

**Education Cabinet  
POLICY/PROCEDURE**

**Policy Number:** EDU-06

**Effective Date:** April 15, 2006

**Revision Date:** April 4, 2006

**Subject: Backup Procedures**

Tower and Server Farms

**Policy:** All information and data resources considered critical to the Cabinet operations shall have backup capabilities defined that will minimize the impact of their disruption or unavailability for whatever reason. Information backup execution is a responsibility of all groups within the Education Cabinet. The backup policy supports the resumption of data processing service necessary to ensure an acceptable level of operations can be maintained. It is prudent and required to anticipate and prepare for the loss of information processing capabilities. The plans and actions to recover from losses include backup of data and software in the preparation for catastrophic losses of information resources.

**Policy/Procedure Maintenance Responsibility:** The Chief Information Officer is responsible for the maintenance of this policy. The Information Security Management Committee is responsible for authorizing changes to the EDU Policy Procedures.

**Applicability:** All EDU employees and contractors shall adhere to the following policy.

**1.0 General**

The regular back up and storage off-site of all critical applications, software, documentation, and data files for all processing platforms are integral to disaster recovery. To minimize the possible disruption to business operations, which an incident resulting in loss of data could entail, EDU shall establish and maintain an effective schedule for the backup of critical data and application resources.

**2.0 Scope**

This policy applies to all EDU employees and contractors who use, process, or store computerized data relevant to agency business on an EDU maintained server or stand-alone workstation.

**3.0 Overview**

On-site backup is used to have current data readily available in machine-readable format in the production area in the event operational data is lost, damaged, or corrupted to avoid having to reenter the data from source material. Off-site storage embodies the same principle but is designed for longer-term protection in a more sterile environment. It requires less frequent updating, and provides an additional protection against threats potentially damaging to the primary site and data.

Data and software applications essential to the continued operation of critical department functions must be backed up. The security controls over the backed up resources must be as stringent as the protection required for the primary resources. Furthermore, as tapes are created that contain backed up information and/or applications, the tape will be assigned a generation number consisting of a date time group and tape drive or library designation from which the tape was created.

The backup procedures on the multi-user computer systems and departmental servers are designed to protect against data losses caused by hardware failures and other disasters. The frequency and timing of these backups may not provide sufficient protection to meet end-user requirements for data backup. Therefore, it is strongly recommended that end-users include a data backup step in their information processing procedures, and not to depend on a single backup procedure to provide all protection. To minimize the potential impact a contingency situation impacting the EDU building may have, critical backups must also be kept at off-site storage facilities and must be incorporated into EDU offsite storage rotation.

#### **4.0 Data Backup**

System backups protect the organization in the event of hardware failure, accidental deletions, and natural or man-made disasters. Similarly, backup files need to be created at appropriate intervals and themselves must be well protected from damage and destruction.

##### **4.1 EDU Backup Strategies:**

- Full Backup: backing up the entire hard drive or server.
- Selected backup: only backing up selected directories. This is useful and efficient if your work is concentrated in a specific area of your hard disk.
- Partial Backup: only backing up those files that have been changed since the last backup. It means using backup software to scan the files to see if they have been changed since the last backup cycle. If so, the file is saved; if not, the previous backup is maintained.

##### **4.2 EDU Backup Schedules:**

- Once daily: partial backup at end of the day for all altered files and software applications. This backup is stored to a tape and maintained within EDU in a fire proof safe. This backup should be run after normal work hours.
- Once a week: full backup of all software applications and files is copied onto tapes with tapes stored within EDU in a fire proof safe, it is recommended that a second set of tape/s be stored at a designated off site location if possible in case of a site disaster. This backup should be run over the weekend or other non-workday.
- Monthly: full backup (of entire system). This backup is recorded on tape/s with one stored within EDU in a fireproof safe it is recommended that a second set of tape/s be stored at a designated off site location if possible in case of a site disaster. This backup should be run over the weekend or other non-workday. Reinstalling a test directory will test the success of the backup.

