NORTH MIAMI POLICE DEPARTMENT

STANDARD OPERATING PROCEDURES

CRIMINAL JUSTICE INFORMATION SYSTEM (CJIS) SECURITY 100.10

EFFECTIVE DATE: 06-15-23 APPROVED: _____
Chief of Police

SUPERSEDES: 08-13-21 CFA: N/A

I. PURPOSE

To provide members with guidance on the proper use of computers and related electronic messaging systems utilized by this Agency for purposes of disseminating electronic mail, utilizing services of the internet and related electronic message transmissions and recording devices.

II. POLICY

That all members abide by the guidelines set forth in this policy when using electronic services of both internal and external databases and information exchange networks, mobile computing terminals and related electronic messaging devices. No devices of any kind may be attached to any City computer equipment without the expressed authorization of the Local Agency Security Officer.

III. SCOPE

This policy applies to all members of the Department.

IV. DEFINITIONS

C.S.A. – Criminal Justice Information System Agency

I.S.O. - Information Security Officer

C.A.C. - CJIS Agency Coordinator (CAC): Will act as the central point of contact regarding all communications between FDLE CJIS and the User. The CAC shall have User authority to ensure that all agency identified personnel, including those with decision making authority, are made aware and able to participate in all FDLE CJIS discussions that may lead to User business and policy changes. Once a CEO or Agency Head has signed and submitted a User Agreement or an ACF designating a CAC, the CAC shall have the authority to appoint other User personnel to serve in other designated CJIS positions, as well as the authority to sign subsequent agency contact forms.

LASO - Local Agency Security Officer (LASO): The LASO is responsible for the agency's compliance with the FBI CJIS Security Policy (CSP) and all applicable security requirements of the criminal justice information network and systems. The LASO/Alt-LASO should be knowledgeable of the technical aspects of the agency's network and maintain an ongoing working relationship with the local technical staff as well as the FCIC Agency Coordinator (FAC/Alt-FAC). The LASO is the main contact for the triennial CJIS Technical Audit and should be able to provide the agency's current network diagram during the audit and whenever additional CJIS access is requested. The LASO must complete the online LASO training available in nexTEST annually and complete the Level 4 Security Awareness Training, every two (2) years, available in CJIS Online.
The responsibilities of the LASO include:

1. Identify who is using the CJIS System Agency (C.S.A.) approved hardware, software, and firmware and ensure no unauthorized individuals or processes have access to the same.

2. Identify and document how the equipment is connected to the State system.

3. Ensure that personnel security screening procedures are being followed as stated in the CJIS Security Policy.

4. Ensure the approved and appropriate security measures are in place and working as expected.

5. Support policy compliance and ensure the C.S.A. Information Security Officer (I.S.O.) is promptly informed of security incidents.

Physically Secure Location - The Department's Physically Secure Location is the entire department. The perimeter of the physically secure location shall be

prominently posted and separated from non- secure location by physical controls.

F.A.C. - FCIC Agency Coordinator. The FAC ensures compliance with the legal and policy requirements contained within the CJIS User Agreement and Requirements Document, and facilitates communication between FDLE.

Visitor - A visitor is defined as a person who visits the Department on a temporary basis who is not employed by the Department and has no unescorted access to the physically secure location within the Department.

V. RELATIONSHIP TO LOCAL SECURITY POLICY AND OTHER POLICIES

The Department shall adhere at a minimum to the CJIS Security Policy (available on PowerDMS). The Department may augment or increase the standards, but will not detract from the CJIS Security Policy Standards.

The Department will post this CJIS Security Policy on PowerDMS and will notify and disseminate updates and changes when needed.

VI. PERSONALLY IDENTIFIABLE INFORMATION (PII)

PII, as defined by the CJIS Security Policy (4.3), is information 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.

The Department will ensure appropriate controls are applied when handling PII that is extracted from CJI. Confidential, proprietary or sensitive information extracted from CJI may be disseminated only to those who are authorized recipients of CJI. Authorized recipients are normally other criminal justice agencies. PII that is extracted shall not be retained beyond the records retention rules for the data and the system it was accessed from. PII shall not be stored or transmitted via personally owned devices. PII may not be taken home by any agency member.

