST/PHONE NUMBERS ................................................................. 1
   16.1. CENTER FOR COMPUTING AND INFORMATION TECHNOLOGY .......... 1
       16.1.1. Units .................................................................................................. 1
       16.1.2. Important Phone Numbers ................................................................. 2
1. Introduction

1.1. Background

The Disaster Recovery Plan is a guiding document containing the necessary instruction, guidelines, organization, responsibilities and information required for a department to be prepared for an emergency that would affect computer and network services.

The content of the document 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.

2. Scope

2.1. Purpose

The purpose of the Disaster Recovery Plan is to provide guidelines and procedures for an orderly and timely recovery from an interruption of data processing and/or network services.

Procedures to recover from a disaster are predicated on the most serious occurrence possible.

2.2. Objectives

The primary objectives of the Disaster Recovery Plan are to make sufficient agreed-upon preparations, and to design and implement a sufficient set of agreed-upon procedures for responding to a disaster of any size in the departmental area of responsibility.

The purpose of these procedures is to minimize the effect of a disaster upon the operations of the department. The emphasis is on safeguarding the vital assets of the University/College/Department and ensuring the continued availability of critical IT services.

Other objectives of the plan are as follows:

- Risk reduction and prevention to help avert any interruption in computing system, application, network 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 departmental services to be notified of delays and to be involved in the recovery process. Establish the personnel responsible for all phases of Disaster Recovery

2.3. Assumptions

In any recovery plan there will be a wide array of disaster possibilities and recovery procedures to consider. To cut the problem down to size, therefore, preliminary assumptions are developed as guidelines. For the recovery effort to be successful, all involved personnel are required to assure that these assumptions are current and correct.

The Disaster Recovery Plan is based on the following assumptions:

• Managers will keep all personnel affected by this plan aware of its current procedures and practices

• All personnel affected by this plan are responsible for understanding their role under a disaster situation

• This plan will be continually maintained.

• The recovery process documented in the plan should be tested annually

• All personnel must react quickly and effectively during the recovery process

• Disaster Recovery can only be successful if there is an initial backup of static components including the system software, proprietary packages, programs, and data, and a routine backup, at least daily, of all changes and modification of these electronic components, and there is a regular testing of hardware and communications backup facilities

2.4. Plans and Goals

The following organizational goals can be pursued.

• Assignment of Internal Staff for Planning and Training

• Obtaining the Interest and support of all Administrators

• Getting Cooperation from the User Departments

• Involving all Related Departments both internal and external

• Setting Priorities for the Planning Effort

• Reviewing the Plan during Its Development
• Considering the Use of Consulting Support
• Ensuring Continuing Commitment once the Plan is in Place
• Periodic Testing of the Plan
• Integration of the Plan in the Normal Business Process.

3. Disaster Recovery Policy

3.1. Policy Statement

All departments and/or divisions should develop, exercise and maintain recovery plans for the business functions and processing operations as necessary for the protection of University/Department information and business activities. Plans should address the full range of resources including data processing, data communications links, personal computers, workspace, and documents. The recovery plans must adhere to the standards established for electronic information processing, and the procedures established by the Disaster Management Team.

University and Department policies and procedure regarding human resources, public relations, customer relations, health and safety, vendor relations, information security and individual privacy must be followed during the development of the recovery plan and any activity associated with the recovery plan execution.

3.1.1. Purpose

• This Disaster Recovery Policy is based on the realization that the department is critically dependent on its computer systems, and network services, and the understanding that disaster planning is necessary because of the storage of large quantities of information within a system, and the electronic processes that are the basis for business activities.
• The formalization of a Disaster Recovery Plan will provide the foundation upon which the necessary procedures for protection of University information assets and the continued operation of critical University applications will be developed.

4. Contingency Planning

4.1. Disaster Planning Strategy and Process

4.1.1. Initial Short-term, High-impact Strategy

• Create a policy statement covering disaster recovery planning
• Obtain copies of all existing policies and procedures governing emergency response from the University Department of Risk Management
• Compile an emergency telephone or contact list consisting of Departmental personnel, CCIT personnel, user personnel, vendors, and emergency services (Appendix C...contact list)
• Assemble all readily available operations and systems documentation
• Create lists of all operating systems software by hardware configuration (Appendix D. DPI)
• Obtain a copy of all Emergency Procedures documentation
• Verify that all systems are backed up as required and stored in a secure site
• Determine the minimum hardware configuration on which mandatory components of application systems can run and arrange for tests
• Create a priority ordered list by application operating system segmented by major organizational function
• Consult with senior management in the financial, student, administrative, and operational areas to get their opinions as to the mandatory and necessary applications in an agreed order of priority

4.1.2. Long-term, Extended Strategy

The Long-term Strategy differs from the short-term by emphasizing greater and continued participation by the department's administrative officers and users of departmental services.

The long-term strategy is directed towards creating a full, effective, disaster recovery capability by:

• Assigning a full-time person or persons to maintain and oversee the plan
• Assigning task groups that report regularly to the Disaster Management Team on developing areas of the plan
• Obtaining budget funding necessary for continued maintenance of the plan
• Involving all organizational groups, such as Security, Risk Management, Facilities, and Procurement and Contracting
• Developing a full disaster recovery capability covering all areas IT use
• Having regular training of all staff in the plan actions and requirements
• Testing the plan realistically and regularly, and report on the results of the testing including recommendations

•
4.2. Planning Considerations

4.2.1. Types of disaster to consider

- Natural disasters: Floods, Storms, Fires, Earthquakes, Lightning, Loss of a Disk Drive or Computer System, etc.
- Man-made disasters: Fire, Transportation Accidents, Chemical Accidents, Sabotage or Willful Destruction, Bomb Threats, Burst Pipes, Electrical Outage, Loss of Environmental Controls, etc.
- Political disasters: Riots, Public Demonstrations, Civil Disturbances, etc.
- Electronic Warfare: Hackers, Cyber terrorism, Computer Viruses, Intrusion Detection, Denial of Service, etc.

The types of disasters that should be considered depend on the team’s area of responsibility and operating parameters and may be specific to a particular application. Some disasters, such as major building fires, would probably affect all teams and must be planned for accordingly.

The most likely threats to occur should receive the most attention. These more common disasters may be localized in the computer, communications, or data input areas.

4.2.2. Most Probable Disaster Occurrences

Come to agreement on the most probable disaster occurrences in their area of responsibility. When several different types of disaster probabilities are noted, the possible occurrences should be grouped.

5. Disaster Recovery Teams

5.1. Recovery Team Plans

Separate Coordination teams responsible for all activities within your department that will manage the recovery process. This breakout of teams enables the activation of any or all of your department’s personnel and/or plans so that the recovery process can scale appropriately based on the requirement. The team leader from each of these coordination teams will be a member of the Disaster Management Team which provides overarching responsibility and direction for plan development, plan maintenance and plan execution.

Each coordination team should be further divided into appropriate sub groups as necessary to develop and manage specific requirements.

The disaster teams identified in this section are loosely coupled to the organizational structure of your department. To assist in the implementation of the Disaster Recovery Plan, the following teams should be established.
5.2. Disaster Management Team

The Disaster Management team is comprised of coordination teams, the Executive Director/Dean/Department Head of your department and a Disaster Recovery Coordinator. An overview of team roles and the responsibilities of each team leader or coordinator are described in this section. The Executive Director/Dean/Department Head for your department, University Information Security Officer and Disaster Recovery Coordinator role are described in this section.

