NORTHERN LANCASTER COUNTY REGIONAL POLICE DEPARTMENT	
☒ General Order ☐ Special Order ☐ Personnel Order	Order Number **6.2.0**

Subject: **Criminal Justice Information and Criminal History Records**		
Original date of issue: **01/01/2012**	Effective date: **09/17/2024**	Expiration Date: **Until amended or revoked**
Reference: **6.2.1, 6.2.2, 6.2.3, 6.2.4, 6.2.5, 6.2.6, 6.2.7, 6.2.8**		
Amends: **** (Chapters combined under a single policy), 02/26/21, 04/02/2023, 04/24/2024		Rescinds:
Review Dates: 2/26/21, 04/27/23, 04/24/2024, 09/17/2024		
Index words: CJI, CHRI, criminal justice information, criminal history records information, dissemination		
Distributions: 1. General Order Manuals 2. Reading Verification to all Personnel 3. Distribution via Power DMS		
In interpretation of this chapter, the singular shall include the plural and the masculine shall include the feminine and the neuter.		

This order contains the following sections:

6.2.1 Purpose and scope

It shall be the policy of the NLCRPD to adhere to a uniform policy for the establishment of guidelines in the regulation of maintaining, disseminating, expunging, discipline, and the destruction of criminal justice information, criminal history records information, and unused automated system components in compliance with state and federal regulations associated with the protection of restricted information.

6.2.2 Definitions

1. CJI: criminal justice information –hot file data (stolen cars, etc.) and criminal history data.

2. CJIS: Criminal Justice Information Services – which includes any system used to process, store, and/or transmit CJI. National and State CJIS systems contain CHRI.

3. CHRI: Criminal History Record Information – arrest-based data and any derivative information from that record. CHRI data included:

    a. Descriptive data.
    b. FBI number.
    c. Conviction status.
    d. Sentencing data.
    e. Incarceration.
    f. Probation and Parole information.

4. CLEAN: Commonwealth Law Enforcement Assistance Network – A statewide computerized information system established as a service to all law enforcement and criminal justice agencies within the Commonwealth Of Pa.

5. NCIC: National Crime Information Center.

6. CPIC: Canadian Police Information Center – administered by the Royal Canadian Mounted Police.

7. INTERPOL: International Criminal Police Organization.

8. NLETS: The International Justice and Public Safety Information Sharing Network – provides interstate and/or interagency exchange of information.

9. Automated Systems - A computer or other internally programmed device capable of automatically accepting and processing data, including computer programs, data communication links, input and output data and data storage devices.

10. Criminal History Agency - A court, including the minor judiciary, with criminal

jurisdiction or another governmental agency, or sub-unit thereof, created by statute or by the State of Federal Constitution, specifically authorized to perform as its principle function the administration of criminal justice, and which allocates a substantial portion of its annual budget to that function. the term includes organized state and municipal police departments, local detention facilities, county, regional and state correction facilities; probation agencies; district or prosecuting attorneys; parole boards, pardon boards and agencies or sub-units thereof, as are declared by the Attorney General to be criminal justice agencies as determined by a review of applicable statutes and the State and Federal Constitution, or both.

11. Dissemination - The oral or written transmission or disclosure of criminal history record information.

12. Intelligence Information - Information concerning the habits, practices, characteristics, possessions, associations, or financial status of an individual compiled in an effort to anticipate, prevent, monitor, investigate, or prosecute criminal activity.

13. Investigative Information - Information assembled as a result of the performance of an inquiry, formal or informal, into a criminal incident or an allegation of criminal wrongdoing and may include modus operandi information.

14. Treatment Information - Information concerning medical, psychiatric, psychological, or other rehabilitative treatment provided, suggested or prescribed for an individual charged with or convicted of a crime.

6.2.3 CJI Physical Protection

The purpose of this section is to provide guidance for agency personnel, support personnel, and private contractors/vendors for the physical, logical, and electronic protection of Criminal Justice Information (CJI). All physical, logical, and electronic access must be properly documented, authorized and controlled on devices that store, process, or transmit unencrypted CJI. This Physical Protection Policy focuses on the appropriate access control methods needed to protect the full lifecycle of CJI from insider and outsider threats.

This Physical Protection Policy was developed using the FBI's *CJIS Security Policy* 5.1 dated July 13, 2012. The intended target audience is [NLCRPD] personnel, support personnel, and private contractor/vendors with access to CJI whether

logically or physically. The local agency may complement this policy with a local policy; however, the *CJIS Security Policy* shall always be the minimum standard and local policy may augment, or increase the standards, but shall not detract from the *CJIS Security Policy* standards.

