CANUTILLO INDEPENDENT SCHOOL DISTRICT
Data Back-Up and Resumption Planning Guide

Distribution List: Administrators, Campus Principals, Directors, Coordinators

Designated Sensitive Information

Approved by School Board: April 17, 2003

PREFACE

This document has been developed to minimize loss of critical information resources necessary for the continuation of the school district's operations and services following a disaster. It contains procedures and processes for conducting risk analysis, setting priorities for the recovery of information resources, and identifying which automation-based services are most critical to the district. Canutillo ISD is aware that emphasis has shifted, over the years, from "disaster recovery" to "business (or service) resumption" and planning procedures have been developed around a framework of planning steps.

ACKNOWLEDGMENT TO

State of Texas Department of Information Resources [March 2000 and April 1994], Telecommunication Infrastructure Fund Board [March 2002], and Massachusetts Institute of Technology [MIT Business Continuity Plan, 1995] for providing information that facilitated the development of this document.

TABLE OF CONTENTS

1.0 WHAT IS AN INFORMATION BACK-UP AND RESUMPTION PLAN?

The purpose of this plan is to provide a road map of predetermined actions which will reduce decision-making during data recovery operations, resumption of critical services at the earliest possible time in the most cost-effective manner. The plan will establish, organize, and document risk assessments, responsibilities, policies and procedures, and agreements and understandings for internal and external entities. The planning process enables Canutillo ISD to identify maximum acceptable down times which can be incurred in the performance of each of its mission related functions and to identify recovery actions accordingly. Functions and/or services must be restored within 24-48 hours require significantly different recovery actions than those that can be delayed a number of days.

2.0 IMPLEMENTATION

The strategy for a district-wide information back-up and contingency planning is important because the process affects virtually every area of the district.
TEN STEP PROCESS:

1. Administration and School Board Awareness
2. Information Services Resumption Team (ISR Team)
3. Capability Assessment
4. Perform a Risk Analysis
5. Establish System Priorities
6. Analyze and Define Requirements for Recovery
7. Design the Program for Recovery Operations
8. Conduct Service Resumption Training
9. Test the Service Resumption Plan
10. Updating Information Service Resumption Plan
11. Appendices

STEP 1. ADMINISTRATION AND SCHOOL BOARD AWARENESS

Canutillo ISD relies on information resources to deliver services and to perform educational and administrative functions. Administration and the School Board have been supportive of the technology efforts of the school district.

STEP 2. INFORMATION SERVICES RESUMPTION TEAM (ISR Team)

Position	***Department***
Assistant Superintendent of Facilities and Support Services	Administration
Comptroller	Finance
Director of Technology	Technology
Public Relations Officer	Public Relations
Technology Coordinator	Technology
Network Engineer	Technology
PEIMS Coordinator	Finance

STEP 3. CAPABILITY ASSESSMENT

An overall survey of the information resources environment has been performed to identify strengths and weaknesses and an assessment of the ability to recover from a service disruption. A failure may require that Canutillo ISD take tapes to a shell facility and use a similar AS400 system. The shell facility identified to be compatible with Canutillo ISD is Clint ISD in El Paso County. Contact person at Clint ISD is John McNicol, Manager of Network Services. *See Appendix B.*

STEP 4. NETWORK SECURITY ASSESSMENT

Network infrastructure security will address:

1. User Access – includes access privileges to data files, applications, predefined number of failed attempts, nonuse automatically log users off the network, etc.
2. Network Housekeeping – maintains audit trail of all adds, moves and changes to the network, access rights, server passwords, configuration management system, etc.
3. Data Protection and Fault Tolerance – LAN switch redundancy, hot swaps, Virus protection, Internet intruder protection, WEB Server Encryption, Firewalls, RAID level 5[1], WEP, etc.
4. Equipment Protection – use of uninterrupted power supplies (UPS), protect behind locked doors (servers, routers, switches), etc.
5. Hardware, Software, Maintenance –

    Include WEB, Database, and Application Servers (redundancy, load balancing and clustering, security, enterprise-level operating system, enterprise-level software, and high availability).

    Network Isolation should insure that unauthorized access does not occur in shared hosting environments.

    Multiple Firewalls must meet minimum standards (i.e., Cisco Pix).

    Multi-tier Environment should be achieved by isolating networks and having multiple firewalls.