VII. INFORMATION EXCHANGE

The Department maintains a Criminal Dissemination Log of all criminal histories which are disseminated outside of the Records Department, including those instances considered to be secondary dissemination. The release of criminal history information from the FCIC/NCIC computer systems is governed by FCIC/NCIC and is only released for criminal justice purposes. Before disseminating CJI, all requestors shall be validated to ensure they are an authorized recipient of CJI. When requested by an outside agency, before information is disseminated, validation of the requesting officer's employment with a law enforcement agency will be made. Dissemination of CJI will be logged in a secondary dissemination log.

Personnel found in violation of FCIC/NCIC access restrictions will be subject to disciplinary action.

VIII. INFORMATION HANDLING

The Department shall ensure that CJI is protected from unauthorized disclosure, alteration or misuse. These procedures shall include CJI inquiries for both criminal justice and noncriminal justice purposes. All CJI inquiries shall be logged completely into the Dissemination Log. All CJI inquiries that are not disseminated shall be shredded immediately. All CJI that is disseminated outside of the Department shall be stamped "CONFIDENTIAL LAW

ENFORCEMENT USE ONLY" and include the operator's name, requestor's name, requestor's agency, reason for the inquiry, and the date of dissemination.

IX. SECURITY INCIDENT RESPONSE

A "security incident" is a violation or possible violation of the technical aspects of the CJIS Security Policy that threatens the confidentiality, integrity or availability of FCIC/NCIC. Users may only see indicators of a "security incident." The following is a partial list of incident indicators that deserve special attention from users and/or Network Administrators:

- The system unexpectedly crashes without clear reason;
- New user accounts are mysteriously created which bypass standard procedures;
- Sudden high activity on an account that has had little or no activity for months;
- New files with novel or strange names appear;

- Accounting discrepancies;
- Changes in file lengths or modification dates;
- Attempts to write to system files;
- Data modification or deletion;
- Denial of service;
- Unexplained poor system performance.
- Anomalies;
- Suspicious probes; and
- Suspicious browsing.

If an incident occurs involving any device (workstations, laptops, etc.) that is on the North Miami Police Department network, the LASO shall be contacted immediately, who shall document the actions throughout the process from initial detection to final resolution. If it is deemed by the LASO to be a security breach of confidential information, a Security Incident Response Form will be filled out and submitted electronically to FDLE ISO. All Security Incidents will be documented on a security incident reporting form, kept by the LASO and FAC and will be retained for no less than a three year period.

All users are responsible for reporting known or suspected information or information technology security incidents. All incidents must be reported immediately to the Agency LASO. The LASO will inform a member of IT and document the incident.

If a suspected incident occurs on a user's mobile device, the user shall not turn off the device. The user will leave the device on and report the incident. A member of IT will look over the device and determine if the incident is contained to the one device or if it is within the Agency system.

The Agency will employ VIPRE antivirus software on all desktop and laptop devices and will ensure that the antivirus software is up-to-date.

The Agency will identify the security breach by conducting the following:

1. Confirm the discovery of a compromised resource(s);
2. Evaluate the security incident;
3. Identify the system(s) of information affected;
4. Review all preliminary details;
5. Characterize the impact on the agency as: minimal, serious, or critical;
6. Determine where and how the breach occurred;
    a. Identify the source of compromise and the time frame involved.

b. Review the network to identify all compromised or affected systems.

7. Examine appropriate system and audit logs for further irregularities; and
8. Document all internet protocol (IP) addresses, operating systems, domain system names and other pertinent system information. Initiate measures to contain and control the incident to prevent further unauthorized access.