Physically Secure Location:

A physically secure location is a facility or an area, a room, or a group of rooms within a facility with both the physical and personnel security controls sufficient to protect the FBI CJI and associated information systems. The perimeter of the physically secure location shall be prominently posted and separated from non-secure locations by physical controls. Security perimeters shall be defined, controlled, and secured. Restricted non-public areas in the [NLCRPD] shall be identified with a sign at the entrance.

Visitors Access:

A visitor is defined as a person who visits the [NLCRPD] facility on a temporary basis who is not employed by the [NLCRPD] and has no unescorted access to the physically secure location within the [NLCRPD] where FBI CJI and associated information systems are located. For agencies with jails with CJIS terminals, additional visit specifications need to be established per agency purview and approval.

Visitors shall:

1. Check in before entering a physically secure location by:
    a. Completing the visitor access log, which includes name and visitor's agency, the purpose for the visit, date of visit, time of arrival and departure, name and agency of person visited, and form of identification used to authenticate visitor.
    b. Document the badge number on the visitor log if a visitor badge is issued. If [NLCRPD] issues visitor badges, the visitor badge shall be worn on the approved visitor's outer clothing and collected by the agency at the end of the visit.
    c. Planning to check or sign in multiple times if visiting multiple physically secured locations and/or building facilities that are not adjacent or bordering each other that each has its own individual perimeter security to protect CJI.
2. Be accompanied by a [NLCRPD] escort at all times to include delivery or service personnel. An escort is defined as authorized personnel who accompanies a visitor at all times while within a physically secure location to ensure the protection and integrity of the physically secure location and any

CJI therein. The use of cameras or other electronic means used to monitor a physically secure location does not constitute an escort.

3. Show [NLCRPD] personnel a valid form of photo identification.

4. Follow [NLCRPD] policy for authorized unescorted access.

   a. Noncriminal Justice Agency (NCJA) like city or county IT who require frequent unescorted access to a restricted area(s) will be required to establish a Management Control Agreement between the [NLCRPD] and NCJA. Each NCJA employee with CJI access will appropriately have state and national fingerprint-based records.
   b. Private contractors/vendors who require frequent unescorted access to a restricted area(s) will be required to establish a Security Addendum between the [NLCRPD] and each private contractor personnel. Each private contractor personnel will appropriately have state and national fingerprint-based record background check prior to this restricted area access being granted.

5. Not be allowed to view screen information mitigating shoulder surfing.

6. Individuals not having any legitimate business in a restricted area shall be courteously escorted to a public area of the facility. Strangers in physically secure areas without an escort should be challenged. If resistance or behavior of a threatening or suspicious nature is encountered, sworn personnel shall be notified or call 911.

7. Not be allowed to sponsor another visitor.

8. Not enter into a secure area with electronic devices unless approved by the [NLCRPD] Local Area Security Officer (LASO) to include cameras and mobile devices. Photographs are not allowed without the permission of the [NLCRPD] assigned personnel.

9. All requests by groups for tours of the [NLCRPD] facility will be referred to the proper agency point of contact for scheduling. In most cases, these groups will be handled by a single form, to be signed by a designated group leader or representative. The remaining visitor rules apply to each visitor within the group. The group leader will provide a list of names to front desk personnel for instances of emergency evacuation and accountability of each visitor while on agency premises.

Authorized Physical Access:

Only authorized personnel will have access to physically secure non-public locations. The [NLCRPD] will maintain and keep current a 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 personnel with CJI physical and logical access must:

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

    a. 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 a direct responsibility to configure and maintain computer systems and networks with direct access to CJI.
    b. 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.
    c. Prior to granting access to CJI, the [NLCRPD] on whose behalf the contractor is retained shall verify identification via a state of residency and national fingerprint-based record check.
    d. Refer to the *CJIS Security Policy* for handling cases of felony convictions, criminal records, arrest histories, etc.

2. Complete security awareness training.

    a. All authorized [NLCRPD], Noncriminal Justice Agencies (NCJA) like city or county IT 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.
    b. Security awareness training will cover areas specified in the *CJIS Security Policy* at a minimum.

3. Be aware of who is in their secure area before accessing confidential data.

    a. Take appropriate action to protect all confidential data.
    b. Protect all terminal monitors with viewable CJI displayed on a monitor and not allow viewing by the public or escorted visitors.

