

Administrative Polices and Procedures			
SUBJECT: Backup Policy			IS 13.31
Effective Date: February 2008	Revision Date:	Revision #:	Page 1 of 2
Authority: Town Manager		Information Systems Director:	
Revises Policy:			

I. PURPOSE

The Town of Jupiter requires that computer systems maintained by Information Systems be backed up periodically. The purpose of the systems backup is to: (1) provide disaster recovery services to restore the integrity of the computer systems 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. Although security backup files are public records according to Florida's Public Records laws, systems backups are not intended to serve as an archival copy or to meet records retention requirements.

Systems backups will be performed on a regular schedule as determined by the Information Technology Services Systems & Networks group. Backups will be stored in a secure off-site location based on the schedule listed below.

II. SCOPE

This policy applies to all equipment and data owned by the Town and maintained by Information Systems.

III. POLICY

This policy provides guidelines for establishing backup procedures. Exceptions to the standard procedure are permitted when justified. All exceptions must be fully documented.

IV. DEFINITIONS

- Archive: The saving of old or unused files onto magnetic tape or other offline mass storage media for the purpose of releasing on-line storage room.
- Backup: The saving of files onto magnetic tape or other offline mass storage media for the purpose of preventing loss of data in the event of equipment failure or destruction.
- Disaster: An occurrence resulting in hardware or system failures or a natural or man-made catastrophe.
- Restore: The process of bringing off line storage data back from the offline media and putting it on an online storage system such as a file server.

V. PROCEDURES

Standard Procedure

- A full systems backup will be performed weekly.
- The most current weekly backup will be moved to offsite storage when complete.
- Once a month, the last weekly backup prior to the current weekly backup will be moved to the bank vault.
- Differential backups will be performed daily. Differential backups will be retained for 4 weeks, at which time the media will be recycled or destroyed.
- Current weekly and once a month copy of weekly backups will be stored in secure, off-site locations
- Daily Differential and other backups will be stored in a fireproof container within the locked data center.
- 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.
- Periodic tests of the backups will be performed to determine if files can be restored.

Backup Media Disposition

The date each tape or other storage media is put into service shall be recorded on the tape. Magnetic media, i.e. tapes, that have been used longer than two years or evidence 3 or more hard errors shall be discarded and replaced with new tapes.

Testing

Restoration of data from backups shall be tested at least quarterly.

Restoration

Users needing files restored must submit a work order. Information about the file creation date, the name of the file, the last time it was changed, and the date and time it was deleted or destroyed should be included in the restoration request.

Media Storage Locations

On site media shall be stored in fire proof containers within the locked computer room facilities. Off site storage location shall be in a secured vault or other secure location. Proper environmental controls, temperature, humidity and fire protection, shall be maintained at the storage location

VI. RESPONSIBILITIES

The Network Administrator shall delegate a member of the Infrastructure or Deskside Support staff, as deemed appropriate for the system, to perform and monitor all backups for client/server systems. The Systems Analyst shall designate staff to perform and monitor all backups for midrange systems and any Application Services systems within their area of responsibility.