X. ACCOUNT MANAGEMENT

The management of CJI system accounts shall be conducted by the FCIC Agency Coordinator personnel at the direction of the LASO in accordance with all policies and CJIS Security Policy requirements. New employee personnel will gain access to all systems upon start date, but will lose access to CJI systems if training courses are not completed or passed within 30 days. All user accounts of retired, terminated, suspended or otherwise former and non-working employees shall be disabled and revoked immediately or as soon as practicable. User accounts suspected of compromise shall be immediately disabled upon first discovery of compromise. Logs of access privilege changes shall be maintained for a minimum of one year and document the validation process.

The Agency LASO/FAC is the point of contact for all accounts. The LASO/FAC shall manage information system accounts to include establishing, activating, modifying, reviewing, disabling, and removing user accounts on all Criminal Justice Information Systems.

Account Creation:

Upon completion of appropriate state and national fingerprint-based records check, the Agency will notify the FAC and LASO and provide the following information regarding the user:

A. Applicant full name;
B. Applicant date of birth;
C. Applicant social security number;
D. Applicant start date;
E. Applicant assigned MDT (laptop);
F. Applicant system(s) access; and
G. Applicant system(s) permissions.

The LASO will create and establish a Windows Domain account for the applicant. All accounts are created to ensure a unique username for every individual.

A. The Domain account will be assigned a temporary password and will be set up to require the user to create a new password upon activating the first session. The password for the account must adhere to the Agency password requirements outlined in the Authentication Strategy Policy.

B. The LASO will establish an account for the RMS, CAD and mobile CAD systems for the user utilizing the same username requirements.

C. The LASO will identify the level of authority for the user for each application as:

1. Officer;
2. Supervisor;
3. Records;
4. User; and
5. Administrator.

D. The LASO will provide the initial credentials and temporary password to the user's supervisor.

E. Upon completion of paperwork, the user will be issued Agency equipment delegated to the users' position within the Agency. Equipment includes, but is not limited to, Agency laptop, WiFi device for wireless access, keycard and identification badge. Subsequent equipment changes, deletions, enhancements will be documented via Agency equipment receipt form and approved through Agency chain of command.

F. The LASO or FAC will meet with the new user upon starting to ensure proper access to each information system is granted.

Account Modification:

In the event of promotion, demotion, suspension, leave or voluntary or involuntary termination, the supervisor will immediately notify the LASO and/or FAC of the change of status to ensure appropriate access changes are made to systems and applications.

A. Promotion/Demotion- Supervisor will notify LASO and/or FAC of the change of status and change of authority level.

- The LASO and/or FAC will update all systems and applications as necessary to evolve with the current status of employment and will document these changes in the active directory.

B. Suspension/Leave - Supervisor will notify LASO and/or of the temporary change to the users' account.
   - The LASO and/or FAC will temporarily deactivate the account on each system and application.
   - The Supervisor will collect all agency equipment from the user and document the transaction.
   - Upon reinstatement, the supervisor will notify the LASO and FAC to return all agency equipment to the user.
   - The LASO and/or FAC will reactivate the user accounts on all systems and applications.

Account Termination:

- Upon termination from the Agency, whether voluntary or involuntary, the supervisor will inform the LASO and/or FAC of the employment change.
- The LASO and/or FAC will disable all accounts on all information systems and applications.
- The LASO and/or FAC will place the user in the Disabled User Organizational Unit within Active Directory, remove all access of controls from the user, disable Agency e-mail account, and remove remote access ability and all permissions.
- The supervisor will collect all Agency equipment and have the user sign the equipment receipt.

Account Validation:

- The FAC will validate Agency User Accounts and Access Privilege Levels annually.
- The FAC will document the date and time of the validation on the Agency Validation Form.
- The FAC will verify that all active accounts are current and up-to-date.

- Any changes made by the FAC involving an account will be documented.

XI. ACCESS CONTROL

Authorized users are permitted to be logged on to multiple computers concurrently to connect to a secure CJI system. Concurrent sessions are necessary at times to fulfill the operational needs of the department and training requirements.

XII. REMOTE ACCESS

The Agency utilizes remote access to communicate with information systems through an external, non-agency-controlled network. The purpose of this policy is to outline acceptable methods of remote access and the security in place to keep the information system(s) secure.

