

River Road ISD

Information Technology Disaster Recovery Plan

INTRODUCTION

Over the years, dependence upon the use of computers in the day-to-day business activities of many organizations has become the norm. River Road ISD certainly is no exception to this trend. Vital functions of the district depend on the availability of computers. Consider for a moment the impact of a disaster that prevents the use of the system to process student registration, payroll, accounting, or any other vital application. Students and faculty rely upon our systems for instruction and research purposes, all of which are important to the well-being of our district. It is hard to estimate the damage that such an event might cause. Without adequate planning and preparation to deal with a disaster scenario, the district's central computer systems could be unavailable and vital data could be lost.

OVERVIEW of the Plan

Personnel

Immediately following the disaster, a planned sequence of events begins. Key personnel are notified to implement the plan. In a disaster it must be remembered that PEOPLE are your most valuable resource. The recovery personnel working to restore the critical systems will likely be working at great personal sacrifice, especially in the early hours and days following the disaster. They may have injuries hampering their physical abilities. The loss or injury of a loved one or coworker may affect their emotional ability. They will have physical needs for food, shelter, and sleep. The district must take special pains to ensure that the recovery workers are provided with resources to meet their physical and emotional needs.

Salvage Operations at Disaster Site

Early efforts are targeted at protecting and preserving the computer equipment. In particular, any magnetic storage media (hard drives, magnetic tapes, diskettes) are identified and either protected from the elements or removed to a clean, dry environment away from the disaster site.

Designate Alternate Site

At the same time, a survey of the disaster scene is done by appropriate personnel to estimate the amount of time required to put the facility (in this case, the building and utilities) back into working order. A decision is then made whether to use the alternate site, a location where computing and networking capabilities can be temporarily restored until the primary site is ready. Work begins almost immediately at repairing or rebuilding the primary site. This may take months, the details of which are beyond the scope of this document.

Purchase New Equipment

The recovery process relies heavily upon vendors to quickly provide replacements for the resources that cannot be salvaged.

Begin Reassembly at the Alternate Site

Salvaged and new components are reassembled at the alternate site according to the instructions contained in this plan. Since all plans of this type are subject to the inherent changes that occur in the computer industry, it may become necessary for recovery personnel to deviate from the plan, especially if the plan has not been kept up-to-date. If vendors cannot provide a certain piece of equipment on a timely basis, it may be necessary for the recovery personnel to make last-minute substitutions. After the equipment reassembly phase is complete, the work turns to concentrate on the data recovery procedures.

Restore Data from Backups

Data recovery relies entirely upon the use of backups stored in locations off-site from the district data center. Backups can take the form of magnetic tape, CDROMs, disk drives, and other storage media. Early data recovery efforts focus on restoring the operating system(s) for each server. Next, first line recovery of application and user data from the backup tapes is done. Individual application owners may need to be involved at this point.

Restore Applications Data

It is at this point that the disaster recovery plans for users and departments (e.g., the application owners) must merge with the completion of the IT Disaster Recovery Plan. Since some time may have elapsed between the time that the off-site backups were made and the time of the disaster,

application owners must have means for restoring each running application database to the point of the disaster. They must also take all new data collected since that point and input it into the application databases. Some applications may be available only to a limited few key personnel, while others may be available to anyone who can access the computer systems.

Move Back to Restored Permanent Facility

If the recovery process has taken place at the alternate site, physical restoration of the original site will have begun. When that facility is ready for occupancy, the systems assembled at the alternate site may be moved back to their permanent home. This plan does not attempt to address the logistics of this move, which should be vastly less complicated than the work done to do the recovery at the original site.

NOTE: The techniques for backup and recovery used in this plan do *NOT* guarantee zero data loss. River Road ISD is willing to assume the risk of data loss and do without computing for a period of time in a disaster situation. To put it in a more fiscal sense, the district is saving dollars in up-front disaster preparation costs, and then relying upon business interruption and recovery insurance to help restore computer operations after a disaster.

Data recovery efforts in this plan are targeted at getting the systems up and running with the last available off-site backup tapes. *Significant* effort will be required after the system operation is restored to (1) restore data integrity to the point of the disaster and (2) to synchronize that data with any new data collected from the point of the disaster forward.

This plan does not attempt to cover either of these two important aspects of data recovery.

Instead, individual users and departments will need to develop their own disaster recovery plans to cope with the unavailability of the computer systems during the restoration phase of this plan and to cope with potential data loss and synchronization problems.