### 4.3 Backup Requirements

- **Server Farm:** All critical servers will be backed up to the tape library. As a general rule, full backups will occur on the weekends and incremental backups will occur daily. All backups will be kept active for four (4) weeks. At the end of this period the media will be placed back into the scratch pool and will be available for reuse. If a different backup criterion is needed, the administrator of the server or critical applications residing on the server should inform the backup administrators so accommodations can be made. All tapes in the library will be rotated bi-weekly. Tapes not in the library will be placed in a fire proof safe. Catalog backups will alternate between disk and tape. A catalog backup will occur after each session of automated, manual, or user-directed backups. Status of backups will be checked daily. Media will be replaced and drives will be cleaned as required as indicated by the software or hardware.
- **Software:** Back up information, programs, and operating system utilities. Also maintain current copies of critical application software and documentation as securely as if they were sensitive data.
- **Files:** Do not compress files on the network drive since it can affect the reliability of the data being restored.
- **Schedules:** Schedule backups to run automatically by starting the back-up drive and backing up files automatically at set intervals with the ability to modify the schedule through operator intervention.
- **Responsibility:** Two personnel are responsible for all weekly and monthly backups of servers in the server farm.
- **Testing:** Verify that your backups are written to the disk or tape accurately.
- **Documentation:** Maintain a log of all backup dates, locations, and responsible personnel. Remember to store the logs securely.
- **Retention Policies:** Partial backup tapes generated on a daily basis will be maintained for a minimum of seven (7) calendar days. Full backup tapes generated on a weekly basis will be maintained for four (4) weeks. At the conclusion of the required storage period individual tapes will then be reused.
- **Storing Backup Media:** Until backup tapes designated for recommended off site storage can be removed from EDU they will be stored in a fireproof safe, at no time should anything other than backup tapes be stored in EDU's fireproof safe(s).
- **Tape Maintenance:** Clear hard drives, servers, and other storage media that contain old backup files to save space once you have properly secured (and verified) the last complete and partial backup.
- **Tape drive cleaning:** Clean the tape drive when the hardware or software indicates cleaning is required. The cleaning tape is an abrasive and over-cleaning will reduce life of the hardware.
- **Dispose of tapes** as outlined in policy EDU-08 and form EDU-F02 completed.
- **Restoration Order:** If a computer's files are lost, the last full backup is restored first. Then partial backups are restored in the order in which they were made.
- **Testing Backup:** If no restoration of files from user requests has occurred within thirty (30) days the backup system should be tested on a monthly basis by reinstalling test directory on existing machines or by installing a file/directory to an alternate location.

**Subject: Backup Procedures**  
Field Offices

**Policy:** Above policy applies.

**Policy/Procedure Maintenance Responsibility:** Above policy applies.

**Applicability:** All EDU employees and contractors shall adhere to the following policy.

**1.0 General:** Above policy applies.

**2.0 Scope:** Above policy applies.

**3.0 Overview:** Above policy applies.

**4.0 Data Backup:** Above policy applies.

**4.1 EDU Backup Strategies:** Above policy applies.

**4.2 EDU Backup Schedules:** Above policy applies.

**4.3 Backup Requirements:**

- **Field Office Servers:** Two people (one primary/one backup) in each office will be in charge of changing tapes daily. Local offices will supply new media tapes as needed. There should be 11 tapes: Monday through Friday for week one (1) and Monday through Friday for week two (2), as well one (1) cleaning tape. All tapes should be labeled with the day they are to be used (i.e. Monday one (1), Friday two (2)). All tapes should be stored in a safe place (preferably a fireproof safe) it is recommended that a second set of tape/s be stored at a designated off site location if possible in case of a site disaster.
- **Workstations.** Each user should use their best judgment regarding critical files to back up. There is generally no need to back up system files or application files, as these can be readily reinstalled. Critical data should be stored on the network drive. The data stored on the workstation (local computer drive) will be the responsibility of the user, Education Cabinet will have no liability in restoration of files in event of workstation hard drive failure.
- **Laptop/Remote Workstations.** Each user should use their best judgment regarding critical files to back up. There is generally no need to back up system files or application files, as these can be readily reinstalled. Critical data should be transferred to the network drive as soon as possible to prevent loss. The data stored on the workstation (local computer drive) will be the responsibility of the user, Education Cabinet will have no liability in restoration of files in event of workstation hard drive failure.

**Review Cycle:**  
Annually

**Timeline:**  
Revision Date: April 4, 2006  
Effective Date: April 15, 2006

**Enterprise Security and Policies**

**Cross Reference #** <http://gotsource.ky.gov/dsweb/Get/Document-21385/2010+-+Backup+and+Recovery+.doc>

**DTS Standards**

**Cross Reference #** [EDU-08](#), [EDU-F02](#)