

Appendix C

Plano ISD Data Disaster Recovery Plan

Definition of a disaster:

Webster defines a disaster as: a sudden calamitous event bringing great damage, loss, or destruction; *broadly*: a sudden or great misfortune or failure.

A disaster for the Plano ISD network is the total loss of all user data due to a server (or servers) hardware malfunction.

Disaster Prevention:

Anti-virus software is installed and operational on every server and computer workstation. This software protects from computer viruses all information written to the file servers and all information downloaded to the workstations from either floppy disks or the Internet. E-mail entering the district is also scanned for viruses and rejected if found to contain any.

Network users store critical data on file servers in home directories that are secure and backed up nightly. Additionally, the district file servers store the data using RAID5 technology. This technology spreads the data across multiple disk drives for redundancy and implements the most reliable method of disk storage available.

Effective backup procedures require more than simply performing daily on-site backups with tape cartridges, which is extremely unreliable, and therefore not used for data recovery in the event of a major disaster. The process of backing up servers is outsourced to a central hosted site, where backups are run each night for all district network server data. The district utilizes a fiber gig-e connection to the hosted site to accomplish this process.

The procedure for backup, media rotation, and data recovery of all district file server data is included below:

Media Backup, Rotation, and Recovery Procedures

Backups - the duplication of network data to separate media - are considered to be the best means of ensuring that data is not lost. Backups are crucial to the preservation of records and the continued operations of the district in the event of a disaster. The hosted service provider performs all server backups at an offsite location. Media management functions are the responsibility of the provider. This includes providing and changing tapes for backup purposes, off-site storage for tapes, verifying backups are run as scheduled, restoring data when requested, and troubleshooting errors when backup jobs do not run. The hosted service provider furnishes daily reports to district



network personnel detailing the status of each server backup. It is the responsibility of district networking personnel to oversee the complete backup process, including maintaining complete documentation of all servers requiring backups, and ensuring that the hosted service provider is notified immediately of any necessary changes. Backup software installed on district servers is the responsibility of district network engineers. District network personnel will work closely with the hosted service provider to troubleshoot errors, review status reports and restore user data.

The backup procedures allow for consistent backups and the ability to restore user data, application data, and system files. Since the procedures provide server level backups only, it is important that district network users understand that it is their responsibility to backup applications and data that reside on their local workstations.

Frequency of Backups and Retention

A full backup of each server is run weekly, and incremental backups (changed files only) are run daily between the weekly full backups. A full backup of each Netware server is scheduled between 8PM Friday and 5AM Monday. Each process includes backups of the data volume (VOL1 on Netware). A full backup of each NT/2000 server is scheduled each Tuesday through Friday morning between midnight and 7AM. The schedule for UNIX is slightly different. The library system that runs on the SUN platform runs from midnight to 3a.m. seven days a week. The SCO and Linux boxes (Prologix and Switchview) run from 2a.m – 5a.m. Monday through Friday and do not run on the weekends

If a full backup of a server fails to run at the scheduled time, a full backup of that server will be rescheduled each evening until the full backup is completed.

Once a full backup has succeeded, incremental backups will run each day until the end of the week.

Daily Backups:

Incremental backups with 3-week retention

Weekly Backups:

Full backups with 3-week retention

Monthly Backups:

Every 4th week, full and incremental backups with 1-year retention

Annual Backups:

The schedule is adjusted to fit the end of the school year by using a monthly backup as needed to obtain 1-year retention.

Annual full backups at all sites are run on the last business day that teachers and office staff work before going on summer break.