Primary OBJECTIVES of the Plan

This disaster recovery plan has the following primary objectives:

1. Present an orderly course of action for restoring critical computing capability to River Road ISD.
2. Set criteria for making the decision to recover at an alternate site or repair the affected site.
3. Describe an organizational structure for carrying out the plan.
4. Provide information concerning personnel that will be required to carry out the plan and the computing expertise required.
5. Identify the equipment, floor plan, procedures, and other items necessary for the recovery.

1. PURPOSE

River Road ISD's IT Disaster Recovery plan establishes procedures to recover the Information Technology infrastructure following a disruption. The following objectives have been established for this plan:

1. Identify the activities, resources, and procedures needed to carry out River Road ISD's processing requirements during prolonged interruptions to normal operations.
2. Assign responsibilities to the designated Technology Department's personnel and provide guidance for recovering the Information Technology infrastructure during prolonged periods of interruption to normal operations.
3. Ensure coordination with other staff who will participate in the contingency planning strategies. Ensure coordination with external points of contact and vendors who will participate in the contingency planning strategies.
4. Maximize the effectiveness of contingency operations through an established plan that consists of the following phases:
 - a. **Notification/Activation phase** to detect and assess damage and to activate the plan
 - b. **Recovery phase** to restore temporary IT operations and recover damage done to the original system
 - c. **Reconstitution phase** to restore IT system processing capabilities to normal operations.

1.1 APPLICABILITY

The Disaster Recovery Plan applies to the functions, operations, and resources necessary to restore and resume River Road ISD's critical computer systems operations as installed at River Road High School, 101 W. Mobley, Amarillo, Texas 79108. The Disaster Recovery Plan applies to River Road ISD and all other persons associated with the District Technology Department.

1.2 PLANNING PRINCIPLES

Various scenarios were considered to form a basis for the plan, and multiple assumptions were made. The applicability of the plan is predicated on two key principles:

River Road ISD's critical computer systems operations as installed at River Road High School, 101 W. Mobley, Amarillo, Texas 79108 is inaccessible; therefore, River Road ISD is unable to perform critical processes for the district.

River Road ISD Administration Office has been chosen as the designated alternate operating facility, located at 9500 US Hwy 287-N, Amarillo, Texas 79108.

- River Road ISD will use the alternate site building and IT resources to recover critical systems functionality during an emergency situation that prevents access to the original facility.
- A designated computer system at the alternate site will be configured to begin processing critical systems information.
- The alternate site will be used to continue data recovery and processing throughout the period of disruption, until the return to normal operations.

1.3 ASSUMPTIONS

Based on these principles, the following assumptions were used when developing the IT Disaster Recovery Plan. The Information Technology Infrastructure is inoperable at the district data center and cannot be recovered within 48 hours.

- Key technology personnel have been identified and trained in their emergency response and recovery roles; they are available to activate the IT Disaster Recovery Plan.
- Preventive controls (e.g., environmental controls, waterproof tarps, sprinkler systems, fire extinguishers, and fire department assistance) are fully operational at the time of the disaster.
- Data center equipment, including components supporting critical systems, are connected to an uninterruptible power supply (UPS) that provides 30-45 minutes of electricity during a power failure.
- Current backups of the application software and data are intact and available at the offsite storage facility.
- The equipment, connections, and capabilities required to operate critical systems are available at the alternate site.
- Service agreements are maintained with hardware, software, and communications providers to support the emergency system recovery.

1.4 PLAN MAINTENANCE

Basic Maintenance

The plan will be routinely evaluated once each year. All portions of the plan will be reviewed by the District Technology Team. In addition the plan will be tested on a regular basis and any faults will be corrected. The Director of Technology has the responsibility of overseeing the individual documents and files and ensuring that they meet standards and consistent with the rest of the plan.

Change-Driven Maintenance

It is inevitable in the changing environment of the computer industry that this disaster recovery plan will become outdated and unusable unless someone keeps it up to date. Changes that will likely affect the plan fall into several categories:

- Hardware changes
- Software changes
- Facility changes
- Procedural changes
- Personnel changes

As changes occur in any of the areas mentioned above, the District Technology Team will determine if changes to the plan are necessary. Changes that affect the platform recovery portions of the plan will be made by the District Technology Team. After the changes have been made, they will incorporate the changes into the body of the plan and distribute as required

Changes Requiring Plan Maintenance

The following lists some of the types of changes that may require revisions to the disaster recovery plan. Any change that can potentially affect whether the plan can be used to successfully restore the operations of the department's computer and network systems should be reflected in the plan.

Hardware

- Additions, deletions, or upgrades to hardware platforms.