5.3. University Crisis Management Team

The University recognizes that it is impossible to anticipate every possible major emergency or disaster situation that may be encountered and equally impossible to prepare detailed plans for incidents where the extent and nature of the event or condition is not known beforehand. For this reason oversight of any emergency response operation is required to provide appropriate coordination, communication, decision-making and appropriate recovery of an emergency. The University has established this team of individuals to provide this oversight and to advise the President with respect to actions that should be undertaken to deal with an emergency. The department can utilize this team as necessary and as described within this plan.

5.4. Executive Director

The Executive Director/Dean/Department Head for your department participates with the Disaster Management Team to provide guidance, counseling and communication. This person or designee also has the responsibility to provide the communication and coordination link to the University Crisis Management Team. This position also serves as the focal point for ensuring that information security and privacy concerns and issues within this plan are consistent with university, state and federal obligations, policy and procedures.

5.5. Facilities Management

The Facilities Management team will provide the overall coordination of facility issues for all phases of this plan including prevention, response, recovery and resumption. The Disaster Management Team will help establish the tasks assignment and priorities as dictated by the events and requirements at the time of developing team plans and during the recovery phases.

Responsibilities of the Facilities Management Team Leader include providing the coordination and oversight for these activities:

- The evaluation and recommendation of all building and space management issues including any prevention or initial response analysis that may be required
- The design, coordination and implementation of temporary and replacement facilities
- Ordering, coordinating the installation and maintaining facility and environmental requirements including but not limited to:
- Power and emergency systems
- Air handlers
- Chillers and any required water systems
- Raised computer flooring
- Ground grids
- Fire detection, prevention and suppression systems and equipment
- Generators and Uninterruptible Power Systems (UPS)
- Conduit and cabling systems as required

- Identifying, calculating, and balancing all load requirements for electrical, air-conditioning and other environmental requirements
- Monitoring and measuring hardware requirements and resource consumption
- Assisting with the installation of network, computing equipment and support apparatus
- Establishing, posting, communicating, training and maintaining all emergency procedures

5.6. Communications

This Communications group will help facilitate communication, relationships, groups, events and programs in the support of all phases of this plan including prevention, response, recovery and resumption. This support service differs from the Support Teams plans by having responsibility for developing specific announcements and providing the necessary communications to assist staff regarding current events to help them with their recovery efforts. The team also serves as a contact point for providing computing topics to community print and broadcast media, and as a resource for computing-related information to the community.

The Disaster Management Team will help establish the tasks assignment and priorities as dictated by the events and requirements at the time of developing team plans and during the recovery phases. Responsibilities of the Communications Team Leader include providing the coordination and oversight for these activities:

- Developing the official announcements that will be made to internal staff, campus and the private sector regarding information technology issues such as new services, service problems, status report, and other alerts and notifications
- Providing the leadership and coordination for public relations for the University's campus-wide IT efforts as needed during the various phases of this plan
- Determining and providing the necessary outreach activities that may include interacting with, colleges and departments, facilitating vendor contacts and visits, and participating in campus news related sessions
• Providing oversight of the creation and distribution for printed, electronic, and web based publications and announcements, such as newsletters, user guides, brochures, notices, pamphlets, and directories. The publications are designed and produced to deliver both general and specific computing information to all segments of the campus community as may be required by this plan.

5.7. Support Teams

5.7.1. Administrative/Business Function Support
This team will provide the overall coordination for business, financial and any requested project planning needs for all phases of this plan including prevention, response, recovery and resumption.

The Disaster Management Team will help establish the tasks assignment and priorities as dictated by the events and requirements at the time of developing team plans and during the recovery phases. Responsibilities of the Support Team Coordinator include providing the coordination and oversight for these activities:

• Providing financial services, budgets, accounting support, and any business planning needed by your department administrators and managers to enable them to execute their prevention and recovery plans
• Assisting with procurement activities including contract development and coordination
• Establishing, acquiring and maintaining any inventory of supplies, components or other requirements as defined in the individual team plans
• Providing planning and coordination of your department’s information technology projects as required or requested by any team plans or recovery processes and assist with coordination efforts across groups in your department.
• Providing and coordinating the human support items such as food, water and housing that may be required during a recovery process
• Serves as the key administrative liaison as requested by the Executive Director to the Provost office and other administrative and organizational contacts.

5.7.2. User Support
This User Support group assists departmental students, faculty, and staff who use technology to achieve instructional, research, and administrative goals during all phases of this plan including prevention, response, recovery and resumption.

The Disaster Management Team will help establish the tasks assignment and priorities as dictated by the events and requirements at the time of developing team plans and during the recovery phases. Responsibilities of the User Support Coordinator include providing the coordination and oversight for these activities:
- Enabling access to a wide range of technologies and technology experts all dedicated to continuing the teaching / learning experience including institutional initiatives and department-based programs

- Providing Research, Academic, and Administrative Computing support to include:
  - Establishing and implementing the requirements for redundant and recovery systems for systems defined as critical resources
  - Coordination of departmental requirements and issues, priority setting of recovery processes and interpretation of those requirements to collaborative team plans
  - Database administration, application and operating system security and backup for research and instructional systems
  - Providing technical assistance to other teams as may be required to support their prevention plans or recovery efforts
  - Assisting University departments in the application and interconnectivity of desktop computing resources, LANs, client/server tools and workgroup solutions as needed for all phases of this plan

5.7.3. Other potential teams may include:

- Business recover team
- Departmental recovery team
- Computer recovery team
- Damage assessment team
- Security team
- Logistics support team
- Computer backup team
- Off-site storage team
- Software team
- Applications team
- Computer restoration team
- Human relations team
- Marketing/customer relation team
5.8. Team Detail Description

5.8.1. Team Coordinator/Leader

The Team Coordinator/Leader is the individual with primary responsibility for identifying, protecting, and planning, the recovery of all university assets within their area of influence. This Coordinator/Leader will also provide the routine maintenance of their plan and the leadership during the recovery process.

5.8.2. Definition of Team

The definition of each team will describe the area of concern, intended direction and specific assignment for the team.

5.8.3. Roles Required

Each recovery plan will require specific types of people to handle functional and task oriented items. This item will describe those roles.

5.8.4. Assignment of Members (Team Members)

The Team Coordinator/Leader will assign individuals to the roles required to clarify responsibilities and expectation. This pre-assignment will help expedite the recovery process. The list of team members provides a successional list of personnel who can direct the functions of that team in the event the team leader is unavailable. The team members are the personnel that will become the PRIMARY team. They will be the personnel that carry out the activities of that team.

5.8.5. Responsibilities

These are high-level duties that must be initiated as part of program development and implementation. These responsibilities must also be completed in order for the project to move forward, and sustained in order for the organization to maintain a viable continuity capability.

These responsibilities usually consist of job title (not the name of the responsible person) followed by numbered and/or bulleted statements that describe the associated responsibilities.

Business Continuity responsibilities include but are not limited to:

- Departmental Plan Development
- Plan Development Support
- Plan Administration
- Distribution and Maintenance
5.8.6. Task Assignment

This reflects the definitions of tasks or actions that are to be completed by a team and assigned to a team member.

5.8.7. Alternate Assignments

Once leadership and team members have been established, personnel in lowering succession (alternates) on that list, become team members. Each required role will have an alternate identified that can carry out that function. The alternate team members are backup to the PRIMARY team. These members will be activated to supplement missing team members or when a particular disaster requires larger teams or input of a specialized nature.

5.9. Disaster Recovery Coordinator

Overall coordination of Disaster Recovery planning, implementation, and maintenance is the responsibility of the Disaster Recovery Coordinator.