    Encryption must be utilized by:

        Network-to-Network encryption via 3DES IP Sec VPN tunnels and/or

Host-to-Host encryption via Secure Shell and/or
Web Server Encryption and/or
Data encryption within the Database

Communication methods:
Internet Connection and/or
VPN Connection
Frame Relay and T1 Circuits

Intrusion Detection utilized:
External monitors outside the firewall environment and/or
Internal monitors inside the firewall environment and/or
Proactive management reviewing and monitoring signature trends and/or
taking appropriate action including stopping spamming and virus attacks.

STEP 5. PERFORM A RISK ANALYSIS

Risk analysis is used to assess potential service disruptions and to determine levels of protection necessary to reinstate vital services through risk assessment and risk management through control and security measures. *See Appendix C.*

Risk Assessment

Risk assessment is the comprehensive study of potential disruptions to service continuity, assignment of an occurrence probability, determination of probable effects, and definition of controls, which could minimize or eliminate the disruption.

Risk Management

Risk management balances the potential service disruption against the costs of reducing or eliminating vulnerability to provide effective coverage for services at a reasonable cost.

Definition of Controls

1.*Do nothing.* The risk may be so minute that the cost of response is disproportional to exposure.
2.*Improve security measures*. Tightening physical or logical security can reduce exposure and decrease costs associated with protection.
3.*Remove the exposure*. Out source the service or resource to a third party, or change a procedure to reduce exposure.
4.*Spread the exposure*. Perform critical functions at several locations to reduce the risk of total failure. On the other hand, the risk of partial failure will increase.
5.*Purchase redundant equipment*. Partial or complete redundancy of specific resources components is a relatively inexpensive way to reduce vulnerability to certain threats.
6.*Develop reciprocal agreements with other educational entities*. In reality, most agencies lack fully compatible environments and sufficient excess capacity for this option. Coordinated planning is essential for any reciprocal recovery agreement.
7.*Share a recovery center with other educational entities.* Shared resources reduce the costs for individual participants.
8.*Contract for backup services*. Subscribe to a commercial hot site service, which provides a facility configured to meet the critical processing requirements of the agency.

9.*Build a backup facility.* A backup facility for a single entity is both the most expensive and the most complete means of reducing risk.

STEP 6. ESTABLISH SYSTEM PRIORITIES

Automated applications should be reviewed in relation to risk. Critical applications are determined by ranking potential financial or operational loss if an application were unavailable. Securing of financial and student data is 'critical'. System priorities should be classified; for example:

- Class 1- Must be run on schedule
- Class 2- Run as resources become available
- Class 3- Can be delayed

Class 1 systems should be ranked from most critical to least critical, repeating the process for other applications. A resumption plan requires recovery operations to immediately restore all Class 1 systems. Class 2 systems and Class 3 systems should resume operations, in order, as full recovery is achieved. *See Appendices D and E.*

STEP 7. ANALYZE AND DEFINE REQUIREMENTS FOR RECOVERY

Alternate processing needs range from full redundancy to the capability for interim processing of critical systems for one or two days. Service resumption may encompass: inventory, hardware, system software, communications, back-up data, physical facilities, vendor support, interagency support, staff, applications software, security, office equipment, logistics, storage, funding, and acquisitions. *See Appendix F.*

STEP 8. DESIGN THE PROGRAM FOR RECOVERY OPERATIONS

Canutillo ISD recognizes that process planning and training personnel will significantly reduce the cost and time necessary to achieve full recovery and resume normal service operations.

MANAGEMENT AND ORGANIZATIONAL ASSIGNMENTS

A full-scale recovery requires distribution of responsibilities. *Appendix G outlines Management Issues. Appendix H lists possible teams and representative responsibilities.*

RECOVERY PROCEDURES

Staff safety comes first. Emergency supplies and materials are made available *(refer to Appendix I).*

THE RECOVERY PROCESS

When a disruption occurs, the level and extent of the disruption must be immediately determined and appropriate steps taken to safeguard lives and prevent further destruction or escalation of the problem. When the condition is stabilized, a preliminary damage assessment is conducted and the situation evaluated. Management is informed and a decision to activate a Command Center and assemble the Recovery Teams for briefing. Once the damage report has been completed, specific assessments will be made. The Director of Technology will initiate recovery processes appropriate to the level of disaster experienced. In a full or partial recovery operation, the objective is to return to normal operation at the earliest possible time.

