Computer Systems Backup: Policy & Procedure

Introduction

Computers fail periodically. Vital records, systems and work products may be irretrievably lost if they have only been stored on the failed computer or computer system. The resulting frustrations, lack of productivity and cost of replicating this data can seriously harm education institutions. This computer system backup policy is designed to prevent such occurrences by having alternative locations for these systems and data, so the information and systems can be restored.

Policy: Computer Systems Backup

All computer systems maintained by the **{insert Government unit}** must be backed up on a regular schedule. These systems are typically servers but are not necessarily limited to servers. Servers expected to be backed up include the file server, the mail server, and the web server. The backup media will be stored in a secure off-site location. The off-site location can include "cloud" computer storage.

The purpose of the systems backup is to provide a means to: (1) restore the integrity of the computer systems in the event of a hardware/software failure or physical disaster, and (2) provide a measure of protection against human error or the inadvertent deletion of important files.

The systems backups will consist of regular (full) and incremental backups. (Depending upon the size, all backups may be full backups.) These systems backups are not intended to serve as the sole archival copy or to completely meet records retention requirements.

Staff members with computer files independent of the **{insert Government unit**} system are expected to perform periodic routine system and data backups, storing their backups in secure locations.

Procedures: Computer Systems Backup

The head of **{insert Government unit}** IT department is responsible for ensuring that this policy is carried out. Exceptions to the standard computer backup procedure are permitted when justified. All exceptions must be fully documented. The standard procedure for systems backup is as follows:

I. A full or incremental systems backup will be performed with sufficient frequency so that the entire system and all data from the end the prior day can be completely restored, if necessary. Each backup should be maintained for an entire month.

II. Data to be backed up include the following information:

1. User data stored on the hard drive.
2. System state data
3. The registry

Systems to be backed up include but are not limited to:

1. File server
2. Mail server
3. Production web server
4. Production database server
5. Domain controllers

III. The last full backup of the month will be saved as archival records.

IV. *Monthly backups* will be saved for one year, at which time the media will be recycled or destroyed.

V. *Incremental backups* of new data will be performed daily. Incremental backups will be retained for sufficient time to restore data for at least a week, at which time the media will be recycled or destroyed.

VI. Periodic tests of the backups will be performed to determine if files can be restored.

- The testing should be conducted quarterly
- The tests should be personally monitored by an auditor, and the auditor's report of their findings should be maintained for 5 years
- Testing should be conducted on clean servers, and all servers should be restored at the same time.
- Applications testing of the restored servers should be conducted and the results included in the auditor's report

VII. All backups will be stored in a secure, off-site location. Proper environment controls, temperature, humidity and fire protection, shall be maintained at the storage location.

VIII. All backup media that is not re-usable shall be thoroughly destroyed in an approved manner. Backup media that is used for other purposes shall be thoroughly erased.