Responsibilities of the Disaster Recovery Coordinator include:

- Directs the planning, development, and maintenance of the Department disaster recovery plan
- Follows up on the pre-planning preparations required to implement the disaster recovery plan
- Chairs the planning meetings, and assures that each Team Leader accomplishes the agreed pre-planning tasks
- Reviews the disaster recovery planning status, requirements, and relationships with other interested groups
- Inspects all physical installations and personnel arrangements related to the disaster plan, and discusses the plans and their implications with the responsible affected managers
- Maintains the plan on an ongoing basis, keeping the documentation updated and, particularly, to correct names, addresses, and telephone numbers of those with responsibility in the event of a disaster
- Assembles information on the Department disaster recovery, and keeps files on vendors and equipment related to the activities
- Works closely with Internal Audit and Risk Management to test security measures and disaster recovery activities, and reports on the results to management
- Investigates other network security and recovery problems that cross departmental lines
- Checks periodically with outside groups such as vendors, to reaffirm disaster aid arrangements
• Checks on whether schedules for testing sections of the plan have been developed and are being followed
• Confirms the recovery procedures with each participant, and modify as necessary
• Assembles and distributes literature on security and disaster recovery, and attends occasional meetings on the subject to keep abreast of the latest advances and concepts

6. Operations Impact Analysis

6.1. What is an Operations Impact Analysis (OIA)?

It identifies the financial, operational and service impacts that may result from a disruption in daily business or organization’s operations. Disruptions can be short term (power outages or information systems problems) or long term (fires or natural disasters). In all disruptions, there is one common element – business operations have stopped.

6.2. The Importance of an OIA

In order to prepare for and be able to respond promptly to disruptions, an operations impact analysis needs to be conducted first. An operations impact analysis is important because it drives the priorities, strategies, and solutions for managing continuity and recovery. Planning decisions must be weighed against projected needs and costs, so the decisions that are made satisfy the recovery time objectives and are cost effective.

Without the knowledge that an OIA provides, preparing an effective and comprehensive business continuity plan is difficult, if not impossible.

7. Assessment of Resource Requirements

7.1. Audit Control Requirements

It is recognized that audit control requirements of critical applications at the time of a disaster are more complex and may be more difficult to handle than the basic backup and recovery of the system. It should be mandated that all run controls and audit controls that can possibly be handled remain in use during a disaster recovery period and if it is necessary to exclude them that it be done so with expressed permission of the user department.

The following application control objectives should be considered, as they would apply during a disaster event.
• Accurate Data

Accurate data implies the need for correction of inaccuracies associated with data preparation, conversion to machine-readable format, processing by the computer, or in the
output preparation and delivery processes. It also implies the retention of data control capabilities during a disaster.

- **Complete Data**

Completeness of processed data requires that data is not lost during preparation, in transit to the computer, during processing, between interrelated computer systems, and/or in transit to user of that data. It also implies the retention of the audit trail of the data through the disaster recovery operations.

- **Timely Data**

The timely processing of data ensures that management has the necessary information to take action in time to avoid avoidable losses. The discussions on priority should determine the recovery actions required to maintain the necessary timeliness.

- **Authorized Data**

Controls should ensure that any unauthorized data is detected prior to and during processing. This can be sensitive during a disaster recovery.

- **Processed according to GAAP**

Financial data should be processed in accordance with Generally Accepted Accounting Procedures. Controls should assure these procedures are followed even though a disaster has occurred.

### 7.1.1. Data Requirements

- What happens if some of the source data is lost?
- What happens if an incident disrupts a computer in the middle of processing?
- What types of backup files must be routinely created?
- How many generations of backup files are needed to be sure there is rapid, accurate recovery?
- How much information should be put in geographically remote vital records storage facilities?

### 7.2. Software Requirements

Identify systems software needs (see DPI).

### 7.3. Hardware Requirements

Identify systems hardware needs (see DPI).
8. Risk Analysis

8.1. Overview
Risks are always present in a computerized environment and are generated by a variety of threats. Some of these threats are physical, such as, fire or water damage. Other threats are people oriented, such as errors, omissions, acts of violence, fraud, etc. These risks cannot be eliminated, but security measures have been put into place to reduce the probability of the risk turning into a disaster event.

8.2. Environmental Risk Identification

8.2.1. Departmental organization risks checklist
Although it is difficult to measure the significance of each factor, it is generally possible to make an overall evaluation. The organization risk checklist should cover:

- Security Atmosphere
- Authorization
- Recording
- Asset Safeguarding
- Accountability

8.3. Physical Site Risk Identification
Departments should complete a physical site risk analysis of the department/unit. The result of this analysis is a list of pre-disaster precautionary measures.

The physical site risk analysis considerations are:

- Fire
- Flood
- Lightning
- Sabotage
- Power Failure
- Air Conditioning Failure
- Floor/Roof/Wall Collapse
- Major Equipment Failure
9. Risk Reduction

9.1. Computer Data Protection

Computer data is protected by a combination of backup procedures, offsite storage procedures, and database management procedures. A backup process copies the data from disk to magnetic tape or cartridge so that data that is lost or damaged for any reason can be restored. Offsite storage for these media protects the data in the event that the computer itself is destroyed due to a disaster in or surrounding the area where servers are located.

9.2. Cyber-Terrorism and Cyber-Crime Protection

The University has acquired anti-virus software to detect computer viruses. This anti-virus software is available through The University Site License Office and is provided free of charge to all campus affiliates.

Procedures and software should be in place to monitor the network and server utilization that will report any attacks or overloaded segments of the network. Operating system patches should be kept up to date as well as other security patches for applications.

9.3. Physical Security

9.3.1. Building, Computer and Switch Room Access

Access to buildings, secure workspaces, and computer rooms is generally the responsibility of the each employee working in the area. We must be cognizant of existing University security guidelines and, if necessary, modify those to meet each of our individual needs. This would include locking exterior doors, restricting access to server/computer rooms, reviewing OmniLock access lists periodically for changes, changing passwords & passcodes with staffing changes, etc.

9.3.1.1. Building Doors

All exterior doors are generally locked at night seven days a week by Facilities Management. Inform the occupants of your building of the ‘closed hours’ (check with your building monitor for your specific closure hours). If access is needed during ‘closed hours’, arrangements can be made with FM to provide access to the building. DO NOT prop open entrance doors.

9.3.2. Fire Risk

The risk of fire in your building can be reduced by:

- Strategically placing portable Halon fire extinguishers throughout the building with location markers clearly visible
• Installing an overhead pre-action-water fire suppression system
• Training and equipping personnel to take immediate action against incipient and relatively insignificant fires
• Training operating personnel in fire reporting
• Storage of flammable supplies outside of computer/server rooms
• Placing large inventories of printing equipment and paper in a separate room from the computer systems
• Installing a building fire detection system with an alarm system tied to the campus and the City Fire Department systems
• Installing a separate computer room Halon Fire Suppression tied to the building and campus fire alarm and notification systems
• Coordinating installation of major equipment systems and any modifications to the computer/server rooms with the Risk Management and Planning Offices at the University to insure compliance with city, county, state and federal fire codes
• Construction of the computer/server rooms from other occupancies in the building by fire-resistant rated walls, floor, and ceiling

9.3.3. Water Damage Risk

The risk of water damage can be reduced by:

• Removing any existing water pipes from the ceiling and using pre-active-water fire suppression systems
• Installing water-sensing devices under the false floors of computer/server rooms that sound an alarm in the room and identifies the location on a LED panel