STEP 9. CONDUCT DATA BACK-UP AND RESUMPTION TRAINING

Cross-training program and refresher training for key personnel will be conducted as changes occur in the ISR Team or Technology Department.

Proposed Training Class Audience

First Aid Training, All personnel
Safety Training, All personnel
Security Procedures, ISR Team
Overview of Information Service Resumption Plan, ISR Team

STEP 10. TEST INFORMATION SERVICE RESUMPTION PLAN

The critical role of testing to achieve successful planning cannot be overemphasized. Information Service Resumption Plans will be tested regularly using a fully developed scenario of a simulated disruption. Tests should be carefully planned to minimize disruption of normal operations. Plans should be tested in phases. Management will approve and monitor each test to understand planned procedures and to detect and correct shortcomings and/or problems by updating the plan. The various testing approaches include: structured walk-throughs; checklists; simulations; parallel testing; and full-interruption testing.

Some areas to test include, but are not limited to:

- Data backup
- Documentation backup
- Facilities backup
- Critical applications (first singly, then in groups)
- Response during different processing periods and shifts

Impartial observers with specific areas of concern should monitor and evaluate the effectiveness of the test. Planning and conducting test exercises should be the joint responsibility of the Director of Technology and ISR Team members. After each test exercise, results should be thoroughly reviewed for flaws, omissions, and overlaps in the recovery procedures. The plan and/or procedures should be updated based on this analysis. *Appendix J* illustrates a Test Evaluation format and procedure.

STEP 11. UPDATING INFORMATION SERVICE RESUMPTION PLAN

Ongoing changes in systems, software, applications, communications and operations will create many of the changes and up-dates to the plan. Incorporating new information such as:

- organizational and staffing changes
- LAN/WAN/PAN/MAN/VPN infrastructure changes
- safety requirements
- applications
- configuration changes
- vendor agreements
- changes in state resources obtained from other organizations

Iterative reviews of the guide's sections, areas of responsibility, and frequency:

Section	*Responsibility*	*Frequency*
General	Director of Technology	Annually
Data Back-up	Comptroller and Technology Coordinator	Quarterly
Implementation	Director of Technology	Annually
Critical Applications	Users	As Needed
ISR Team Procedures	Team Members	Annually

3.0 RESOURCES

Position	*Department*
Assistant Superintendent of Facilities and Support Services	Administration
Comptroller	Finance
Director of Technology	Technology
Public Relations Officer	Public Relations
Technology Coordinator	Technology
Network Engineer	Technology
PEIMS Coordinator	Finance

A. Offsite Media Storage

CISD has media records storage offsite. Information technology backup of media has been developed for various types of records, with a rotation schedule daily, weekly, monthly, and annual schedules. Canutillo ISD permits the use of most types of storage containers for digital media. The container type to be used must be approved by Canutillo ISD Technology Department before they are used. Storage containers must be labeled.

B. Training

Canutillo ISD provides classes throughout the school year on records management issues, some of which address backup and recovery of media records.