Software

- Additions, deletions, or upgrades to system software.
- Changes to system configuration.
- Changes to applications software affected by the plan.

Facilities

- Changes that affect the availability/usability of the Alternate Site location.
- Changes that affect the cooling or electrical requirements etc.

Personnel

- Changes to personnel identified by name in the plan
- Changes to organizational structure of the department.

Procedural

- Changes to off-site backup procedures, locations, etc.
- Changes to application backups.
- Changes to vendor lists maintained for acquisition and support purposes

2. CONCEPT OF OPERATIONS

2.1 SYSTEM DESCRIPTION AND ARCHITECTURE

Every system that River Road ISD operates is backed up regularly. The backup media for each of these systems is relocated to an off-site storage area where there is a high probability that the media will survive in the event a disaster strikes. Two off-site storage locations are used:

- River Road ISD Administration Office at 9500 US HWY 287-N, Amarillo, Texas 79108
- River Road Middle School located at 7600 Pavillard Drive Amarillo, Texas 79108

Three sets of backups exist at any one time. The most recent backups are stored on a SAN drive within the data center at River Road High School. The second most recent are stored on magnetic media at the River Road ISD Administration Office. And the oldest are stored on magnetic media at River Road Middle School.

When a new backup is written to magnetic media, the tapes are rotated through these sites. The new tapes go to the River Road ISD Administration Office. Its tapes go to River Road Middle School, and its tapes go back to the data center located within River Road High School. The tapes at the data center within River Road High School are retained for use with the next round of backups.

The procedures for making the backups for each individual computer system differ. In general, full file system level backups are taken on a weekly basis and incremental backups are taken on a daily basis. In some instances, there are additional application-level backups for a system that may be run on a daily basis. All critical systems are backed up with a Disk-to-Disk-to-Tape solution over the district network. In the event of network failure at off-site locations, tape backup will be used locally.

2.2 LINE OF SUCCESSION

The Information Technology Department sets forth an order of succession to ensure that decision-making authority for the IT Disaster Recovery Plan is uninterrupted. The Director of Technology, is responsible for ensuring the safety of personnel and the execution of procedures documented within this plan. If the Director of Technology is unable to function as the overall authority or chooses to delegate this responsibility to a successor, the Systems Administrator of Technology shall function as that authority. If the Systems Administrator of Technology is unable to function as the overall authority or chooses to delegate this responsibility to a successor, the District Technology Coordinator shall function as that authority.

2.3 RESPONSIBILITIES

The IT Disaster Recovery Plan establishes responsibilities for personnel in recovering critical systems operations. The District Technology Department is responsible for the recovery of critical system operations and all applications. Members of the department include personnel who are also responsible for the daily operations and maintenance of these systems.

3. NOTIFICATION AND ACTIVATION PHASE

This phase addresses the initial actions taken to detect and assess damage inflicted by a disruption to the Information Technology infrastructure.

NOTE: In an emergency, River Road ISD's top priority is to preserve the health and safety of its staff before proceeding to the Notification and Activation procedures.

Contact information for key personnel is located in Appendix A. The notification sequence is listed below:

- The first responder is to notify the Director of Technology. All known information must be relayed to the Director of Technology.
- The Director of Technology is to contact the Systems Administrator of Technology and inform them of the event. The Director of Technology is to instruct the Systems Administrator of Technology to begin assessment procedures.
- The Systems Administrator of Technology is to notify team members and direct them to complete the assessment procedures outlined below to determine the extent of damage and estimated recovery time. If damage assessment cannot be performed locally because of unsafe conditions, the Systems Administrator of Technology is to follow the outline below.

13.1 DAMAGE ASSESSMENT PROCEDURES:

This damage assessment is a preliminary one intended to establish the extent of damage to critical hardware and the facility that houses it. The primary goal is to determine where the recovery should take place and what hardware must be ordered immediately.

Team members should be liberal in their estimate of the time required to repair or replace a damaged resource. Take into consideration cases where one repair cannot begin until another step is completed. Estimates of repair time should include ordering, shipping, installation, and testing time. The equipment inventory list will be used to help assess the damage to equipment.

Equipment inventory will be separated into two groups. One group will be composed of items that are missing or destroyed. The second will be those that are considered salvageable. These "salvageable" items will have to be evaluated and repaired as necessary. Based on input from this process, the District Technology Team can begin the process of acquiring replacements.

With respect to the facility, evaluation of damage to the structure, electrical system, air conditioning, and building network should be conducted. If estimates from this process indicate that recovery at the original site will require more than 7 days, migration to the alternate site is recommended.

