| POLICY 111.2 | **Computerized Central Records System** | |
|---|---|---|
| | REVISED: 02/07, 09/11, 07/17 | RELATED POLICIES: |
| | CFA STANDARDS: 34.13 | REVIEWED: AS NEEDED |

## 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.

## 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.

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. DEFINITIONS

ITS – Information Technology Services

LASO – Local Area Security Officer

Active Directory Application – An automated system that emails notifications to appropriate ITS personnel when a timekeeper is notified that an employee is suspended or separated from the city.

Criminal Justice Information (CJI) - Criminal Justice Information is the abstract term used to refer to all of the FBI CJIS provided data necessary for law enforcement agencies to perform their mission and enforce the laws, including but not limited to: biometric, identity history, person, organization, property (when accompanied by any personally identifiable information), and case/incident history data. In addition, CJI refers to the FBI CJIS-provided data necessary for civil agencies to perform their mission; including, but not limited to data used to make hiring decisions. The following type of data are exempt from the protection levels required for CJI: transaction control type numbers (e.g. ORI, NIC, FNU, etc.) when not accompanied by information that reveals CJI or PII.

Criminal Justice Information Services Division (FBI CJIS or CJIS) - The FBI division responsible for the collection, warehousing, and timely dissemination of relevant CJI to the FBI and to qualified law enforcement, criminal justice, civilian, academic, employment, and licensing agencies.

Personally Identifiable Information (PII) – For the purposes of this policy, PII is information extracted from CJI which can be used to distinguish or trace an individual's identity such as name, social security number, or biometric records, alone or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, or mother's maiden name.

## D. PROCEDURES

1. ACCOUNT MANAGEMENT

   a. Establishing, activating, modifying, reviewing and disabling user accounts on all system will be managed by the LASO or appropriately designated system administrator of the system on which the account will exist.

   b. All requests for access to the agency computer network and applications must go through ITS or the approved designated account administrator. New account requests must be submitted via email by the employee's supervisor and must include the employee name, CCN, applications to access, and justification for access. Once the account has been set up the user and supervisor will be notified.

   c. Information systems accounts shall be set up using the concept of least privilege as required by users for specific tasks.

   d. When a supervisor determines that an employee's access to the agency computer system must be revoked or the employee's permissions must be modified, the supervisor must notify ITS or the designated account administrator. This notification must include the employee's position and Department, effective date to revoke access or implement changed permissions, and required changes to current access.

   e. Upon separation from city employment, the Active Directory Application will automatically email notification to ITS staff regarding the user. The same day the notification is received, the user's accounts will be disabled and the Police ITS manager will be notified via email that the account has been disabled. The user's personal files and email will be copied to media and provided to the user's immediate supervisor prior to the deletion of email and files. Information system accounts will be removed unless the system auditing functions require existence of the account, in which case the account will instead be permanently disabled.

   f. Upon suspension the Active Directory Application will automatically email notification to ITS staff regarding the user. The same day the

notification is received, the user's accounts will be disabled and the Police ITS manager will be notified via email that the account has been disabled. Accounts for the user on specific systems may be temporarily enabled as directed by command staff to allow for completion of tasks for example to complete outstanding Police reports.

g. Information systems accounts shall be audited at least annually by ITS. A report of current account information will be submitted to supervisors of each area for validation, and a record of the results shall be documented. The audit results shall include a listing of accounts, changes to the account including permissions changes and/or revocation, and verification and deactivation dates.

2. SYSTEM ACCESS CONTROL

a. Multiple concurrent sessions for applications accessing CJI are only allowed for training or other approved purposes. Any use of multiple concurrent sessions other than for training must be approved the LASO or appropriately designated system administrator of the relevant system. The business needs for any approved multiple concurrent sessions must be documented.

b. User active directory accounts shall enforce a limit of no more than 5 consecutive invalid login attempts.

c. Sessions will lock after 15 minutes of inactivity. In the interest of safety, devices that are: (1) part of a criminal justice conveyance; or (2) used to perform dispatch functions and located within a physically secure location; or (3) terminals designated solely for the purpose of receiving alert notifications (i.e. receive only terminals) used within physically secure location facilities that remain staffed when in operation, are exempt from this requirement.

d. User active directory accounts shall enforce the following requirements for passwords:

(1). Must expire every 90 days

(2). Not contain the user's account name or parts of the user's full name that exceed two consecutive characters

(3). Be at least eight characters in length

(4). Contain characters from three of the following four categories:

(a). English uppercase characters (A through Z)

(b). English lowercase characters (a through z)

(c). Base 10 digits (0 through 9)

(d). Non-alphabetic characters (for example, !, $, #, %)

e. Information systems will display a system use notification before granting access, informing users of various usages and monitoring rules per CJIS Security Policy recommendations.

f. Audit logs of network access are maintained for 1 year and are reviewed randomly at least twice a year by the system administrator.