Remote access shall only be used for official use only. This includes those on duty patrol officers remoting in to agency's network using a VPN tunnel. IT personnel may remote access into the agency's network only for emergency purposes. Vendor companies may be granted access to the agency's network only if they are virtually escorted by authorized personnel at all times.

It is the responsibility of Agency employees, contractors and vendors with remote access privileges to the Agency network to ensure that the connection is secure. All remote access to the Agency information systems must be done through the Agency's VPN tunnel. The tunnel will be verified as FIPS 140-2 certified. Those personnel accessing the VPN must use advanced authentication as a secondary form of authentication in order to access the network. All access for contractors and vendors performing IT work will be done utilizing encrypted remote access. The Agency authorizes Bomgar Remote Access for this, which is FIPS 140-2 certified. IT will monitor and control all remote access to the Agency systems. For Virtual escorting, the Agency allows this for compelling operational needs. In these cases, IT will monitor the session, be familiar with the system where work is being performed as well as have the ability to end the session at any time. IT must verify the person gaining access prior to allowing the session. This will be done through advanced authentication (PIN).

XIII. PERSONALLY OWNED INFORMATION SYSTEM

Personally owned information systems (e.g. laptops, tablets, phones) are not authorized to access, process, store or transmit CJI. Personally owned devices are allowed to access the City email system. If a personally owned device used to access the City email system is lost, City IT shall be notified immediately to block access to the City email system.

XIV. AUTHENTICATION STRATEGY

This Password Policy applies to all information systems and applications that contain criminal justice information or services. This includes, but is not limited to:

- Mainframes, servers and other devices that provide centralized computing capabilities;
- SAN, NAS and other devices that provide centralized storage capabilities;
- Agency issued desktops, laptops, or any other device that provides distributed computing capabilities;
- Routers, switches and other devices that provide network capabilities;
- Firewalls and other devices that provide dedicated security capabilities; and
- Windows Domain Accounts, Agency e-mail accounts, mobile CAD application accounts as well as any other criminal justice information system or service.

The Agency LASO will ensure each account is set up with a temporary password. When the user initiates a first time log-on, the temporary password will be entered and the user will be prompted to create a new password.

The Agency dictates that each password and User-ID be unique and not be shared with any other individual. Users are forbidden to share their unique password or write it down. All passwords must be memorized.

XV. AUTHENTICATOR MANAGEMENT

Upon direction of the FAC, the LASO will issue advanced authentication tokens to necessary Department employees. The LASO will assign a token and the employee will download their digital certificate to their assigned token. Digital certificates will be deleted for all lost, damaged or separated employees. Users shall take reasonable measures to safeguard authenticators including maintain possession of their individual authenticators, not loaning or sharing authenticators with others, and immediately report lost or compromised authenticators.

XVI. MEDIA PROTECTION

This Media Protection Policy, derived from the FBI's CJIS Security Policy (available on PowerDMS), applies to any electronic or physical media containing Criminal Justice Information (CJI) while being stored, accessed or physically moved from a secure location from the Department. This policy applies to any authorized person who accesses, stores, and / or transports electronic or physical media. Transporting CJI outside the agency's assigned physically secure area must be monitored and controlled.

The intent of the Media Protection Policy is to ensure the protection of the Criminal Justice Information (CJI) until such time as the information is either released to the public via authorized dissemination (e.g. within a court system or when presented in crime reports data), or is purged or destroyed in accordance with applicable record retention rules.

Controls shall be in place to protect electronic and physical media containing CJI while at rest, stored, or actively being accessed. "Electronic media" includes memory devices in laptops and computers (hard drives) and any removable, transportable digital memory media, such as magnetic tape or disk, backup medium, optical disk, flash drives, external hard drives, or digital memory card. "Physical media" includes printed documents and imagery that contain CJI.

