# Backup Procedures

All computers need a backup plan. Every day, people and companies lose valuable personal information due to a hard disk crash, natural disaster, or other problem. Most modern operating systems include software, called a backup utility, capable of backing up and restoring data. A backup utility allows you to copy selected files or an entire hard disk to another storage medium.

Four types of backup typically are used: full, differential, incremental, or selective. A fifth type, continuous data protection, is used primarily by large enterprises. A full backup, sometimes called an archival backup, copies all of the files in the computer. A full backup provides the best protection against data loss because it copies all program and data files. Performing a full backup can be time-consuming. Users often combine full backups with differential and incremental backups. A differential backup copies only the files that have changed since the last full backup. An incremental backup copies only the files that have changed since the last full or last incremental backup. A selective backup, sometimes called a partial backup, allows the user to choose specific files to back up, regardless of whether or not the files have changed since the last incremental backup.

The main differences between a differential backup and an incremental backup is the number of backup files and the time required for backup. With a differential backup, you always have two backups: the full backup and the differential backup that contains all the changes since the last full backup.

With incremental backups, you have the full backup and one or more incremental backups. The first incremental backup contains changes since the last full backup. Each subsequent incremental backup contains changes only since the previous incremental backup. For files that contain many changes and are comprised of a large portion of the total data, incremental backup usually is fastest. If files contain only a few changes, differential backups may be appropriate. For the greatest flexibility or if backup space is limited, a selective backup allows you to choose specific files that you would like to back up.

The fifth type, continuous data protection (CDP), or continuous backup, is a backup plan in which all data is backed up whenever a change is made. Because CDP is costly, few organizations have implemented it, but its popularity is growing quickly as the cost for the technology falls. Backup procedures specify a regular plan of copying and storing important data and program files. Generally, users should perform a full backup at regular intervals, such as at the end of each week and at the end of the month. Between full backups, you can perform differential or incremental backups. This combination of full and differential or incremental backups provides an efficient way to protect data. Whatever backup procedures a company adopts, they should be stated clearly, documented in writing, and followed consistently.

# Disaster Recovery Plan

A disaster recovery plan is a written plan describing the steps a company would take to restore computer operations in the event of a disaster. Every company and each department or division within an enterprise usually has its own disaster recovery plan. A disaster recovery plan contains four major components: the emergency plan, the backup plan, the recovery plan, and the test plan.

## The Emergency Plan

An emergency plan specifies the steps to be taken immediately after a disaster strikes. The emergency plan usually is organized by type of disaster, such as fire, flood, or earthquake. Depending on the nature and extent of the disaster, the procedures that are followed in an emergency will differ. All emergency plans should contain the following information:

1. Names and telephone numbers of people and organizations to notify (e.g., management, fire department, police department)
2. Procedures to follow with the computer equipment (e.g., equipment shutdown, power shutoff, file removal)
3. Employee evacuation procedures
4. Return procedures; that is, who can reenter the facility and what actions they are to perform

## The Backup Plan

Once the procedures in the emergency plan have been executed, the next step is to follow the backup plan. The backup plan specifies how a company uses backup files and equipment to resume information processing. The backup plan should specify the location of an alternate computer facility in the event the company’s normal location is destroyed or unusable.

When operations are so important that a company cannot afford to lose the operations to a disaster, the company often maintains a hot site, which is a separate facility that mirrors the systems and operations of the critical site. The hot site always operates concurrently with the main site, so that if either site becomes unavailable, the other site continues to meet the company’s needs. The process of one system automatically taking the place of a failed system is called failover. A cold site is a site that mirrors the critical site, but does not become operational until the critical site becomes unavailable. When using a cold site, some time elapses between the disaster and when the cold site becomes functional.

The backup plan identifies these items.

1. The location of backup data, supplies, and equipment
2. The personnel responsible for gathering backup resources and transporting them to the alternate computer facility
3. A schedule indicating the order in which, and approximate time by which, each application should be up and running

For a backup plan to be successful, the company must back up all critical resources. Also, additional people, including possibly nonemployees, must be trained in the backup and recovery procedures because company personnel could be injured in a disaster.

The location of the alternate computer facility is important. It should be close enough to be convenient, yet not too close that a single disaster, such as an earthquake, could destroy both the main and alternate computer facilities. Some companies preinstall all the necessary hardware, software, and communications devices at the alternate computer facility. These facilities immediately are ready in the event of a disaster. In other cases, the alternate computer facility is simply an empty facility that can accommodate the necessary computer resources, if needed. One more alternative is to enter into a reciprocal backup relationship with another firm, where one firm provides space and sometimes equipment to the other in case of a disaster.

## The Recovery Plan

The recovery plan specifies the actions to be taken to restore full information processing operations. As with the emergency plan, the recovery plan differs for each type of disaster. To prepare for disaster recovery, a company should establish planning committees, with each one responsible for different forms of recovery. For example, one committee is in charge of hardware replacement. Another is responsible for software replacement.

## The Test Plan

To provide assurance that the disaster plan is complete, it should be tested. A disaster recovery test plan contains information for simulating various levels of disasters and recording an organization’s ability to recover. In a simulation, all personnel follow the steps in the disaster recovery plan. Any needed recovery actions that are not specified in the plan should be added. Although simulations can be scheduled, the best test of the plan is to simulate a disaster without advance notice.