4.0 APPENDICES

APPENDIX A - GLOSSARY OF TERMS

Application System - A series of automated processes in full production and serving the needs of some part or all of an agency.
Back-up - An alternate source or resource to be used in the event the primary resource is no longer available for use.
Catastrophic Disaster - A disaster in which the damage sustained is sufficiently severe as to render the data processing activity incapable of providing support to the agency; and the condition is anticipated to last for an indefinite period of time.
Class 1 Systems - A classification of operational application systems deemed essential in performing the agency mission and must be processed during information back up and contingency planning.
Class 2 Systems - A classification of operational application systems deemed necessary but not essential in performing the agency mission. During information back up and contingency planning these systems must be processed after all processing of Class 1 systems.
Class 3 Systems - A classification of operational application systems for which delayed processing is acceptable.
Command Center - A temporary location with communication equipment from which initial recovery efforts are manned and media-business communication is maintained.
Controls - Mechanisms implemented to limit exposure, such as card key systems and security software packages.
Critical Application - The prioritization of Class 1 operational application systems, which are classified by the agency as being essential in performing the agency mission.
Disaster - An occurrence that impacts the data processing to the extent that the capability to perform normal and routine operations is impaired.
Enterprise-level – Includes having dual power supplies, multiple disk controllers, multiple physical disk, and disk partitions, and have at a minimum 99.99 percent uptime. Operating System and Server software must be industry supported and accepted, and must have 24x7x365 vendor maintenance and support.
Halon - A gas used to extinguish fires effective only in closed areas.
Localized interruption - An outage caused by fire, sabotage or other isolated even affecting a single building or data center.
Mutual aid agreement - An expansion of a reciprocal agreement whereby several organizations agree to share computing resources with the member that suffers service disruption.
Parallel testing - Historical (e.g., yesterday's) transactions are processed against the preceding day's backup files at the backup site to test agreement with transactions produced under normal operations. Parallel testing can be performed in conjunction with checklist testing.
Shell Facility - A facility, which can be made available for use as a data processing facility in a relatively short period of time with a minimum, cost.
Simulation Testing - A disaster is simulated so normal operations will not be interrupted. Hardware, software, personnel, communications, procedures, supplies and forms, documentation, transportation, utilities, and alternate site processing should be thoroughly tested in a simulation test. Extensive travel, moving equipment, and eliminating voice or data communications may not be practical or economically feasible during a simulated test.
Threat - A potential action, which could occur to a data processing activity causing serious to catastrophic results.
User - An organization within the agency, which is a customer of data processing, services.

APPENDIX B - CAPABILITY ASSESSMENT

___ Location:
- not advertised
- not readily accessible by general public
- away from high traffic areas or glass enclosures
- close to emergency response units (e.g., Fire Dept.)
- separate from user location

___ Video monitor used to scan entrances/exits
___ Security Guards or receptionists at entrances
___ Photo-badges used
___ Sign-in log at entrances
___ Visitors and/or Vendors required to wear identification badges
___ Entrance security devices requiring keys and pass-codes
___ Controlled access to MC and IC areas during working hours at Campus and District Level
___ Controlled access to MC and IC areas during off-shift hours at Campus and District Level
___ Limit access to Main Communication (MC) and Intermediate Communication (IC) to Technology Department and Finance Department employees as needed
___ Control physical access to all data libraries
___ Security awareness training program for employees
___ Published security policy/procedures
___ Require positive identification of vendor personnel
___ Vendor service personnel supervised while on premises
___ Age of infrastructure
___ Collect keys and badges and/or change passwords when employees leave employment

FLOOD CONTROL

___ Equipment located away from water pipes
___ Adequate water drainage and controls:
- under raised floor, if possible
- on floors above
- in adjacent areas

___ Inform employees of location of water pipe shut-off valves
___ Age of water mains
___ Equipment located away from sprinkler heads
___ Equipment located away from restrooms, cafeterias, etc.
___ Sealed windows

HOUSEKEEPING

___ Flammable materials properly stored
___ Paper, supplies and trash stored outside computer area
___ No asbestos on utility steam pipes

FIRE CONTROL

___ Fire resistant/noncombustible materials used for:
- buildings
- classrooms
- partitions, walls, doors
- furnishings

___ Solid walls constructed to extend to the true ceiling of each floor
___ Smoke or heat detectors installed, including above ceiling and below floors
___ A/C facilities automatically deactivated by smoke detectors

___ Smoke detector system tested periodically
___ Automatic carbon dioxide/water/HALON fire extinguishers
___ Fire extinguishers easily accessible, with type and use identified
___ Fire extinguishers inspected and tested regularly
___ Established current emergency fire procedures and evacuation plan
___ Conduct fire drills
___ Post fire department's phone number on/near each phone
___ Close liaison established with the local fire department
___ Training for all employees in fire prevention
___ Alarm pull-boxes installed
___ No-Smoking policy in school district facilities
___ Emergency power switches located at exits
___ Air conditioning system tied to emergency power switches
___ Fire alarms tested every 12 months
___ Emergency exit diagrams posted near all exits
___ Regular fire prevention inspections
___ Fire exits clearly identified and kept open
___ Multiple alarm zones
___ Audible and visible alarms

ELECTRICAL POWER

___ Reliable electrical power
___ Power supply monitored and recorded
___ Master power shutdown controls for computer
___ Backup power available
___ Emergency power available for gradual power-down
___ Emergency lights installed and working