9.3.4. Lightning Damage Risk

The risk of electronic component damage due to lightning strikes or associated electrical spikes can be reduced by:

• Installing lightning rods on the building
• Installing a grounding grid for all computers
• Providing power conditioners to protect major computer systems from power surges

9.3.5. Risk of Sabotage

The risk of damage to University buildings as a result of sabotage of any kind can be reduced by:
• Controlling access to computer/server rooms
• Providing limited access to high security risk areas
• Installing exterior doors of sufficient strength to deter impulse intrusion
• Replacing all windows in computer/server rooms with wired glass windows or walls
• Training personnel regarding proper reporting procedures for bomb threat, presence of unauthorized personnel and activist sit-ins
• Monitoring the facility with cameras and recording the activities of several locations

Recommendations for future consideration are:

• Classifying critical positions as sensitive and require pre-employment criminal background investigations

9.3.6. Power Failure

The risk of damage or prolonged downtime due to power failure can be reduced by:

• Installation of a backup diesel generator capable of providing long-term emergency power to the building
• Installation of Uninterrupted Power Supply (UPS) capable of sustaining power until the backup generator takes over
• Installation of Uninterrupted Power Supplies (UPS) capable of sustaining power to computer/server rooms providing clean power with the capability to ride thru power faults and giving the operations staff ample time to power down and protect servers in the event of a total loss of electrical services
• Having the capability to switch power for the building to a different feeder on the same sub-station in the event of a power source failure

9.3.7. Air Conditioning Failure

The risk of service interruptions caused by air conditioning failures can be reduced by:

• Having independent air conditioners in the computer/server rooms
• Installation of a redundant chilled water supply system

9.3.8. Particulates Contamination

The risk of service interruptions due to paper dust and other particulates can be reduced by:

• Separation of printers and disk drives into different computer rooms
• Regular cleaning by Facilities of the top floor and/or concrete sub-floor
• Cleaning or replacing filters on disk drives and other hardware during regular Preventative Maintenance sessions
• Routine cleaning of equipment by Computer personnel

9.3.9. Floor/Roof/Wall Collapse

Comparing statistics provided by Risk Management on floor weight limitations with equipment weight specifications to insure the weight-load threshold for each floor is not surpassed can reduce the risk of floor/roof/wall collapse.

9.3.10. Major Equipment Failure

The risk of major equipment failure can be reduced by:

• Installing devices to monitor temperature and humidity
• Requiring maintenance agreements on all equipment dictating vendor response time to preclude any system from being down an inordinate amount of time and scheduling adequate preventive maintenance for each component
• Having reciprocal, or mutual aid, agreements with another facility to run critical applications when one facility is temporarily inoperative

9.4. Access to Computing Systems

9.4.1. Data Access and Ownership Policy

Data access is the process of granting individuals the use of the information systems as set forth in a Data Access and Ownership procedure.

9.4.2. System Administration

The department has responsibility to establish standards, procedures, and guidelines necessary to administer access to University data and monitor login security of on-line systems. There are University approved policies that are in use by the Department Computer support office. These are:

• CCIT Computer and Network Usage Policy
• CCIT Online Access Policy
• UAINFO Web Page Policy
• The Computing Account Privilege Policy screen that is displayed when creating an account through the ACCOUNT program
9.5. Computer Operations

The Computer Operations staff should be responsible for logistical planning in the event it is necessary to implement the Disaster Recovery Plan. This planning includes:

- Maintaining space, power, communication, and utility requirements, which would be needed at an alternate site for acceptable operation
- Locating backup sites, checking for suitability, and negotiating as necessary for their use in a disaster situation
- Maintaining a list of supplies consumed each week by building personnel
- Maintaining an off-site emergency stockpile of consumables to cover the lead-time taken to reorder and deliver
- Working with Procurement and Contracting Services to see that they prepare a list of emergency suppliers of the items needed and that are not available from Surplus Property
- Compiling and maintaining a list of all supplier and emergency contacts and numbers

9.6. Insurance

The State of Arizona self-insurance program covers the University of Arizona. This self-insurance program as described by the Department of Risk Management contains the necessary ingredients to cover University building disaster recovery needs.

9.7. Backup Procedures and Schedule

9.7.1. Equipment Operations Backup Procedures

A comprehensive backup schedule by hardware should be identified and listed in a separate checklist. For example, general backup procedures for computer data are as follows:

- Incremental backups are done nightly on all disks
- Full backups are done weekly on all disks
- Special backups are done as required or requested by systems users

9.7.2. Storage Procedures

Backup tapes should be stored both on-site and offsite, in approved and known locations.
10. Disaster Recovery Strategies

10.1. Strategy Development

No single strategy appropriate to the University of Arizona operating environment has been identified short of providing a totally redundant facility.

10.2. User Service Level Requirements

Requirements are discovered using the DPI (Appendix D).

10.3. Service Level Alternatives

10.3.1. Service Degradation Strategies

In analysis of disaster recovery alternatives it is necessary to identify as many candidates for a service degradation strategy as possible. If a major disaster event occurs, the Disaster Management Team may have available computer resources that amount to a fraction of that which we normally need to process all our applications.

Service degradation strategies that should be considered are:

- Reduction of Service or Normal Response: This strategy normally applies to lower priority batch processing that could be accomplished on a time available basis at University or non-University facilities. It is not applicable to interactive processes or when the batch processing is necessary to support a high-priority function.

- Implementation of Manual Procedures: Almost all applications represent an electronic data processing solution to what was previously a manual process. Reversion to the manual process should always be considered because in some cases it may be the only solution available.

- Withdrawal of Services: There are some functions where the obvious strategy may be to simply not perform their primary functions (develop new applications) until full service has been restored.

11. General Disaster Procedures

A series of procedures follow as a reference for prompt and appropriate actions to be taken in potential emergencies or events that cause interruption of computer service.

Orientation sessions should be held periodically to familiarize employees with these procedures and to outline responsibilities in the event of such emergencies. All general emergency procedures should be reviewed twice each year.

Copies of this Plan are to be kept in key locations for ready reference.
The most important asset is our personnel. Risks should not be taken to save other assets when personnel may be in jeopardy.

11.1. Emergency Calls

The emergency phone list is provided in Appendix C - Contact List. The most critical of those numbers at the University of Arizona main campus are summarized as follows:

<table>
<thead>
<tr>
<th>Service</th>
<th>Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fire</td>
<td>911</td>
</tr>
<tr>
<td>Police</td>
<td>911</td>
</tr>
<tr>
<td>Accidents</td>
<td>911</td>
</tr>
<tr>
<td>Medical Assistance</td>
<td>911</td>
</tr>
<tr>
<td>Poison Control Center</td>
<td>626-6016 or 1-800-362-0101</td>
</tr>
<tr>
<td>UMC Hospital Emergency Room</td>
<td>694-6093</td>
</tr>
<tr>
<td>Facilities Management (Elevator)</td>
<td>621-3000</td>
</tr>
<tr>
<td>Victim Witness</td>
<td>740-5525</td>
</tr>
<tr>
<td>Tucson Rape Crisis Center</td>
<td>327-1171</td>
</tr>
<tr>
<td>Crisis Line</td>
<td>327-7273</td>
</tr>
</tbody>
</table>

11.2. Fires

11.2.1. Prevention

- Review all areas of responsibility for combustible materials including below raised floors. Floor panel lifters are located in the computer room and operations area.

- Operational areas are to be sight checked by each shift before they leave, and particularly if the area is to be left unoccupied. All new employees will be educated about department’s fire procedures by their departmental managers during employee orientation.