To protect CJI, the department personnel shall:

- Lock or log off computer when not in immediate vicinity of work area to protect CJI. Not all personnel have the same CJI access permissions and need to keep CJI protected on a need-to-know basis;
- Securely store electronic and physical media within a physically secure or controlled area;
- Restrict access to electronic and physical media to authorized individuals;
- Ensure that only authorized users remove printed or digital media from the CJI;
- Physically protect CJI until media end of life. End of life CJI is destroyed or sanitized using approved equipment, techniques and procedures;

- Not use personally owned information system to access, process, store, or transmit CJI; and

- Not utilize publicly accessible computers to access, process, store, or transmit CJI. Publicly accessible computers include but are not limited to: hotel business center computers, convention center computers, public library computers, public kiosk computers, etc.

All hardcopy CJI printouts maintained by the Department will be stored in a secure area accessible to only those employees whose job function requires them to handle such documents.

Personnel should take appropriate action when in possession of CJI while not in a secure area. CJI must not leave the employee's immediate control. CJI printouts cannot be left unsupervised while physical controls are not in place.

Precautions must be taken to obscure CJI from public view, such as by means of an opaque file folder or envelope for hard copy printouts. For electronic devices like laptops, use session lock use and /or privacy screens. CJI shall not be left in plain public view. When CJI is electronically transmitted outside the boundary of the physically secure location, the data shall be immediately protected using encryption.

When CJI is at rest (i.e. stored electronically) outside the boundary of the physically secure location, the data shall be protected using encryption that is certified to meet FIPS 140-2 standards. Storage devices include external hard drives from computers, printers and copiers used with CJI. In addition, storage devices include thumb drives, flash drives, back-up tapes, mobile devices, laptops, etc.

Controls shall be in place to protect electronic and physical media containing CJI while in transport (physically moved from one location to another) to prevent inadvertent or inappropriate disclosure and use. "Electronic media" means electronic storage media including memory devices in laptops and computers (hard drives) and any removable, transportable digital memory media, such as magnetic tape or disk, backup medium, optical disk, flash drives, external hard drives, or digital memory card.

The Department personnel shall control, protect and secure electronic and physical media during transport outside of the physically secured area from public disclosure by:

- Restricting the pickup, receipt, transfer, delivery and possession of such media to authorized personnel.

- Securing hand carried confidential electronic and paper documents by storing CJI in a sealed envelope marked 'Confidential', maintaining continuous immediate control over CJI during transport and only viewing or accessing the CJI electronically or document printouts in a physically secure location by authorized personnel.

XVII. ELECTRONIC MEDIA SANITATION AND DISPOSAL

When no longer usable, hard drives, diskettes, tape cartridges, CDs, ribbons, hard copies, print-outs, and other similar items used to process, store and/or transmit CJI and classified and sensitive data shall be properly disposed of. Electronic media (hard drives, CDs, flash drives, printer and copier hard drives, etc.) shall be disposed of by one of the following methods:

- Overwriting (at least 3 times) – an effective method of clearing data from magnetic media. As the name implies, overwriting uses a program to write (1s, 0s or a combination of both) onto the location of the media where the file to be sanitized is located.

- Destruction – a method of destroying magnetic media. As the name implies, destruction of magnetic media is to physically dismantle by methods of crushing, disassembling, etc., ensuring that the plates have been physically destroyed to that no data can be pulled.

- A sworn officer must accompany I.T. personnel transporting media for destruction, and witness same.

IT systems that have been used to process, store, or transmit CJI and/or sensitive and classified information shall not be released from the Department's control until the equipment has been sanitized and all stored information has been cleared by one of the above methods.

XVIII. DISPOSAL OF PHYSICAL MEDIA

When no longer usable, hard drives, CDs, hard copies, print-outs, and other similar items used to process, store and/or transmit CJI and classified and sensitive data shall be properly disposed of.

Physical media (print-outs and other physical media) shall be disposed of by one of the following methods:

- Shredding by using Department equipment; and
- Placing in locked shredding bins for a contracted Shredding company. The company shall shred onsite and be witnessed by Department personnel throughout the entire process.

IT systems that have been used to process, store, or transmit CJI and/or sensitive and classified information shall not be released from the Department's control until the equipment has been sanitized and all stored information has been cleared by one of the above methods.