CLIMATE CONTROL

___ Separate system for the computer facility
___ System protected from accidental and/or intentional shut-down
___ Controlled humidity
___ Backup air-conditioning facilities available
___ Air conditioning shut-off readily accessible
___ Air conditioning filtration
___ Preventive maintenance schedule observed

PERSONNEL CONSIDERATIONS

___ Employee background checks performed
___ Controls established for departing employees
___ Personnel policies and procedures available:

- Drug and alcohol abuse
- Security breaches
- Cross-training
- Vacations
- Acceptable Use Policy
- Record keeping and Storage

HARDWARE CONSIDERATIONS

___ Operations compared to scheduled activities
___ Meter hours compared to reported use
___ All periods of reported downtime verified
___ Incoming work checked against an authorized user list

___ Output spot-checked for possible misuse
___ Output distribution lists updated periodically
___ Digital media cleaned at regular intervals
___ Digital media utilization records maintained
___ Magnetic detection equipment used
___ Printers located in separate room (financial and student systems only)
___ Darkroom or "lights-out" operation
___ Preventive maintenance schedule observed

SOFTWARE CONSIDERATIONS

___ All software and documentation secured
___ Backup files stored off-site regularly
___ Restricted access to operating software
___ Restricted access to production software
___ Access to systems software limited by terminal address
___ Multilevel access to files controlled by:
- levels of security
- breakdowns within files
- restrictions read-only, write-only

___ Security software and access codes validated
___ Monitor log maintained of access to sensitive data files
___ Monitor unauthorized attempts to sensitive data files
___ Passwords used to identify network and terminal users
___ Passwords changed frequently
___ Operating system security bypass protection built-in
___ Operating system change control and tests following maintenance, program load, etc.
___ Restart/recovery procedures for application programs
___ Program change documentation and control
___ Operating system software backed-up before system changes

FILE CONSIDERATIONS

___ Duplicate program files stored off-site
___ Program files in fire-resistant containers
___ Maintain current inventory of program files
___ Programming change controls to use duplicate rather than the original program file
___ Record any items removed from files
___ Duplicate copies of documentation maintained
___ Copies of documentation stored off-site
___ Fire-resistant storage used for documentation
___ Duplicate documentation verified periodically
___ Data files physically controlled by computer center personnel rather than by user
___ Data files classified by degree of sensitivity
___ Duplicate data files fire protected and stored outside the computer room

RESOURCE SHARING CONSIDERATIONS

___ Remote terminal access limited to specific individuals
___ Remote terminal access controlled by:
- locked doors
- password protection

___ Password identification of terminals/users
___ Passwords controlled by requiring frequent changes
___ Limited number of invalid access attempts

___ Restricted access to password file
___ Users restricted to specific files
___ Control authorization to add, delete or modify files
___ Software record of all activity against data files
___ Software protection for on-line operating systems and applications programs
___ Security override procedures classified at highest level
___ Use of overrides monitored
___ Debugging of security system monitored

COMMUNICATIONS CONSIDERATIONS

___ All communications lines backed up
___ Dual paths to processor for all communications lines
___ Alternate path to backup for all communications lines
___ System use log verified periodically
___ Network control function password protected
___ Access to the network control center restricted
___ Configure and change management system access from anywhere in the network
___ Network failure detection equipment in use
___ Communications failure troubleshoot/correction procedures
___ Network troubleshooting procedures updated regularly
___ Vendor list for trouble calls available
___ Vendor list regularly updated
___ Multiple carrier connections
___ Switchable network topology based on intelligence embedded into carrier backbone networks
___ Records of cabling plan offsite
___ Critical network circuits tagged
___ Offsite records to restore voice/data/video communication systems

DATA ENTRY

___ Data secure to data entry/CD/DVD
___ Input data backed-up at an alternate location
___ Data validated going to data entry/CD/DVD
___ Equipment access secured
___ Output validated against input
___ Output backed-up at an alternate location
___ Back-up equipment available at an alternate site

INFORMATION BACK-UP AND CONTINGENCY PLANNING

___ Formal written information back up and resumption plan
___ Plan training
___ Back-up computer(s) available
___ Information Back-Up and Contingency Plan tested yearly

NETWORK AS PLACED DRAWINGS

___ Equipment/network configurations documented/standardized
___ Equipment and/or network configurations stored offsite
___ Standard back-up procedures
___ Offsite storage of data, software, and documentation
___ Availability of spare hardware/software [HOT SWAPS]