- Regular site inspections, which include general area review, and checks of electrical connections, fire extinguishers, and smoke detectors, are to be made every 6 months. Should anyone discharge an extinguisher or notice one with the safety seal broken, the Facilities Management Maintenance desk should be contacted.

- As designated by state law there is NO SMOKING allowed in any building.

11.2.2. Detection

- The Department of Risk Management and Safety insures that each fire alarm system throughout the campus is tested on a periodic basis. The system, including all component parts, is verified for operation, serviceability and audibility by a qualified electrician trained, fire safety person or University approved contractor in fire alarm systems used at the University of Arizona.
• The fire alarm systems are tested and maintained in accordance with frequencies established by the National Fire Codes and the State Fire Code. A report of these tests is maintained in the Division of Facilities Management.

11.2.3. Fire Extinguisher locations

• Enter your Extinguisher plan here.
• **DO NOT PLAY HERO.** If the fire is of any consequence, leave the building immediately.

11.2.4. Policy for Appropriate Action if a Fire or Alarm Occurs

If you discover fire, smoke, or hear the fire alarm:

• Leave the building **immediately** via the stairs. **DO NOT USE THE ELEVATORS.**
• As you leave **close all doors**, including those propped open,
• On your way out, you will pass a fire alarm pull station. If the alarm is not already ringing **PULL IT**.
• Once outside, move as far away from the building as possible to allow easy access by fire department vehicles.
• **Insert departmental plan here.**
• The Building Monitor should call the University Policy Department and report the details of the fire:
  • **UAPD: 621-8273 or 9-1-1**
  • Remain outside the building until the “ALL CLEAR” is given by the Tucson Fire Department or UAPD. Silencing of the alarms does not constitute and “ALL CLEAR.”

*For mobility impaired persons:* If a person with a mobility impairment is able to exit the building without use of the elevator, then evacuation should follow the appropriate route out of the building. If the exit from the building is only possible by use of the elevator, follow the procedures outlined below:

• The mobility-impaired person should proceed or ask for assistance to the nearest enclosed stairwell or “area of safe refuge” and remain there. In case of a fire, enclosed building stairwells are “safe refuge areas,” and have a higher fire resistive rating. The person should notify someone (a coworker, supervisor, instructor, or building monitor) that they are seeking refuge in the stairwell. If possible, a means of communication (i.e. cell phone) should be taken to the stairwell.
• Make sure the door to the stairwell is closed. Open doors will violate the “safe refuge area” and will allow smoke, and possibly fire, into the stairwell.

• Once outside, the person with information should inform the Tucson Fire Department (TFD) Incident Command Center that there is a mobility-impaired person in a stairwell, which floor the person is on and location of the stairwell or refuge area. When stairwell evacuations are necessitated, such decisions and evacuations will be made by TFD. **UNIVERSITY PERSONNEL SHOULD NEVER ATTEMPT TO CARRY ANYONE DOWN THE STAIRS.**

• After the “ALL CLEAR” has been given by TFD or University Police, UAPD personnel will immediately go the stairwell or refuge area and inform the person that it is safe to re-occupy the building.

**11.2.5. Additional Building Evacuation Issues**

• If you are trapped in an area with no windows or other exits, close all possible doors or other barriers between you and the fire. Attempt to seal the gap below the bottom of the door with wet towels or other low-flammability material. If a phone is available and working call the campus emergency number (911). Wait calmly for help.

• It is not necessary to take magnetic tapes or computer disk packs with you when evacuating the building. All systems should be backed up offsite on a frequent enough basis to make recovery possible from tapes stored at the offsite storage location.

• If time permits before evacuation, all power is to be shut off to equipment and overhead lights. If you have emergency power off (EPO) switches, pull them. Any of these switches will cut off all power to the equipment in the computer room.

**11.2.6. Goals**

• Protect the lives and health of employees
• Protect essential documents, records, and data
• Minimize damage to data processing equipment and other property

**11.3. Fire Extinguisher Procedures**

The following procedures are posted next to each fire extinguisher in the data processing area. These procedures are to be followed in the event of a fire.

• Call the campus emergency number: 911. Inform them of the building address, the location of the fire, and what type of fire it is (paper, electrical, etc.).

• If there is time, computer operators should power down the system(s) before cutting power.

• Cut off all electrical power by pushing the Emergency Power Off (EPO) switches, if you have them.
• If the fire is small, use a fire extinguisher AFTER YOU HAVE CALLED THE
CAMPUS EMERGENCY NUMBER (911). Pull the pin on the fire extinguisher, and
then discharge the extinguisher by aiming at the base of the fire using a side-to-side
sweeping motion.
• If the fire is such that employees should evacuate the building and no alarm has sounded,
follow the procedures define in the “Policy for Appropriate Action if a Fire or Alarm
Occurs.”
• Notify the designated Building Monitor, Disaster Management Coordinator and your
Executive Director.
• When leaving the building, exit by using the stairs. DO NOT USE THE ELEVATORS.

11.4. Building Monitors

Facilities Management maintains a list of building monitors as their contact for communicating
issues regarding each building, the campus and other facility related concerns. This list can be
used as a contact point regarding computing and telecommunication outages, changes or other
distributed computing requirements and issues. Check with Facilities Management for the latest
listing.

11.5. Electrical Power Outages

The occurrence of an unexpected power outage is most likely caused by a failure of the public
power utility or the Facilities Management distribution system. In most cases, return of power is
usually within a few hours, but the Operations Manager is responsible to contact Facilities to
determine how long the outage is expected to last. When power has been restored the first action taken is the verification of data integrity. The
amount of time needed prior to returning the system to the users depends on the condition of the
data and the number of recovery procedures needed to return the systems to an operational status.
If a power problem exists even though public power is not out of service, such as after
restoration of power, the following people need to be notified:

• Facilities Management (normal hours) at 621-3000. (This number is forwarded to the
Central Plant after hours)
• Campus Police (after hours)

11.6. Flooding

11.6.1. Prevention

• Review the facility at least annually for knowledge of risks relative to flooding. The
review should include identifying where water pipes and drains are in respect to the
computer rooms, the route of pipes and drains to make sure any risk of flooding is
reduced. Additionally, knowing what the potential is for flooding from above (upper floors or roof) is key to prevention.

- Review how the computer facility lies physically in respect to external flood possibilities and what steps can be taken for prevention.
- During heavy weather conditions, particularly the annual monsoon season, inspect windows, roofs, and basements in proximity to the computer rooms for flooding or water buildup.
- Inspect at least twice annually all pipes and valves within the computer facility for leaks.

11.6.2. Detection

- The detection of water within the computer facility, particularly under the raised floors, is vitally important to prevent electrical shocks, short-circuits, or equipment damage.

11.6.3. Evacuation

- If flooding is such that employees must evacuate the building, call the Campus Emergency Number at 911 and give them the details (what is happening, where in the building, etc.) and notify the designated building monitor and the Disaster Management Coordinator.

- Before evacuation, all power is to be shut off to equipment and overhead lights.

11.7. Flooding Procedures

- Call Facilities Management building maintenance immediately.
- If flooding is such that there is no risk of electrical shock, computer operators should power down the system(s) before cutting power. Otherwise, computer operators should leave the area immediately and shutoff power (trip EPO) when leaving.
- Cut off all electrical power to the room.
- If time allows, do all that is possible to provide for the protection of the equipment. If flooding is coming from overhead, drape the equipment with heavy plastic.
- If flooding is such that employees must evacuate the building, call the Campus Emergency Number at 911 and give them the details (what is happening, where in the building, etc.) and notify the designated building monitor and the Disaster Management Coordinator.

