



Donation Tracker (Back-up Practices)

by

Cascade Data Solutions

All backup routines must balance expense and effort against risk. That said, here are a couple of rules of thumb that should guide you in developing a backup strategy:

1) Develop a **written backup plan** that tells you:

- **What's being backed up?** - (In Donation Tracker you need to backup the "Data" folder; location varies depending on your network configuration, i.e. Local or Network Drive.)
- **Where it's being backed up to?** - (CD/RW, Zip Drive, Tape Drive, ETC.)
- **How often backups are occurring?** - (Hourly, Daily, Weekly, Monthly)
- **Who's in charge of performing backups?** - (Assign someone this responsibility, and familiarize yourself with the process.)
- **Who's in charge of monitoring whether backups are being performed successfully?** - (Assigning this task is a very important aspect; Responsibility and commitment!)

2) You should **back up your other documents (e.g. "My Documents" folders) and email files at least once a week**, and or some once per day. Each organization needs to decide how much work they're willing to risk losing, and set a frequency of backups accordingly.

3) You should **store a copy of your backups off-site** to insure against a site-specific disaster such as a fire, break-in, or flood. Ideally, you should store your backups in a safety deposit box, SAN (Storage Area Network), or a Fire Proof safe. Generally, we recommend rotating a set of backups off-site once per week.

4) It is **not usually necessary to back up the complete contents of each hard drive** -- most of that space is taken up by the operating system and program files, which can be easily reloaded from CD if necessary. The only exception is if your organization has a dedicated file server; it is a good practice to do a full backup of your server so that have a way to restore your Server's configurations users, computers & files The best practice in a Domain environment is to have all data put on the server, then back up the server at regular intervals.

5) **Test your backups BEFORE you need them.** You need confidence in your backups. Make sure your backup software has full read-back verification. Try restoring a few files.

Backing up your data regularly is vital insurance against a "data catastrophe." Unfortunately, this is a lesson that most people learn only from bitter experience. Developing a solid backup plan requires some investment of time and money, but the cost is far less than the often-impossible task of recreating data for which no backup exists!