3. AUTHENTICATION

a. Unique user name and password is required for access to all information systems. Advanced authentication shall be required for access to CJI where it is required. The advanced authentication shall adhere to the CJIS Security policy at a minimum.

b. The agency shall use a unique username and password, combined with an individually assigned security fob for the advanced authentication strategy.

c. Authenticator Management Procedures shall be followed for issuing and revoking authenticators, and to handle lost/compromised or damaged authenticators.

4. REMOTE ACCESS

a. The agency shall control all remote access through managed access control points.

b. All remote access mechanisms require prior approval of the city security team.

c. Remote access shall only be allowed for official use only.

d. Patrol officers and detectives will use remote access to access the agency network to utilize the field reporting system as well as other databases and systems that support law enforcement activities.

e. Personnel using remote access shall be in a physically secure area if they access systems that display CJI.

f. IT staff may remotely access the agency network for privileged functions only as required for operational needs.

g. Unescorted remote access is only permitted for personnel who have successfully passed the Police department background screening process, which includes the CJIS required fingerprint-based background checks, CJIS certification, and security awareness training.

h. Escorted remote access is permitted only under the following conditions:

(1). The session shall be monitored at all times by an authorized escort.

(2). The escort shall be familiar with the system/area in which the work is being performed.

(3). The escort shall have the ability to end the session at any time.

(4). The remote administrative personnel connection shall be via an encrypted (FIPS 140-2 certified) path.

(5). The remote administrative personnel shall be identified prior to access and authenticated prior to or during the session. This authentication may be accomplished prior to the session via an Advanced Authentication (AA) solution or during the session via active teleconference with the escort throughout the session.

5. PERSONNALLY OWNED INFORMATION SYSTEMS

a. Personally owned information system are not allowed access to the agency's information systems which process, store, or transmit CJI data. This control does not apply to the use of personally owned information systems used to access agency information systems and information that are intended for public access (e.g. the agency's public website).

6. DIGITIAL MEDIA ENCRYPTION

a. When CJI is transmitted in digital format outside the physically secure location, the agency will encrypt all data with at least 128-bit encryption. The encryption mechanism shall meet FIPS 140-2 requirements. The ITS department maintains a list of acceptable products that meet the FIPS 140-2 requirements.

b. The agency does not currently use public key infrastructure (PKI).

7. DIGITAL MEDIA SANITATION AND DISPOSAL

a. Information systems that have been used to process, store, or transmit CJI and/or sensitive and classified information shall not be released from the agency's control until the equipment has been sanitized and all stored information has been cleared. Devices that contain digital media on which CJI and/or sensitive information may have been stored must have the media removed and sanitized.

b. Sanitation must be performed using one of the methods listed below:

(1). A software application executed on the computer which overwrites the digital media three times

(2). An electronic device which will overwrite the digital media three times

(3). An electronic hard drive degausser

(4). Physical destruction which ensures no data can be retrieved from the device.

c. Digital media sanitization will be witnessed by authorized agency personnel.

8. PATCH MANAGEMENT

a. ITS staff will review all relevant security patches, service packs and other updates from vendors and will deploy as expediently possible. Patch requirements identified during security assessments, monitoring, or incident response will be addressed expeditiously.

b. Where technically feasible, centralized patch management and automated updating will be configured for information systems.

c. Where technically and operationally feasible, rollback capability will be implemented and testing of patches will be conducted prior to deployment on production systems.

9. COMPUTER FILE MAINTENANCE, BACKUP, and RETENTION

a. Network files are backed up daily. Copies of backups are encrypted and stored offsite.

b. A server backup is performed on all servers that hold critical data.

10. ANTIVIRUS PROTECTION

a. All systems should be protected by antivirus software that is regularly updated. Exceptions to this must be documented, and approved by the Police ITS manager.