11.7.1. Goals

- Protect the lives and health of employees
- Protect essential documents, records, and data
- Minimize damage to data processing and telecommunications equipment and other property
11.8. Hardware Failures

11.8.1. Hardware Inventory

A complete Hardware Inventory list should be maintained. A template for this is included in (see DPI) of this document.

11.9. Systems Software Failures

Review the software inventory for priority recovery of critical applications. (see DPI)

11.10. Custom or third-party Application Failures

Some of the applications packages were purchased from third-party sources and are maintained by those companies. Some may be developed or highly customized and are now maintained in house. (see DPI) provides a list of the application software in production.

11.11. Cyber-Terrorism and Cyber-Crime

The network includes Cisco Secure Intrusion Detection Systems that are capable of detecting and taking action against malicious network traffic coming to campus and leaving campus. Anti-virus protection software is also available to the campus community to provide protection against virus attacks. It is strongly recommended that all centrally connected and supported systems have and routinely update the anti-virus software as well as security patches.

11.12. Major Disasters

A major disaster is the inability to operate the computers for a period of time long enough to seriously affect business operations. Reasons may vary from actual destruction of the data center to less severe emergencies that affect the computer operation while leaving the data center intact.

12. Disaster Recovery Plan Activation

12.1. Initial Response

12.1.1. Emergency Response Procedures

- In the event of any emergency situation such as a fire, power outage, telecommunications failure, network attack, flood, explosion, hardware failure, etc., the appropriate general procedures will be followed as described in the section “General Disaster Procedures”.

- If the emergency occurs while Computer support staff is on duty, they will utilize the emergency phone notification list as appropriate to the nature of the emergency in order to report the incident to the appropriate supervisor, manager, or administrator. If no support staff is on duty, the Campus Police have procedures for proper notification.
In the event a building evacuation occurs during normal prime time business hours (Monday thru Friday, 8 a.m. to 5 p.m.), all Disaster Management Team members will assemble at a designated location. If the weather dictates that an indoor assembly location be used an alternative site will be used. This will enable the communication and coordination for further instruction and any activity planning that may be required.

12.1.2. Disaster Management Team Notification

- Depending upon the severity of the emergency the Disaster Recovery Coordinator should be notified immediately. The Coordinator maintains an emergency notification list and will ensure that all key personnel have it available. If the Coordinator cannot be reached other members of the Disaster Management Team will be called until one of them is notified.

- The first member of the Disaster Management Team to be notified is responsible to notify other critical members of the team and to initiate action. The Disaster Management Team, or their alternates, will call other supervisors and specialists with current information on the disaster and instruction as appropriate. The Disaster Management Team members will start the telephone contacts for their own staffs.

12.1.3. Initial Disaster Management Procedures

- Once the Disaster Management Team has been notified, they will proceed to make an immediate assessment of the situation and to initiate appropriate actions. If necessary the initial action will be to assemble the Disaster Management Team.

- If the Disaster Recovery Coordinator has not yet been contacted, an alternate shall be selected by the Disaster Management Team and will assume full responsibilities of the Disaster Recovery Coordinator, until he or she has arrived and been fully briefed. The Disaster Recovery Coordinator or acting Coordinator will proceed to implement the contingency plans.

- Make an assessment of the situation directly at the scene if possible, or if not, indirectly based on reported information from the notification sources.

- Based on the Team’s assessment of the situation, determine the severity of the problem and decide on the appropriate actions.

- If the Disaster Management Team determines the emergency to be a major disaster proceed to do the following: activate an emergency control center; notify the appropriate emergency teams; notify upper administrative officers and other top management; and determine viable contingency alternatives. These steps constitute activation of the Disaster Recovery Plan for a major disaster.

- If it is necessary to declare a major disaster a complete record of all actions taken must be recorded. To accomplish this, a log will be supplied to the Disaster Management Team members and each Disaster Recovery Team Leader. The logs should contain as much information as possible. Summary entries are appropriate if time is a constraint; the details may be added later. The logs provide a written time-stamped record of actions taken and provide an invaluable tool for use in the disaster recovery review process. The
Communication Team will generate and maintain a photo album of events to aid in the review and communication of issues.

- If the Disaster Management Team does not determine the emergency to be a major disaster, then the appropriate correction or recovery procedure will be implemented. In such a case, selected recovery teams may or may not be called upon to take action.

**12.1.4. Activation of an Emergency Control Center**

- In the event of a major disaster, a centralized control center will be established from which all communications and activities will be directed.

**12.1.5. Notification of Necessary Disaster Teams**

In the event of a major disaster scenario, the University Administration and the Disaster Recovery Teams will be notified and apprised of the emergency. The administration will be kept apprised of the status of personnel, property, and the recovery effort. A template is provided in Appendix A to outline the basics for the creation of your own specialized Disaster Recovery Teams. Use this template to define your teams and insert the appropriate information in your Disaster Recovery Plan. Designated team leaders, alternate team leaders, and team members should be identified. Also specify are the responsibilities and disaster recovery functions of each team.

- Determine which Disaster Recovery Teams should be activated and if the presence of additional administrative support is required to support the recovery activities or contingency procedures.

- The Disaster Management Team will determine which individuals within the University administration should be notified and the College Executive Director will be the selected representative to provide the notification. The Coordinator or anyone else on the Disaster Management Team can notify the Disaster Recovery Teams.

- Notifications to the Administration should cover what happened, the current status, the plan of action, and the location and phone numbers of the Emergency Control Center. They should also be informed whether their presence is required and when.

- Notifications to the Disaster Recovery Teams should cover what happened, the current status, the plan of action, and the location and phone numbers of the Emergency Control Center. Each Team Leader and alternate has a copy of the Disaster Recovery Plan and is prepared to initiate action appropriate to his or her Team. The Team Leaders are responsible for notifying their teams to assemble and act according to their responsibilities and disaster recovery functions.

- All emergency personnel will bring their personal copies of the Disaster Recovery Plan and other documentation for which they are responsible to the emergency coordination meeting at the Control Center.

- Individuals responsible for the physical offsite backup storage locations and University designated cold-sites and hot-sites will be notified that a disaster has occurred if it is deemed necessary to activate them.
12.1.6. Disaster Management Team Coordination

- When all of the required Disaster Management Teams have been assembled at the Emergency Control Center, the Disaster Recovery Coordinator will brief them on what has occurred and provide an overview of the Disaster Management Team’s assessment of the status.

- Based on this information, all teams will be asked if they are aware of other information or circumstances that need to be considered. The teams should collectively discuss all of the basic aspects of the situation, and considerations of problems due to the processing schedule or anything else, before proceeding to carry out their individual team functions.

- Before any team leaves, the Disaster Recovery Coordinator will review with each team leader the actions that each team will be taking.

12.1.7. Preparation for use of Contingency Site(s)

No single strategy appropriate to the University of Arizona operating environment has been identified for the selection and use of contingency sites. The development of appropriate disaster recovery strategies covering the University of Arizona’s diverse facilities, hardware configurations, operating systems, and application requirements is very complex and impossible to document considering the full range of disaster scenarios possible.

The approach therefore has been to define a matrix of the application needs of our users, the minimal hardware and software requirements of applications, critical periods of operation, and priority processing. The Disaster Management Team will match these requirements to the inventory of contingency site alternatives and then processing priorities will be established.

12.1.8. Contingency Operations Procedures

- All Disaster Recovery Teams will assemble at the Emergency Control Center for briefing, discussion of any identified problems, and coordination of the recovery effort.