APPENDIX C - EXAMPLES OF POTENTIAL RISKS

- Air Conditioning Failure
- Bomb
- Civil Disturbance
- Communications (voice/data/video) Interruption
- Data Unavailable
- Disgruntled Employee
- Electrical Failure
- Employee Error
- Equipment Malfunction
- Facility Structural Failure
- Fire
- Flood
- Postal Strike
- Sabotage
- Software Error
- SPAMMING
- State or Federal Funds Unavailable
- Strike
- High Level Winds
- Utility Outage

APPENDIX D- PRIORITY APPLICATION RECORD

System Identification and Title:

Classification: Critical/Class 1___ Class 2___ Class 3___

Key technical contact and telephone number:

Key User(s) Identification and use of data/reports:

Critical Period:

Maximum Allowable Processing Delay:

Processing Time Required:

Equipment Required (batch and online):

Software Required:

Location of back-up applications software:

Data Source and Medium:

Data Location:

Back-up data, frequency and location:

Special forms, back-up supply and location:

Documentation and instructions:

Location of back-up documentation:

Special Forms Required:

Location of Back-Up Forms:

Legal Requirements:

Key User:

Approval Date:

APPENDIX E- RISK EVALUATION

(List each operational application system)

APPLICATION SYSTEMS	IMPACT CODE	VALUE/HOUR

Risk Impact Code

1 - Catastrophic effect on public education, health, safety, welfare
2 - Major impact on normal operation
3 - Minor impact

APPENDIX F- ASSET INVENTORY

APPLICATION SYSTEMS	LOSS CODE
Computer Hardware	
Network Systems	
Logical/Physical Configuration Diagram	
Operating Systems Software	
Application Software	
Facilities	
Communications Equipment	
Data Files	
Documentation	
Supplies	
Office Equipment	

Impact of Loss Codes:

1 - Unable to deliver vital agency service
2 - Production schedule impacted
3 - Minor processing impact
4 - Unknown

APPENDIX G - MANAGEMENT ISSUES

Location or Site Information

- Multiple hot site locations
- Multiple locations networked together
- Availability of mobile recovery services and normal length of set-up time

Configuration Information

- By manufacturer, model/series number, and size/quantity
- Processors Types
- Operating systems software
- Back-Up units (gigabyte), tape drives, CDs
- Front end processors
- Printers
- Any critical unusual equipment
- Telecommunications Terminals
- Telecommunications systems (Fiber, T1, satellite, microwave, or dial-up); network availability 24 hours a day, 7 days a week
- Voice communications options: (number of incoming and outgoing lines)
- Secured Telephone Lines

Other Information

- Levels of physical security access
- Internal fire protection
- Petty cash for staff
- Available inventory of scratch tapes/cartridges and quantity
- Familiarity with recovery plans for local utilities (electric, water, gas, and voice communications)
- Provision of administrative supplies (pens, paper, staplers, scotch tape, etc.)

APPENDIX H- RECOVERY ORGANIZATION AND RESPONSIBILITY ASSIGNMENTS

Director of Technology

Responsible for directing, coordinating, and reporting to management until full recovery has been accomplished.

Recovery Command Center

The Board Room will serve as the Recovery Command Center with phone lines, status boards, conference equipment, etc. to function as information and operations center for an extended period of time.

Damage Assessment Team

A technical group made up of the Assistant Superintendent of Facilities and Support Services, Comptroller, Director of Technology, Campus Administrators, Technology Coordinator, Network Engineer, District Technicians will be responsible for assessing damage to a facility and its components:

- Identify extent of damage to the facility.
- Determine condition of equipment.
- Identify software problems.
- Define data problems.
- Identify data communications problems.
- Describe salvageability of supplies.
- Assess operational capability.
- Define restoration requirements.
- Schedule salvage and restoration.
- Monitor salvage and restoration operation.
- Provide a detailed accounting of damages for insurance claims, if applicable.
- Advise users of critical systems of the disruption and recovery production schedule.
- Provide programming and support services for alternate processing of critical systems.
- Help system users prepare for resumption of normal operations as recovery progresses.
- Initiate emergency production schedule for critical applications systems.
- Coordinate input/output from recovery facility.
- Receive backup versions of appropriate software.
- Advise Recovery Command Center of status and progress.