11. WIRELESS ACCESS

a. Wireless Access Points (APs) placed on the agency's network shall first be approved by the Police ITS manager.

b. ITS staff will keep an inventory of deployed APs.

c. AP's will be placed in secured areas to prevent unauthorized access.

d. Validation testing will be performed to ensure rogue APs are not attached to the agency network.

e. AP range boundaries will be tested to determine the extent of wireless coverage.

f. Management - User authentication and encryption will be enabled for the management interface of the APs and FIPS compliant secure protocols will be used. Non-essential management protocols will be disabled on APs. Default passwords will be changed and strong administrative passwords will be utilized.

g. The AP reset function shall only be used when needed and will only be invoked by authorized personnel. The AP will be restored to the latest security settings when the reset function is used.

h. The default SSID will be changed and broadcast SSID will be disabled for the SSID allowing access to the agency internal network.

i. Security features of the AP shall be enabled, including cryptographic authentication, firewall and other available privacy features.

j. Wireless access logs will be reviewed on a monthly basis by ITS staff.

k. The wireless network shall be virtually separated from the production wired network and access will be limited to only operational needs.

12. VOIP (Voice over Internet Protocol)

a. VoIP is a collection of technologies that enables the delivery of voice communications and multimedia sessions over Internet Protocol. The Fort Lauderdale Police Department ensures the implementation of VoIP within a network that contains unencrypted CJI will receive the minimum security standards that the Fort Lauderdale Police Department abides by as well as:

(1). Change the default administrative password on the IP phones and VoIP switches.

(2). Utilize Virtual Local Area Network (VLAN) technology to logically segment VoIP traffic from data traffic.

(3). Allow only agency approved VOIP devices on the network.

(4). VOIP technology shall only be used for voice and video.

13. BLUETOOTH

a. Bluetooth will only be used for official business purposes.

b. Only agency approved devices are allowed to be used. This includes such devices as the agency's RAPID ID devices, printers, wireless mice, cellular phones, and headsets.

14. PHYSICAL PROTECTION

a. Media in all forms shall be protected at all times. Electronic media (i.e. hard drives, disks, flash drives, etc.) shall be in physically secure areas with either access card control or locked doors at all times with access granted only to authorized personnel only. Documents containing CJI or PII shall be protected as described in Policy 112.2 – D.1.

15. SECURITY ALERTS AND ADVISORIES

a. ITS staff will subscribe to security alerts and advisories.

b. Each notification shall be evaluated for urgency and relevance to the agency. Based on the evaluation a plan will be developed and promptly executed to perform actions such as applying updates, changing system configuration, modifying policies or notifying appropriate personnel.

16. INCIDENT RESPONSE

a. Should a security incident occur involving any device (workstations, smart phones, laptops, tablets, etc.) that is on the Fort Lauderdale Police Department's network, ITS security personnel and the LASO shall be contacted immediately. The Computer Security Incident Response procedure will be followed.

b. If the Computer Security Incident Response procedure deems it necessary, the City of Fort Lauderdale's Computer Incident Response Team will be activated. If it is determined by the LASO to be a security breach associated with CJI, a Security Incident Response Form will be filled out and submitted to FDLE Information Security Officer and FDLE Customer Support Center.

c. In the event that a mobile device with CJI data is left unattended in an unsecured location for any period of time, or the mobile device is lost or stolen, the LASO must be contacted immediately and an incident report must be created if deemed necessary.

17. DEPARTMENT RESPONSIBILITIES

a. Information Technology Services is responsible for the maintenance, security, and backups of all the agency computer systems.

b. Information Technology Services will assist the Public Records Coordinator with services to include providing search and duplication of electronic records.

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.

18. COMPUTER USE POLICY

The following applies to use of desktop, laptop, and tablet computers connecting to the agency network.

a. 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.

b. Users shall lock their sessions when they leave their computer unattended.

c. 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.

d. Users of personal computers must store all important data files onto individual folders mapped to networked servers. The backup process for all network servers protects this data. Data files stored on the local computer desktop are NOT backed up.

e. Incidental personal use of agency computers and network may be permitted provided such use does not interfere with agency resources, does not interfere with the employee's job, does not incur costs for the agency, and otherwise complies with agency and city policies.

f. All employees with proper approval are allowed access to the Internet and Intranet through agency computers. Employees will not use the agency'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.

g. All computer security related incidents should be reported to ITS staff immediately.

h. All employees will adhere to the Digital Media Encryption Policy when transporting CJI or confidential data on digital media. The digital media shall be provided to ITS for destruction when the device is no longer in use.

i. All employees will adhere to Policy 112.2 – Criminal Justice Information Access when accessing PII or CJI from their computers.