- The Applications and Production Services teams will identify the work in progress that needs to be recovered and how that can best be accomplished. The teams will be prepared to help bring the applications up and recover work in progress. They will be responsible for notifying the user departments and coordinating their interface procedures.

- As needed, teams will proceed to the contingency site(s) immediately and begin loading software and data to prepare for system operations. Once established, processing will be maintained at the contingency site as directed by the Disaster Management Team.

- If hardware has been destroyed, damaged, or negatively affected, the needed teams will take the appropriate action to repair or replace the affected hardware.

- If facilities have been destroyed, damaged, or negatively affected, the Disaster Management Team will take the appropriate action to repair or replace the affected facilities through the Facilities Management Team.

- The as needed notification and summary of event information to departmental staff, the University and the Tucson community will be defined.
• The Support Teams will assist the operation of the Emergency Control Center and the Disaster Recovery Teams as required. A primary role will be to provide human essential support such as food, water and other comfort accommodations.

• The Disaster Management Team will continue to maintain the Emergency Control Center as long as necessary and will coordinate the contingency operations until they can be returned to a normal, non-emergency state.

12.2. Initial Recovery at a Contingency Site

12.2.1. Initial Procedures at Contingency Site

• If a site has been selected which is already in use by another department, the appropriate department administrator(s) will be contacted to discuss the use of their system and how it may best be accomplished.

• Every effort will be made to leave the existing system and applications intact. A priority to use the contingency facility is to coordinate with appropriate vendors the upgrade of these facilities to include in-cabinet upgrades of the CPU, the addition of controllers, disks and other peripherals, the addition of memory and the use of expansion cabinets as needed.

• Additional hardware and environmental upgrades will be ordered as necessary to upgrade the site. This needs to include security and emergency protection as required. A full precautionary backup of the system will be completed even if it is not necessary to remove the resident applications.

12.2.2. Offsite Storage and Pickup of Backup Materials

• The Computer Support Team will proceed to the offsite backup storage location and identify the most recent backup tapes and documentation.

• The Computer Support Team will assemble from the offsite inventory storage facility all necessary supplies for computer operations.

• The tapes, documentation, and supplies will be delivered to the selected contingency sites as specifically instructed by the Disaster Management Team. Once the backup tapes and documentation have been loaded at the contingency site it is imperative that they be returned to the backup storage location.

12.3. Full Operation at a Contingency Site(s)

12.3.1. Establishing Contingency Site Operations

• Before operations may begin at a contingency site, it is necessary to determine the status of production files and work in progress. In cases where the combination of work schedule, backup schedule, and offsite storage schedule results in serious loss of data, the different teams will need to meet to evaluate alternatives.

• Once issues of lost data or lost work have been resolved operations at the contingency site may commence. The Support Team will organize all materials (tapes, documentation,
hardware, and supplies) in an area designated by the contingency site personnel. For simplicity and control, these should be restricted to a single area if possible.

- The Support Team should familiarize themselves with the facility, the operations environment, emergency procedures and any security procedures to be observed. When the contingency site personnel have completed their preparations as agreed upon (purged the system, installed upgrades, etc.) the teams may begin to restore the required systems and files.

- Once the systems and files have been restored, tested, and verified coordination will take place with the Support Teams about their specific steps to recover lost work (data lost due to lost incremental backups and work in progress at the time of the emergency). It is the responsibility of the Support Team to work with the Users to resolve what will be done.

- Once the recovery procedures have been agreed upon, the Users will be asked to verify results at each step. All personnel may be required to assist with data entry during the recovery process.

- When the key users have determined that the recovery work has been completed, the resumption of processing can be scheduled.

### 12.3.2. Recovery of Lost Data

- The Support teams are responsible for coordinating with the Users to first identify what work has been lost, if any, through lost incremental backups, lost work that was in progress, and lost source documents.

- In the case of lost work in progress and lost documents, the Users are responsible for recovering or duplicating the lost documents or the information contained in them.

- If data has been lost the combined teams will determine how the data or work will be recovered. The lost work will be recovered as best possible. This may involve around the clock efforts, doing data entry, correcting data files, running special jobs, or rerunning production jobs.

### 12.3.3. Coordination with Application Users

- It is the responsibility the Support Teams to ensure that the applications systems work properly for the users, that lost work is recovered, and that the users understand the how to interact with and use the systems during the contingency operation.

- Upon completion of the joint disaster review meeting, the Support Team’s first priority is to determine the status of production files and work in progress.

- The Support Team leaders will brief the key users on the initial status situation, then divide employees up into groups by application system or subsystem, preferably with a mix of users, programmers and production services staff in each group.

- When the issues of recovering lost work have been ironed out, the Support Team leaders will coordinate a work schedule with the key users. At this point, impact on ongoing work should be carefully discussed so the key users clearly understand the situation and can give appropriate directions to their subordinates. User departments must understand
what their interim work plans will be until their automated systems are recovered and
back online.

• Once the recovery process is completed, the Support Teams will coordinate with the key
users to ensure that they understand how they interface with their applications and what
the restrictions are. If the numbers of workstations cannot handle the workload, users will
need to work in shifts to take advantage of nighttime hours. If unexpected problems are
encountered, the Support Teams will work quickly to find alternatives.

12.3.4. Specific Application Procedures

• Documentation describing specific application procedures is the responsibility of each
Support Team. This documentation will include systems and program level
documentation, run flow documentation, users manuals and other documentation as may
be necessary. Reference may be made to the Administrative Information Systems
Programming Standards manual for specific descriptions.

12.4. Restoring Original Operations

12.4.1. Hardware Replacement

• Depending on the component, vendor maintenance agreements may cover replacement or
the order time can range from two weeks to two months for hardware systems from the
original hardware vendors. Used equipment vendors usually have hardware available for
immediate shipping; in most cases delivery could be expected within two weeks. The
Contracted vendor for equipment in the event of an emergency can also provide
permanent replacement hardware.

• The Support Teams are responsible for maintaining lists of hardware components,
purchase alternatives, delivery times, and costs.

• The departmental accounting office is responsible for coordinating with Procurement the
replacement of hardware on an emergency basis in a manner more expedient than that
normally possible using standard procurement procedure.

12.4.2. Return to Normal Operations

• When the operation is transferred back either to the department or to a new facility the
contingency operation will be quickly phased out.

• The final activity of the disaster recovery process will be a meeting and briefing of the
Disaster Management Teams. The Disaster Recovery Coordinator is responsible for
collecting the Action Logs maintained by the individuals asked to keep them, and to
document the events, problems and solutions, etc.

• During the next review of the Disaster Recovery Plan, the Disaster Recovery Coordinator
will be responsible to ensure that any lessons learned are incorporated in the Plan.

13. Maintenance & Testing of the Disaster Plan
After the plan has been formalized, and appears to be reasonably sufficient, there are two principal activities that must be planned and accomplished. They are:

- Periodic reviews of the plan to ensure it is kept up to date, distributed, and understood. The maintenance of the Disaster Recover and Team Plans is to keep it synchronous with program, hardware, software, physical environment, network and applications changes over time.
- Testing of the plan within imposed constraints to determine whether it is effective, efficient, and up to date.

### 13.1. Review & Maintenance of the Plan

Any reasonable review of this (or any other disaster recovery plan) cannot be conducted without understanding what types of disasters could realistically affect the operations in the department, what the most probable disaster scenarios are, and under what assumptions and constraints the Disaster Recovery Plan was created.