The procedure for backup, media rotation, and data recovery of the AS/400 server data (CIMS applications) is included below:

Daily backups:

- The backup up is run the following morning (e.g. work day 4-22-03 back up is run early morning on 4-23-03)
- The tape is saved for 7 days at the Resource Center (in a fire-proof, locked safe)
- The tape is sent to the OneSafe Place offsite storage facility and stored there
- The tape is returned 7-13 days later
- The tape is saved for 10 days at the Resource Center
- The tape is used again for another backup

Full backups:

- Full back ups are run on the weekend as close to the end of the month as possible
- The backup is stored at the resource center for 1 month
- The tapes are then sent to OneSafe Place and stored there for 1 month
- The returned tapes are saved for a year at the Resource Center

Special backups:

- PEIMS backups are made three times a year, one for each submission. One set is stored at OneSafe Place and one remains at the Resource Center. Both sets are retained for five years
- A fiscal year end backup is produced circa June 30 before year-end rollover begins. These tapes are retained for five years
- A calendar year-end backup is produced for December 31. These tapes are retained for five years



Novell's Directory Service (Security Database Backups)

Novell's database has been partitioned and replicated to ensure fast data retrieval and fault tolerance. Each replica has at least two copies. One of the copies is held on a server in a different physical location in the event of a disaster to all the servers at one site.

A tape backup of the data is run from the PL501CARS01 Novell server, which has higher order partitions of the entire District. This ensures that the entire directory is on tape. This backup conforms to the backup frequency required of data volumes.

E-Mail Backups

Primary and Secondary Domain Servers:

The most important database in the GroupWise system is the primary domain database (WPDOMAIN.DB). Because it stores the configuration information for the entire messaging system, it should be carefully guarded. A secondary domain database can always be rebuilt from the primary domain database. However, if the primary domain database is lost, the entire GroupWise system will be frozen. It is impossible to administer the GroupWise system without a working copy of the primary domain database.

Even though the secondary domain databases (WPDOMAIN.DB on MAIL02 and MAIL03) can be rebuilt from the primary domain database, the secondary domain databases should also be backed up as administrative changes occur.

Backups of all Domain servers are done as part of the regular backup schedule for all Netware servers.

Post Office Databases:

Post office databases contain the user's email messages, as well as attachments to those messages. Calendar data is also stored in the post office database. Structure checks and contents checks are run on the post office databases on a regular basis to ensure the integrity of the databases. All post office databases are backed up as part of the regular backup schedule for all Netware servers. Important: Since a user's email is dynamic and ever changing, an item that a user deletes and empties from their trash between backups may not be recoverable.



Maintenance of Tapes and Backup Equipment

It is important that problems with the backup media hardware, the media, or the backup jobs be identified in a timely manner. The district does not want to be put in the position of having to restore data, only to discover that the backups are defective, the job never ran, or the tape is either blank or contains old data.

Maintenance of all hardware and tapes relating to the backup process is the responsibility of the hosted service provider.

Media with 1-year retention are stored in a fire safe vault.

Verifying Backups

The Network Engineer for each region is responsible for verifying that all backups for servers included in his/her region are running successfully and completely by working closely with the hosted service provider.

Data Restoration

If a disaster occurs and the engineer in charge deems the server unrecoverable, then the disaster recovery plan will be implemented.

Disaster Recovery Plan

On Novell Netware:

Step 1:

Remove the current “bad” server from the network. This server should be turned off and removed from all power and network connections. This will ensure that it cannot come up as the server it will be replacing.

Step 2:

Obtain a new server to act as a replacement. With the original server being down, the engineer will go into the directory service and remove the server and all of its volumes out of the directory. The engineer will then ensure that the replica ring in which the server participated is up and running with a valid Master and other replicas - without the “bad” server participating.

Step 3:

Re-image the new server with a basic copy of the NetWare OS and partition the drives/volumes properly. Re-name the server to match the name it will be assuming and give it the same addresses (IPX/Internal Network number and TCP/IP). At this point, the engineer will place this server back into the tree into



the same location. The server should show up with the same volume names that were assigned.

Step 4:

Repair the directory service replicas and ensure that it is participating like the old server did. Once this has been verified, the engineer will install the backup agents back onto the server and inform the hosted service provider that the server is ready to restore VOL1. (the data volume). Upon completion of the correct data restoration, the engineer will install any other service that the server was running (virus detection/DHCP/Zenworks, etc...)