Communications Team

- District Technology Technicians are responsible for restoring voice, data, and video communications links between users and servers/computers, regardless of location.
- Assist in damage assessment.
- Coordinate restoration of service with vendors.
- Test data communications operation.
- Establish data communications for critical applications.
- Identify equipment and software requirements.
- Provide necessary telephone service.
- Monitor restoration of normal communication operation.
- Advise Recovery Command Center of status and progress.

Procurement Team

Persons knowledgeable of the information resources and supplies inventory and the budgetary, funding, and acquisition processes responsible for expediting acquisition of necessary resources:

- Assist Damage Assessment Team in determining equipment, software, facility, and other components beyond repair and in determining additional equipment or supplies required at the back-up site for expediting the recovery process.
- Coordinate identification of purchases.
- Contact vendors to procure necessary equipment, software and supplies.
- Monitor acquisition and delivery of purchases.
- Advise Recovery Command Center of status and progress.

Facilities Team

Technology Department personnel will arrange the primary and back-up facilities and all components:

- Assist the Damage Assessment Team in identifying specific damage to the facility.
- Reference floor plan documentation for required dimensions and environmentals.
- Identify repair or replacement requirements.
- Prepare back-up site for occupation and operation.
- Advise Recovery Command Center of status and progress.

Internal Audit Team

Finance Department and Technology Department personnel are responsible for observation and oversight participation in the recovery effort:

- Review the existence of sufficient control to assure reliability and consistency of financial records.
- Observe implementation of necessary supervision and controls during recovery.
- Review logs of recovery activities.
- Advise Recovery Command Center of status and progress.

Public Information Office

Responsible for disseminating information concerning the emergency or event requiring the recovery effort.

- Have a single spokesperson accessible to employees and external forces.
- Provide accurate, essential, and timely information to combat spread of rumors and adverse publicity.

APPENDIX I- EMERGENCY SUPPLIES & MATERIALS

___Batteries
___Beepers/Pagers
___Blankets
___Buckets
___Bull Horn
___Cash and/or Credit Cards
___Cellular Phones
___Crow Bar
___Drinking Water
___Emergency Lighting
___Emergency Radio Network with Remote Suitcase Repeaters
___First aid kits
___Flash Lights
___Food
___Gasoline Generator
___Hand Held Tape Recorders and Tapes
___Hard Hats
___Laptop PC with Printer
___Lumber/Plywood
___Minimum Processing Schedules
___ PDAs/Pocket PCs
___Plastic Sheeting
___Portable Rest rooms
___Press Information
___Radio
___Rain Gear
___Spare Cable
___Spare Controllers & Terminals
___Special Forms (one-month supply suggested)
___Tables and Chairs
___Tablet PCs
___Telephone Lists
___Tents
___Tools
___Walkie Talkies
___Writing Materials

APPENDIX J- TESTING ISSUES

Evaluation of Test Results

It is essential to quantitatively measure the test results, including: elapsed time to perform various activities, accuracy of each activity, and amount of work completed. Pre-formatted forms can be useful to document and evaluate test results.

- *Disaster Recovery Hour* - the estimated time to perform the action or procedure
- *Plan Cross Reference* - cross-reference to the specific section of the plan that is to be tested
- *Action Number* - sequential number assigned to each action or procedure
- *Action* - description of the action or procedure to be performed during the test
- *Sequential or Parallel Notation* - certain actions or procedures need to be performed sequentially and others can be performed concurrently or in parallel
- *Responsibility* - Person(s) assigned specific responsibility for performing the testing action or procedure
- *Actual Time* - Actual time required to perform the specific action or procedure
- *Successful/Unsuccessful Notation* - description of result
- *Comments* - further description of the evaluation of the test results

Sample Scenario

Assume that all external data communications have been lost during a holiday for an indeterminate length of time, which would trigger the initiation of the Data Back-Up and Resumption Plan. Notification of management would be followed by assembly of the appropriate teams, an assessment of the damage and initiation of the recovery process. The scenario could proceed into running one or more critical application systems from the backed-up data at the alternate site or could be terminated at the option of management. This test would validate the recall list of key management and team personnel, the effectiveness of back-up data and files associated with the processing of Class 1 systems at the alternate facility and the effectiveness of the alternate communications system.