The effectiveness of the Disaster Recovery Plan is impacted by changes in the environment that the plan was created to protect. Some major factors that will impact the plan are: new equipment, changes to existing equipment, changes to the network, a changing software environment, staff and organizational changes, and new or changing applications.

Review and Maintenance of the Disaster Recovery Plan is an ongoing process and should be conducted with the following points in mind:

- **Disaster Scenarios**
  - Procedures to recover from a disaster are written for the most serious occurrence; for purposes of formalizing the plan the following was considered:
    - The Facility - specifically the loss of the building facility itself or any of the hardware contained within it and;
    - The Personnel - the non-availability of key personnel or project team responsible for a particular application
  - Occurrences of lesser magnitude can be handled at the appropriate level, as a subset, of the recovery procedures developed.

- **Objectives**
  - Identification of critical functions with consideration of priority scheduling.
  - Identify alternate sites of operation, which 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 and database so that they can be summoned without delay when needed.
- Identify users of department services to be notified of delays and to be involved in the recovery process.
- Establish the personnel responsible for all phases of Disaster Recovery.

**Assumptions**

- Managers will keep all personnel affected by this plan aware of its procedures and amendments.
- All personnel affected by this plan are responsible for understanding their role under a disaster situation.
- A current copy of this plan should reside with each member of the Disaster Management Team (DMT).
- This plan will be continually maintained, reviewed, and tested at least once annually.
- All personnel will react quickly and effectively during the recovery process.
- Disaster Recovery can only be successful if there are routine backups according to the schedules provided, of the system software, proprietary packages, programs, and data, and with regular testing of hardware and communications backup facilities.

**13.2. Testing the Disaster Recovery Plan**

Disaster Recovery testing verifies that all facets of the Plan have been implemented and have been found to be accurate and sufficient. After initial acceptance of the Plan, ongoing testing on a periodic basis is necessary to ensure the continued viability of its contents.

**Test Parameters**

Testing can be as simple as examining the existence of documentation, or as complex as simulating a major disaster. This Disaster Recovery Plan is tested for all procedural and organizational aspects and technical recovery capabilities up to but not including testing at contingency site locations.

The reason for the contingency site test restriction is because the contingency locations are in fact operational systems supporting University functions, equipment that will only be made available in the event of a disaster, and a vendor hot site recovery facility has not been funded. In the event of an emergency, the hardware at these contingency locations would be upgraded to accommodate the emergency operations of other University departments and applications impacted by the disaster, or space would be allocated to enable the installation of vendor supplied equipment to provide recovery.

**Procedures**

GENERATE YOUR DEPARTMENTAL PROCEDURES HERE
14. Disaster Team Template

14.1. Team Coordinator/Leader

(Team Leader Name):    Home #:    
Cell phone#:               Pager#:    
Email Address:
Office Rm/Bldg:

The Primary responsibility of the Team Leader is to provide leadership of the recovery team and coordinate support for the recovery effort. Other responsibilities include:

1. Participate in recovery meetings with the Crisis Management Team.
2. Direct the Business Continuity efforts of your team.
3. Oversee communications activities of the team.
4. Coordinate with the Emergency Operations Center regarding all administrative issues.

14.2. Definition of Team

Define what this team is in charge of, who they will contact.

14.3. Roles Required

Define the role this team plays in the recovery process.

14.4. Team Members

List all team members, contact information, associated teams.

14.5. Responsibilities

Define responsibilities of each member.

14.6. Task Assignments

What specific task should be accomplished?
### 15. Information Technology Crisis Management Team

<table>
<thead>
<tr>
<th>Employee Name</th>
<th>(netID)</th>
<th>Management Position</th>
<th>Reports To Position</th>
<th>Approval Limit</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ray Corral</td>
<td>corrar</td>
<td>Residence Life Campus</td>
<td>Team Chair CMT</td>
<td></td>
</tr>
<tr>
<td>George Davis</td>
<td>davig</td>
<td>Senior Vice President</td>
<td>Team Chair CMT - Academic Affairs/Provost</td>
<td></td>
</tr>
<tr>
<td>Anthony Daykin</td>
<td>daykia</td>
<td>Chief, UAPD</td>
<td>Team Chair CMT - Director, UA Security</td>
<td></td>
</tr>
<tr>
<td>Steve Holland</td>
<td>hollas</td>
<td>Risk Management Campus CMT</td>
<td>Team Chair CMT</td>
<td></td>
</tr>
<tr>
<td>Sharon Kha</td>
<td>khas</td>
<td>Institutional Advancement CMT</td>
<td>Team Chair CMT</td>
<td></td>
</tr>
<tr>
<td>Peter Likins</td>
<td>likinp</td>
<td>President of the University CMT</td>
<td>Team Chair CMT</td>
<td></td>
</tr>
<tr>
<td>Peter J Perona</td>
<td>peronp</td>
<td>CCIT Executive Director CMT</td>
<td>Team Chair CMT</td>
<td></td>
</tr>
<tr>
<td>Al Tarcola</td>
<td>tarcoa</td>
<td>Facilities Management CMT</td>
<td>Team Chair CMT</td>
<td></td>
</tr>
<tr>
<td>Melissa Vito</td>
<td>vitom</td>
<td>Assoc. Vice President, Campus Life &amp; Dean of Students CMT</td>
<td>Team Chair CMT</td>
<td></td>
</tr>
</tbody>
</table>
16. Contact List/Phone Numbers

16.1. CENTER FOR COMPUTING AND INFORMATION TECHNOLOGY

email: consult@u.arizona.edu  
CCITInfo Line (pre-recorded information)  621-CCIT  
Computing  621-CCIT  
Computer (email) Accounts  621-2985  
Repair--Phone and Network  621-7999  
Support Desk  621-HELP  
Network/Data  621-7999

SIRT Team: sirt@arizona.edu  
SIRT (Security Incident Response Team)  626-0100  
Customer Service--Phone and Data Work Orders  621-8999  
Modems--Dial In Service  618-3190  
Network Consulting  621-ENET  
Repair--Phone and Network  621-7999  
IT Services  621-CCIT  
Faculty Ctr. for Instructional Innovation  626-2621  
Labs--Open Access and Reservations  621-9491  
Multimedia and Visualization Lab  621-9404  
Site License Software  626-SITE  
Training Classes and Tours  621-8682  
UAINFO Implementation Team  621-WWWS  
Production Services  621-2781  
Telephone/Voice  621-7999  
Customer Service--Phone AND Data Work Orders  621-8999  
Repair--Phone and Network  621-7999  
Voice Mail  621-8999  
Directory Assistance (UA)  621-2211  
Research Computing Support  621-4245  
Telephone Billing Inquiries  621-4126  
Switchboard Supervisor  621-1938

16.1.1. Units

Administrative Computing  621-2701  
Business Office  621-4126  
Computer Operations  621-4036  
Telecommunications  621-5100  
User Support  621-8737  
CCIT FAX Number  621-8668
### 16.1.2. Important Phone Numbers

<table>
<thead>
<tr>
<th>Service</th>
<th>Phone Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data Line Orders &amp; Service Changes</td>
<td>621-8999</td>
</tr>
<tr>
<td>Telephone Orders &amp; Service Changes</td>
<td>621-8999</td>
</tr>
<tr>
<td>Data Line Trouble Reports</td>
<td>621-7999</td>
</tr>
<tr>
<td>Telephone Trouble Reports</td>
<td>621-7999</td>
</tr>
<tr>
<td>Telecommunications Billing Inquiries</td>
<td>621-4126</td>
</tr>
<tr>
<td>University Operator, Directory Assistance</td>
<td>621-2211</td>
</tr>
</tbody>
</table>