POLICY 111.2	**Computerized Central Records System**	
	REVISED: 02/07, **09/11**	RELATED POLICIES:
	CFA STANDARDS: 34.13	REVIEWED: **09/11**

A. PURPOSE

The purpose of this policy is to establish procedures for a computerized central records system and guidelines for agency computer use. Computer hardware and software acquisition, implementation, and maintenance guidelines are necessary to maintain agency computer data integrity. All of the computer oriented tasks are the responsibility of and to be processed by the Police Department's Information Management Division.

B. POLICY

It is the policy of the Fort Lauderdale Police Department to maintain a system for the retention, archiving, and purging of electronic data which ensures and promotes compliance with generally accepted principles and other regulatory agency requirements. Members will adhere to the administrative and management control procedures outlined in this policy.

The Information Management Division is responsible for maintenance, control and retrieval of the Department's criminal and civil records. After being reviewed for accuracy and completeness, reports submitted from other bureaus are analyzed for statistical information necessary for both State and Federal Uniform Crime Reports (UCR).

It shall be the policy of the Fort Lauderdale Police Department to establish administrative and management, privacy, security and control procedures, within statutory guidelines, for the orderly maintenance, backup, retention, distribution, retrieval, release and destruction of documents in order to ensure records accountability.

C. PROCEDURES

1. INTERNAL ACCESS SECURITY

   a. All network access is restricted to User Name and Password access.

   b. When a member/employee is terminated, resigns or retires, the Personnel Manager or designee shall notify Information Management Division immediately in order to ensure that the User name/Password account is suspended. The account history is held in the event access is needed to the user's email or other files.

   c. Audit logs (of network access) are maintained and reviewed randomly.

d. Network files are backed up to a tape system; incremental back-ups are performed daily and a full system back-up is conducted once a week. The back-up tapes are stored in a secure, off-site location. Full system back-up tapes are retained for one (1) month.

e. Members/employees issued any digital certificates are solely responsible for the use and security of the certificate. No certificate shall be given to, loaned to or used by anyone other than the person named on the digital certificate.

f. Information Management Division shall perform random system audits twice a year to insure security.

g. To protect the integrity of User Name and Password access, users shall log off or lock their computer when they leave their immediate work area.

h. When users log in to applications that require a separate user name and password, the screen may offer an option to "remember" the information. To prevent the bypass of application security, the box should not be checked.

2. EXTERNAL ACCESS

a. The Fort Lauderdale Police Department's computer network is protected from unauthorized external access by a secure firewall.

b. A virtual private network will be used to provide a secure, encrypted means of remote data access for law enforcement.

3. DEPARTMENT RESPONSIBILITIES

a. The Information Management Division maintains all electronic offense/incident and supplementary reports, computer operating systems and other duties.

b. The Information Management Division will assist the Public Records Coordinator with services to include providing citizen information, records duplication and release, and the handling of general information.

c. The Records Unit is responsible for coding and disseminating of criminal and non-criminal reports for compiling statistics for the Uniform Crime Report (UCR). This section maintains a centralized, automated (computerized) records system for information storage and retrieval.

d. The Information Management Division is responsible for the Department's computer system.

D. SYSTEM USER ACCESS

1. All requests for access to the agency computer network and associated servers must go through the Information Management Division. When a new employee needs to be added to the computer network and have authority to use software applications contained within, the employee's supervisor must complete and sign an Information Systems Request Form and forward it to the Information Management Division. This form must include the member's CCN and Unit, applications to access, and justification for access. Once the employee has been added to the system with a user ID, password, and correct authority level, an Information Management Division administrator signs the form and forwards a copy back to the appropriate supervisor.

2. Employees will be given the login and password to those programs in which they are authorized to access. Employees will retain the confidentiality of their passwords to prevent unauthorized access. Passwords should not be written down and stored in any unsecured location e.g., under keyboard, on the side of a monitor, or in an unlocked desk drawer. All employees with proper approval are allowed access to the Internet or Intranet through Department computers. Employees will not use the Department's computer system or any of its features to create, generate, perpetuate, comment on, or send any communication that is derogatory, demeaning, unprofessional, obscene, or harassing to any person or group. When a supervisor determines that an employee's access to the agency computer system must be revoked or the employee's level must be modified, the supervisor must complete an Information Systems Request Form and forward it to the Information Management Division. This form must include the employee's position and Department, effective date to revoke access to the system, and/or changes to current access. The form must always be completed when an employee leaves the agency and is no longer considered an active member.

E. ACCESS RESTRICTIONS

1. No employee of the Fort Lauderdale Police Department or any other individual or organization is authorized to utilize any computer hardware, software, or related facilities and supplies for other than official business.

2. All employees should lock their computer at the end of their work day and properly shut down their computers once a week. This does not apply to shared computers or computers and equipment with a designated task to be performed after hours.

F. COMPUTER FILE MAINTENANCE, BACKUP, AND RETENTION

1. Security for Networking Components and Computer System

    a. Information Management Division members are responsible for security and service of the electronic data processing system.

b. The security safeguards control over who can use devices, data, and programs. It also prevents accidental or intentional destruction of the system resources.

c. All software shared via any network server is to be protected by anti-virus software and regular data backups.

d. Browser based software is to be installed/updated with the latest versions of secured, encrypted software compatible with attached hardware and software.

2. Protection of System Data (Backups Stored on Removable Media)

a. Information Management Division employees are required to protect agency electronic data processing information by performing a daily "backup" or "save" procedure. This save procedure copies the organization's data to recordable media. The backup process performed by the designated Information Management Division employee is a process approved by the Information Management Division manager.

b. Users of personal computers are required to store their data files onto individual folders mapped to networked servers. The backup process for all network servers protects this data.

3. Information Management Division Backup: Server resources are backed up daily onto recordable media.

4. Server Backup

a. A server backup is done on all servers which hold critical data.

b. Full backups are done once a week and incrementally every day of the week.

c. A set of system backup media are kept in the computer room.

d. The Information Management Division shall keep the previous month's backup of the system at a location off-site.

5. Network Server Backups

a. All data which resides on the agency network through servers as "shared folder" data will be backed up on a daily basis.

b. A weekly backup tape will be created and stored off-site at a secure location.

c. The backup processes are scheduled and maintained by the Information Management Division.

6. The Records Unit is secured at all times by a locked entrance door. During normal business hours, a member of the Records Section is present at all times.

   a. The Records Unit shall maintain a repository/database of records by incident numbers that are filed by the following methods:

      (1). All Offense Reports are filed by incident number, by the year, and in numerical order. (e.g. the first incident of 2006 would be 06-000001).

      (2). Offense/Incident Reports and Traffic Crash Reports shall be maintained in the Records Unit. Investigative reports are sent to the Records Unit for attaching to the original reports. The disposition contained in the investigative information is entered into the Records Management System and the report is attached to the original Offense/Incident Report.

   b. Access to the electronic records system is managed and maintained by the police department's Information Management Division. They are responsible for insuring that the current security system prevents unauthorized attempts to access, alter, remove, disclose or destroy stored information.

      (1). Access, and the levels thereof, is granted to users through the electronic records system administration module. Access to the system is controlled with unique user names and passwords for each user. Levels of access are granted as specified by the Information Management Division to prevent unauthorized use.

      (2). The Information Management Division will perform an annual audit to verify all passwords, access codes and access violations. This is accomplished by submitting a report of all current user information an Information Management Division supervisor for validation.