13.2 CRITERIA

The IT Disaster Recovery Plan is to be activated if one or more of the following criteria are met:

1. Any critical system(s) will be unavailable for more than 48 hours
2. Facility is damaged and will be unavailable for more than 24 hours
3. Other criteria, as appropriate.

If the plan is to be activated, the Director of Technology is to notify all team members and inform them of the details of the event and if relocation is required.

Team members are to be informed of all applicable information and prepared to respond and relocate if necessary.

The Director of Technology is to notify the District Technology Coordinator that a contingency event has been declared and the backup media must be retrieved from the off-site storage facility (as determined by damage assessment).

The Director of Technology is to notify the Alternate site that a contingency event has been declared and to prepare the facility.

The Director of Technology is to notify remaining personnel (via notification procedures) on the general status of the incident.

4. RECOVERY OPERATIONS

This section provides procedures for recovering the application at the alternate site, whereas other efforts are directed to repair damage to the original system and capabilities. The following procedures are for recovering the critical systems at the alternate site. Procedures are outlined below. Each procedure should be executed in the sequence it is presented to maintain efficient operations.

4.1 PLATFORM RECOVERY PROCEDURES

This portion of the plan documents the recovery procedures for each of the critical systems to be restored at the recovery facility. This procedure documents the list of equipment necessary to restore service, power and cooling requirements, cabling and networking requirements, operating system and data restoration procedures, and procedures for placing the system into final form for general use.

1. Procure new equipment.
2. Verify that the correct power and data connectivity is in place (one 20A/120V power feed, network connectivity, air conditioning, rack or table space, cables, etc).
3. Connect the new system.
4. Complete any vendor-prescribed pre-installation diagnostics.
5. Install operating system.
6. As soon as possible, re-evaluate desirability of backups. It should be possible to proceed with normal operations at this point.
7. Restore system data if necessary.

4.2 CRITICAL APPLICATIONS RECOVERY PROCEDURES

The district has identified the following applications as critical applications. This means that delaying the processing of these applications could cause much hardship on faculty, staff, students, and others that depend on it.

1. The Finance and Payroll systems are currently being housed on the same server and utilize the same database. These systems are backed up nightly. The server is set up as RAID level 1 + 0 and therefore if drive failure were to occur, the redundant drive would be used until the failed drive were replaced. After platform recovery the following steps will take place:
 - a. Installation of Finance and Payroll software.
 - b. Database restoration and configuration (if required).
 - c. Installation of end user client software (if required).
2. The Student Management System is currently housed on two separate servers; a database server and a reporting server. These servers are backed up nightly. Both servers is set up as RAID level 1 + 0 and therefore if drive failure were to occur, the redundant drive would be used until the failed drive were replaced. After platform recovery the following steps will take place:
 - a. Installation of Student management software.
 - b. Database restoration and configuration (if required).
 - c. Installation of end user client software (if required).
3. The Special Education System is currently housed on a dedicated server. This server is backed up nightly. This server is set up with RAID level 5 and therefore if drive failure were to occur, a spare parity drive would take over until the failed drive was replaced. After platform recovery the following steps will take place:
 - a. Installation of Special Education software.
 - b. Database restoration and configuration (if required).
 - c. Setup Terminal Services in Application mode and reinstallation of Terminal Services Licensing (if required).

4.3 REMAINING APPLICATIONS

Once the platform system software and subsystems are operating correctly, the task of preparing the remaining applications can begin. Each platform will have a unique recovery road to follow. In some cases, there may be very little to do except for general testing. In other cases, considerable analysis and data synchronization work will likely be required. The District Technology Team will be responsible for carrying out this phase of the recovery. Each application area will require a review. This review should be conducted by an analyst familiar with the application while working closely with an application user representative. Items to be considered should include:

1. Review of the user department's IT Disaster Recovery Plan with special attention to any "interim" procedures that have been required in the time period since the disaster event occurred.
2. Review of the application documentation concerning file and database recovery.
3. Review the status of files and databases after the general platform recovery processing is complete.
4. Identify any changes to bring the application to a ready for production status.
5. Identify any areas where the application must be synchronized with other applications and coordinate with those application areas.
6. Identify and review application outputs to certify the application ready for production use.

5. RETURN TO NORMAL OPERATIONS

If the recovery process has taken place at the alternate site, physical restoration of the original site (or an alternate facility) will have begun. When that facility is ready for occupancy, the systems assembled at the alternate site may be moved back to their permanent home. This plan does not attempt to address the logistics of this move, which should be vastly less complicated than the work done to do the recovery at the alternate site.