

Boards are responsible for backing up child care data in the Child Care Service Delivery Application (CCSD). Back up and recovery procedures should be in writing and available for Board system administrators. The procedures used to create backup copies may differ based on the value of the data, how frequently the data is modified, the software used to back up data and other factors. Accidents, computer equipment malfunction or failure, and human error are the most common causes of data loss. In most cases, damaged or lost data cannot be restored at any cost. In any case, don't rely solely on a single copy of data stored on a file server, or any other media, if losing that data would disrupt service delivery.

There are a number of alternatives for storing backup data. For moderate numbers or sized files, ZIP disks or CDs are quite adequate. For users with very large amounts of data, other options, both hardware and specialized software are available on the market.

It is recommended that a full backup be done on a daily basis rather than depending on a differential backup which only creates a copy of all the files in a database that have been modified since the last database backup. A database backup creates a copy of the full backup and can be used to re-create the database as it was at the time the BACKUP statement completed.

Recommended Procedures

A Backup Procedure Policy

This should be revised on an annual basis, in order to incorporate the changes that may occur during the year and it will give the IT staff a more current version of the rules and regulations with respect to the backup process. The Board and child care contractor system administrator should be familiar with this policy.

Before deploying a new server, Network/System Administrators should:

- a) Perform the first backup of the data/information on the server;
- b) Confirm that a full restoration can be made from the first backup.

At minimum, Network/System Administrators should schedule backups as follows:

- a) Full Daily Backup – to be retained for a period of 1 week;
- b) Full Weekly Backup - to be retained for a period of 6 weeks;
- c) Full monthly backup 1st week - to be retained for a period of 16 weeks.

Network/System Administrators should ensure that backup logs are:

- a) Generated and record details of files backed up, files skipped, and tapes used;
- b) Retained for 14 days;
- c) Documentation will ensure that in an event of an emergency, appropriate personnel will have access to vital information. There are three main areas, which will need to be recorded and filed. Firstly, the employee log will be filed for a period of two weeks, at which time they

Minimum Child Care Service Delivery (CCSD) Application Backup Procedures for Board and Contractor System Administrators

12/3/2003

may be discarded. Secondly, spot-check reports will need to be in order to determine the pass or fail status of the backup/recovery test and/or any exceptions that should occur. Finally, an equipment status report should be prepared every month, in order to ensure that all equipment is functioning properly

Network/System Administrators should be aware that open files may be backed up or skipped depending on the type of lock applied to the file.

Network/System Administrators should ensure proper storage and tape management by:

- a) Storing weekly backup tapes off site;
- b) Rotating backup tapes;
- c) Destroying physically damaged or corrupt tapes;
- d) Managing the integrity of the physical tape device.

Network/System Administrators should:

- a) Verify that it is possible to restore files from backup tapes once a month;
- b) Verify that backup data from older backup files can be retrieved by scanning backup tapes; Verification of data should be conducted without fail in order to ensure that, at the most, only one day's worth of data would be lost.
- c) Ensure that the correct file protection and file ownership controls are present in the restored files.