Step 5: The final step will be to shut the server down and restart it and verify it comes up properly.

On Microsoft Windows Server:

In the event of a disaster on a computer running the Microsoft Windows OS, some of the same steps will need to be initiated.

Step 1:

The first step in a restore procedure is to remove the current “bad” server from the network. This server should be turned off and removed from all power and network connections. This will ensure that it can’t ever come up as the server which will be replacing it.

Step 2:

Obtain a new server to act as a replacement. The engineer will place a copy of the Microsoft Windows OS at the same revision of the server that went down. The configuration of the drives should be the same or larger on the server replacing the bad unit. The backup software would need to be re-installed.

Step 3:

The engineer will notify the hosted service provider that the new server is in place and that the data needs to be re-installed. Since we back up the whole server for Windows, the engineer should just have to re-boot after the restore takes place and the server should be back up and functional.

On Unix hosts:

The current Unix hosts are under vendor support contracts. The TSS department works with the vendors on the restoration component. We would give approval on when and how the restore would take place from the vendor to the Unix host. It would be the sole support of the vendor who is providing the Unix hosted service to restore the OS back to a point where the restore could take place.



Plano Disaster Recovery Action Plan for CIMS applications

1. Prior to an actual disaster, it is the understanding of Prologic Technology Systems, Inc. that Plano Independent School District Resource Center is the sole responsible party to make readable backups on a daily basis. These backups will be made on IBM Magstar MP Fast Access C-format tapes provided by Plano Independent School District. It is also the understanding of Prologic Technology Systems, Inc. that Plano Independent School District has procured an off-site storage facility and has established an off-site storage procedure consisting of the following:
Monthly Archive tapes
Daily Backup tapes
System Save tapes
These tapes will be stored at One Safe Place storage facility located at 1550 W. Walnut Hill Lane, Irving, TX. 75038.
2. Testing will be done twice annually in June and December. Testing will consist of backup tapes being loaded and verifying that the data can be read on the iSeries 400, Model 820, O/S version 4.5 in the Corporate Office of Prologic Technology Systems, Inc. located at 2600 Via Fortuna, Suite 350, Austin, TX 78746.
3. Plano Independent School District has the following third party software that will need to be loaded in the event of a disaster:
FormSprint
Seagate Crystal
Mercator Trading Partner (Office Depot EDI)
PGP Personal Security (Used to send Plan and Compliance file)
eSchool Solutions SEMS (Substitute Employee Management System)
Client Access
SOQ (iSeries)
Visio
4. In the event of a disaster, Plano Independent School District will be required to give Prologic Technology Systems, Inc. an immediate oral notification that a disaster has occurred, as well as follow up with a written notification. It will then be Plano Independent School District's sole responsibility to overnight, courier or hand-deliver the most recent Monthly Archive tape, the most recent Daily Backup tape and the most recent System Save tape to Prologic Technology Systems, Inc. located at 2600 Via Fortuna, Suite 350, Austin, TX 78746. Upon reception of the tapes, Prologic Technology Systems, Inc. will have 24 hours to restore data and have the Plano Independent School District CIMS system available for use. In the event Prologic Technology Systems, Inc. has difficulty reading the backup tapes, a contingency plan has been devised to take Plano



Independent School District's tapes to the IBM Office in Austin and for a nominal fee, convert the tapes to a format Prologic Technology Systems, Inc. can read.

5. In the event of a disaster, Plano Independent School District will have alternate locations available to access their data. They are as follows:

Plano Independent School District Resource Center
2711 West 15th Street
Plano, TX 75075

GISD Technology - Computer Labs
410 Stadium Drive
Garland, TX 75040

Prologic Technology Systems, Inc. – Computer Lab
2600 Via Fortuna
Suite 350
Austin, TX 78746

6. Plano Independent School District will go to <http://www.mochasoft.dk> website to download the MochaSoft shareware for each remote user they want to give access to their data. At that time, we will give the connection information required to access their data residing on Prologic's iSeries 400.