4. Properly protect and do not share any individually issued keys, proximity cards, computer account passwords, etc.

    a. Report loss of issued keys, proximity cards, etc. to authorized agency

personnel.

b. If the loss occurs after normal business hours, or on weekends or holidays, personnel are to call the [NLCRPD] POC to have authorized credentials like a proximity card de-activated and/or door locks possibly rekeyed.

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

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

6. Web usage—allowed versus prohibited, monitoring of user activity. (allowed versus prohibited is at the agency's discretion)

7. Do not use personally owned devices on the [NLCRPD] computers with CJI access. (Agency discretion).

8. Use of electronic media is allowed only by authorized [NLCRPD] personnel. Controls shall be in place to protect electronic media and printouts containing CJI while in transport. When CJI is physically moved from a secure location to a non-secure location, appropriate controls will prevent data compromise and/or unauthorized access.

9. Encrypt emails when electronic mail is allowed to transmit CJI-related data as such in the case of Information Exchange Agreements.

   a. (Agency Discretion for allowance of CJI via email)
   b. If CJI is transmitted by email, the email must be encrypted, and the email recipient must be authorized to receive and view CJI.

10. Report any physical security incidents to the [NLCRPD]'s LASO including facility access violations, loss of CJI, loss of laptops, Blackberries, thumb drives, CDs/DVDs, and printouts containing CJI.

11. Properly release hard copy printouts of CJI only to authorized vetted and authorized personnel in a secure envelope and shred or burn hard copy printouts when no longer needed. Information should be shared on a "need-to-know" basis. (See Sanitization and Destruction Policy)

12. Ensure data centers with CJI are physically and logically secure.

13. Keep appropriate [NLCRPD] security personnel informed when CJI access is no longer needed. In the event of ended employment, the individual must surrender all property and access managed by the local agency, state, and/or federal agencies.

14. No use of food or drink around information technology equipment.

15. Know which door to use for proper entry and exit of the [NLCRPD] and only use marked alarmed fire exits in emergency situations.

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

Roles and Responsibilities: Terminal Agency Coordinator (TAC)

The TAC serves as the point of contact at the [NLCRPD] for matters relating to CJIS information access. The TAC administers CJIS systems programs within the agency and oversees the agency's compliance with FBI and state CJIS systems policies.

Local Agency Security Officer (LASO)

Each LASO shall:

1. Identify who is using the CSA (state) 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 this policy.

4. Ensure the approved and appropriate security measures are in place and working as expected. Support policy compliance and ensure the CSA ISO is promptly informed of security incidents.

5. Support policy compliance and ensure the CSA ISO is promptly informed of security incidents.

Agency Coordinator (AC)

An AC is a staff member of the Contracting Government Agency (CGA) who manages the agreement between the private contractor(s)/vendor(s) and the [NLCRPD]. A CGA is a government agency, whether a Criminal Justice Agency (CJA) or a NCJA, that enters into an agreement with a private contractor/vendor subject to the CJIS Security Addendum. The AC shall be responsible for the supervision and integrity of the system, training and continuing education of private contractor/vendor employees and operators, scheduling of initial training and

testing, certification testing, and all required reports by NCIC.

CJIS System Agency Information Security Officer (CSA ISO)
The CSA ISO shall:

1. Serve as the security point of contact (POC) to the FBI CJIS Division ISO.

2. Document technical compliance with the CJIS Security Policy with the goal to assure the confidentiality, integrity, and availability of criminal justice information to the user community throughout the CSA's user community, including the local level.

3. Document and provide assistance for implementing security-related controls for the Interface Agency and its users.

4. ISOs have been identified as the POC on security-related issues for their respective agencies and shall ensure LASOs institute the CSA incident response reporting procedures at the local level. Establish a security incident response and reporting procedure to discover, investigate, document, and report to the CSA, the affected criminal justice agency, and the FBI CJIS Division ISO major incidents that significantly endanger the security or integrity of CJI.

Information Technology Support

In coordination with the above roles, all vetted IT support staff will protect CJI from compromise at the [NLCRPD] by performing the following:

1. Protect information subject to confidentiality concerns—in systems, archived, on backup media, and until destroyed. Know where CJI is stored, printed, copied, transmitted, and planned end of life. CJI is stored on laptops, mobile data terminals (MDTs), computers, servers, tape backups, CDs, DVDs, thumb drives, RISC devices, and internet connections as authorized by the [NLCRPD]. For agencies that submit fingerprints using Live Scan terminals, only Live Scan terminals that receive CJI back to the Live Scan terminal will be assessed for physical security.

2. Be knowledgeable of required [NLCRPD] technical requirements and policies taking appropriate preventative measures and corrective actions to protect CJI at rest, in transit, and at the end of life.