XIX. PHYSICAL PROTECTION

All visitors must be identified and accompanied by a Department escort at all times, including vendors, contractors, and delivery personnel. Visitors must not be allowed to view computer screens.

Only authorized personnel will have access to physically secure non-public locations. The Department will maintain and keep a current list of authorized personnel. All physical access points into the agency's secure areas will be authorized before granting access. The agency will implement access controls and monitoring of physically secure areas for protecting all transmission and display mediums of CJI. Authorized personnel will take necessary steps to prevent and protect the agency from physical, logical and electronic breaches. All computer screens will be turned away from public view or minimized. All physical media containing CJI will be locked in filing cabinet in a restricted area. Only authorized personnel will have a key to the cabinet.

All personnel with CJI physical and logical access must:

A. Meet the minimum personnel screening requirements prior to CJI access.

- To verify identification, a state of residency and national fingerprint-based record checks shall be conducted within 30 days of assignment for all personnel who have direct access to CJI and those who have direct responsibility to configure and maintain computer systems and networks with direct access to CJI.

- Support personnel, private contractors/vendors, and custodial workers with access to physically secure locations or controlled areas (during CJI processing) shall be subject to a state and national fingerprint-based record check unless these individuals are escorted by authorized personnel at all times.

- Prior to granting access to CJI, the Department on whose behalf the contractor is retained shall verify identification via a state of residency and national fingerprint -based record check.

- Refer to the CJIS Security Policy for handling cases of felony convictions, criminal records, arrest histories, etc.

B. Complete security awareness training.

- All authorized Department Noncriminal Justice Agencies (NCJA) and private contractor/vendor personnel will receive security awareness training within six months of being granted duties that require CJI access and every two years thereafter.

- Security awareness training will cover areas specified in the CJIS Security Policy at a minimum.

C. Be diligent of who is in their secure area before accessing confidential data.

- Take appropriate action to protect all confidential data.

- Protect all terminal monitors with viewable CJI displayed on monitor and not allow viewing by the public or escorted visitors.

D. Properly protect and not share any individually issued keys, computer account passwords, etc.

- Report loss of issued keys to authorized agency personnel

- Safeguard and not share passwords, Personal Identification Numbers (PIN), Security Tokens (i.e. Smartcard), and all other facility and computer systems security access procedures.

E. Properly protect from viruses, worms, Trojan horses, and other malicious code.

F. Not use personally owned devices on the Department computers with CJI access.

G. Ensure the perimeter security door securely locks after entry or departure. Do not leave any perimeter door propped opened and take measures to prevent piggybacking entries.

XX. EMAILING CJI

Due to the inability of the Department to meet the encryption standards of CJIS Security Policy, emailing of any CJI data shall be strictly prohibited.

XXI. PATCH MANAGEMENT

All components of the IT system with CJIS connectivity shall be updated with all available security hot fixes, updates and patches within 30 days of availability. This applies to workstations, servers, laptops, switches, routers, and all other managed IT equipment. All workstations, servers and MDT's shall be configured to automatically download and install Windows updates. When feasible, third party software patches shall be tested prior to installation and provide the ability to rollback patches and updates. The Department's antivirus program will monitor all system computers for antivirus and operating system patch levels. Any machine found in violation of this Policy shall require immediate corrective action.

XXII. ACTIONS IN RESPONSE TO ALERTS

The LASO will receive security alerts and advisories. These alerts can come from servers, databases, systems, boundary protection (firewalls) devices, and by various email registrations or list servers. When applicable, and if necessary, the LASO will issue alerts and advisories to agency personnel when necessary and if applicable.

In the event of a serious security alert/advisory, the LASO will document actions to be taken, for internal documentation/logging and will also act to mitigate the threat (i.e. keep system from crashing, disruption of service, etc.) accordingly.

Additionally, the Department uses Anti-Virus software to ensure when necessary, that Department computers provide alerts and advisories to users. If you receive a security notice on your computer or experience any incident indicators previously outlined, contact the LASO immediately.

XXIII. PERSONAL SECURITY SANCTIONS PROCESS

All Department employees will abide by this policy.

