

Carteret County Schools Disaster Recovery Plan 2007-2008

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 Carteret County Schools network is the total loss of all user **data** due to a server or hardware malfunction.

Disaster Prevention:

Anti-virus/Spyware 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. (Firewall level).

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 all servers at all schools are run each night for all locations using USB drives.

The district utilizes a fiber or Ethernet connection to the host computer to accomplish this process.

The procedure for backup 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 folders on a USB drive - is 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 host/tech computer performs all server backups at that location. Media management functions are the responsibility of Technical Support Team . This includes the following:

Verifying backups are run as scheduled, restoring **data** when requested, and troubleshooting errors when backup jobs do not run.

It is the responsibility of district networking engineer to oversee the complete backup process, including maintaining complete documentation of all servers requiring backups, and ensuring that the host school is notified immediately of any necessary changes.

Backup software installed on district servers is the responsibility of district network engineer. District network engineer and technicians will work closely with all schools 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 their document folder or home directory that resides on the local server.

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 Windows 2003 server is scheduled each Monday through Friday between midnight and 7AM.

The library system (Destiny) runs from midnight to 3a.m. seven days a week.

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.

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.

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.

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 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 relating to the backup process is the responsibility of Technical Support Team.

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

Verifying Backups

The Network Engineer is responsible for verifying that all backups for servers are running successfully and completely.

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.