3. Take appropriate action to ensure maximum uptime of CJI and expedited backup restores by using agency-approved best practices for power backup and data backup means such as generators, backup universal power supplies on CJI-based terminals, servers, switches, etc.

4. Properly protect the [NLCRPD]'s CJIS system(s) from viruses, worms, Trojan horses, and other malicious code (real-time scanning and ensuring updated definitions).

    a. Install and update the antivirus on computers, laptops, MDTs, servers, etc.
    b. Scan any outside non-agency owned CDs, DVDs, thumb drives, etc., for viruses, if the [NLCRPD] allows the use of personally owned devices. (See the [NLCRPD] Personally Owned Device Policy)

5. Data backup and storage—centralized or decentralized approach.

    a. Perform data backups and take appropriate measures to protect all stored CJI.
    b. Ensure only authorized vetted personnel transport off-site tape backups or any other media that store CJI that is removed from a physically secured location.
    c. Ensure any media released from the [NLCRPD] is properly sanitized/destroyed. (See Sanitization and Destruction Policy)

6. Timely application of system patches—part of configuration management.

    a. The agency shall identify applications, services, and information systems containing software or components affected by recently announced software flaws and potential vulnerabilities resulting from those flaws.
    b. When applicable, see the [NLCRPD] Patch Management Policy.

7. Access control measures

    a. Address the least privilege and separation of duties.
    b. Enable event logging of:
        i. Successful and unsuccessful system log-on attempts.
        ii. Successful and unsuccessful attempts to access, create, write, delete, or change permission on a user account, file, directory, or other system resource.
        iii. Successful and unsuccessful attempts to change account passwords.
        iv. Successful and unsuccessful actions by privileged accounts.
        v. Successful and unsuccessful attempts for users to access, modify, or destroy the audit log file.

    c. Prevent authorized users from utilizing 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.

8. Account Management in coordination with TAC

    a. Agencies shall ensure that all user IDs belong to currently authorized users.
    b. Keep login access current, updated, and monitored. Remove or disable terminated or transferred or associated accounts.
    c. Authenticate verified users as uniquely identified.
    d. Prevent multiple concurrent active sessions for one user identification, for those applications accessing CJI, unless the agency grants authority based upon operational business needs.
    e. Do Not use shared generic or default administrative user accounts or passwords for any device used with CJI.
    f. Passwords

        i. Be a minimum length of eight (8) characters on all systems.
        ii. Not be a dictionary word or proper name.
        iii. Not be the same as the User ID.
        iv. Expire within a maximum of 90 calendar days.
        v. Not be identical to the previous ten (10) passwords.
        vi. Not be transmitted in clear or plaintext outside the secure location.
        vii. Not be displayed when entered.
        viii. Ensure passwords are only reset for authorized users.

9. Network infrastructure protection measures.

    a. Take action to protect CJI-related data from unauthorized public access.
    b. Control access, monitor, enabling, and updating configurations of boundary protection firewalls.
    c. Enable and update personal firewalls on mobile devices as needed.
    d. Ensure confidential electronic data is only transmitted on secure network channels using encryption and *advanced authentication when leaving a physically secure location. No confidential data should be transmitted in clear text. **Note: for interim compliance, and for the sole purpose of meeting the advanced authentication policy, a police vehicle shall be considered a physically secure location until September 30th, 2013. For the purposes of this policy, a police vehicle is defined as an enclosed criminal justice conveyance with the capability to comply, during operational periods.*
    e. Ensure any media that is removed from a physically secured location is encrypted in transit by a person or network.
    f. Not use default accounts on network equipment that passes CJI like switches, routers, and firewalls.

g. Make sure law enforcement networks with CJI shall be on their own network and accessible by authorized personnel who have been vetted by the [NLCRPD]. Utilize Virtual Local Area Network (VLAN) technology to segment CJI traffic from other noncriminal justice agency traffic to include other city and/or county agencies using the same wide area network.

10. Communicate and keep the [NLCRPD] informed of all scheduled and unscheduled network and computer downtimes, all security incidents, and misuse. The ultimate information technology management control belongs to [NLCRPD].

See Attachment C – CLEAN System Diagram

Front Desk and Visitor Sponsoring Personnel
Administration of the Visitor Check-In / Check-Out procedure is the responsibility of identified individuals in each facility. In most facilities, this duty is done by the Front desk or Reception Desk.