Violations are subject to disciplinary actions such as termination, and/or civil or criminal penalties.

XXIV. WIRELESS ACCESS RESTRICTIONS

Department-issued computers and devices are for the sole purpose of conducting official work related functions. CJI data and systems can only be accessed for the administration of criminal justice.

XXV. BLUETOOTH

Bluetooth connections are only approved for Department issued printers and Rapid ID devices. No other Bluetooth devices are approved for use with Department issued equipment.

XXVI. INCIDENT RESPONSE LOSS OF DEVICE CONTROL

If at any time there is a loss of mobile device control, i.e., the device is in the physical control of non-CJIS authorized individual or the device is left unattended in an unsecure location, the LASO will be notified immediately. Examples of loss of device control are but not limited to:

- Device left at call location;
- Inability to locate device for any length of time;
- Device left in a non-physically secure location (Outside of station or patrol car); and
- Upon notification, the LASO will take appropriate steps to mitigate potential CJI access based on device state, duration of loss, and scenario, and submit an incident report to F.D.L.E. if necessary.

XXVII. FCIC/NCIC

Criminal history record information derived from Federal and State records systems will be disseminated only to criminal justice agencies, and only for criminal justice purposes.

Personnel having access or use of criminal history record information shall access or use such information only for legitimate and approved criminal justice purposes and shall not release such information to unauthorized agencies or individuals.

Personnel authorized to access and control the release of criminal history record information shall comply with all guidelines, regulations, and Standard Operation Procedures established by the Department concerning access and control of such information.

XXVIII. ACCESS TO FCIC/NCIC CRIMINAL HISTORY RECORDS

Access to FCIC/NCIC criminal history record information is restricted to those personnel designed by the Department to perform this function.

Personnel authorized to access criminal history record information will meet training and certification requirements in effect for the performance of this function, and will be familiar with all terminology, guidelines, regulations, and user agreements in effect regarding access and control of such information.

FCIC/NCIC criminal history record information may be accessed only for legitimate criminal justice purposes and controlled by Federal and State statutes, regulations, and guidelines.

The Department shall institute security precautions and Standard Operation Procedures in compliance with provisions established within User Agreements pertaining to information access.

Personnel found in violation of FCIC/NCIC access restrictions will be subject to disciplinary action, including up to termination

Violation of access restrictions may result in termination of the User Agreement, cessation of FCIC/NCIC access services to the Department, and may result in fines and penalties being assessed against the Department and/or responsible employees.

For further details on FCIC/NCIC, please refer to SOP 400.13 FCIC/NCIC

Procedures.

XXIX. VOICE OVER INTERNET PROTOCOL

The agency utilizes a Voice over Internet Protocol (VoIP) for the telephone system. It is located on its own network and is encrypted.

The entire VOIP system resides on its own Network, bandwidth and utilization are all ensured and monitored via QoS and software restrictions.

IT will ensure that software patches for the VoIP system and servers originate from the system manufacturer and are applied in accordance with the manufacturer's instructions prior to implementing the patches.

North Miami Police will ensure all critical VoIP network and server components are located in the physically secured area and that only authorized personnel have access to them. This will limit physical access to the VoIP network segment.

North Miami Police will ensure that the default administrative password on the IP phones and VoIP switches are changed prior to implementation.

North Miami Police will utilize Virtual Local Area Network technology to segment VoIP traffic from the data traffic. The Agency will ensure that the VoIP system is not on the same VLAN as the Agency's information network.

North Miami Police will use IPsec for all remote management and auditing access of the VoIP system.

Remote access of the Voice network can only be completed with the use of an IPSec VPN connection

Our agency has enabled a VoIP-ready firewall designed for VoIP to aid in securing the system.

Any member of the North Miami Police Department will avoid openly discussing criminal justice information over the VoIP phone lines unless there is an immediate need such as officer safety.

XXX. ENCRYPTION

When CJI is transmitted 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 and certificate shall be kept on file at all

times.

At the moment the agency does not utilize PKI.