Prior to visitor gaining access to a physically secure area:

1. The visitor will be screened by the [NLCRPD] personnel for weapons. No weapons are allowed in the agency except when carried by authorized personnel as deemed authorized by the [NLCRPD].
2. The visitor will be screened for electronic devices. No personal electronic devices are allowed in any agency facility except when carried by authorized personnel as deemed authorized by the [NLCRPD].
3. Escort personnel will acknowledge being responsible for properly evacuating visitors in cases of emergency. Escort personnel will know appropriate evacuation routes and procedures.
4. Escort and/or Front desk personnel will validate visitor is not leaving the agency with any agency-owned equipment or sensitive data prior to Visitor departure.

All [NLCRPD] personnel and supporting entities are responsible to report any unauthorized physical, logical, and electronic access to the [NLCRPD] officials. For [NLCRPD], the point of contact to report any non-secure access **is defined in special order (S.O. 6.2.0.1).**

6.2.4 Discipline

In support of *[NLCRPD]*'s mission of public service to the city of/county of [city or county name] citizens, the *[NLCRPD]* provides the needed technological resources needed to personnel to access FBI CJIS systems and information in support of the agency's mission. All agency personnel, with access to FBI Criminal Justice

Information (CJI) or any system with stored FBI CJI, have a duty to protect the system and related systems from physical and environmental damage and are responsible for correct use, operation, care, and maintenance of the information.

All technology equipment: computers, laptops, software, copiers, printers, terminals, MDTs, mobile devices, live scan devices, fingerprint scanners, software to include RMS/CAD, operating systems, etc., used to process, store, and/or transmit FBI CJIS is a privilege allowed by *[NLCRPD]*, state CSO, and the FBI.

To maintain the integrity and security of the *[NLCRPD]*'s and FBI's CJIS systems and data, this computer use privilege requires adherence to relevant federal, state, and local laws, regulations, and contractual obligations. All existing laws and *[NLCRPD]* regulations and policies apply, including not only those laws and regulations that are specific to computers and networks but also those that may apply to personal conduct.

Misuse of computing, networking, or information resources may result in temporary or permanent restriction of computing privileges up to employment termination. In some misuse situations, account privileges will be suspended to prevent ongoing misuse while under investigation. Additionally, misuse can be prosecuted under applicable statutes.

All files are subject to search. Where follow-up actions against a person or agency after an information security incident involve legal action (either civil or criminal), the evidence shall be collected, retained, and presented to conform to the rules for evidence laid down in the relevant jurisdiction(s). Complaints alleging misuse of *[NLCRPD]*'s computing and network resources and FBI CJIS systems and/or data will be directed to those responsible for taking appropriate disciplinary action.

A. Examples of Misuse with access to FBI CJI

1. Using someone else's log-in who is not the owner.

2. Leaving the computer logged in with your login credentials unlocked in a physically un-secure location allows anyone to access *[NLCRPD]* systems and/or FBI CJIS systems and data in your name.

3. Allowing unauthorized persons to access FBI CJI at any time for any reason. Note: Unauthorized use of the FBI CJIS systems is prohibited and may be subject to criminal and/or civil penalties.

4. Allowing remote access of *[NLCRPD]* issued computer equipment to FBI CJIS systems and/or data without prior authorization by *[NLCRPD]*.

5. Obtaining a computer account that you are not authorized to use.

6. Obtaining a password for a computer account of another account owner.

7. Using the *[NLCRPD]*'s network to gain unauthorized access to FBI CJI.

8. Knowingly performing an act that will interfere with the normal operation of FBI CJIS systems.

9. Knowingly propagating a computer virus, Trojan horse, worm, and malware to circumvent data protection or compromise existing security holes in FBI CJIS systems.

10. Violating terms of software and/or operating system licensing agreements or copyright laws.

11. Duplication of licensed software, except for backup and archival purposes that circumvent copyright laws for use in *[NLCRPD]*, for home use or for any customer or contractor.

12. Deliberately wasting computing resources to include streaming audio, and videos for personal use that interferes with *[NLCRPD]* network performance.

13. Using electronic mail or instant messaging to harass others.

14. Masking the identity of an account or machine.

15. Posting materials publicly that violate existing laws or *[NLCRPD]*'s codes of conduct.

16. Attempting to monitor or tamper with another user's electronic mail or files by reading, copying, changing, or deleting without the explicit agreement of the owner.

17. Using *[NLCRPD]*'s technology resources to advance unwelcome solicitation of a personal or sexual relationship while on duty or through the use of an official capacity.

18. Unauthorized possession of, loss of, or damage to *[NLCRPD]*'s technology equipment with access to FBI CJI through unreasonable carelessness or maliciousness.

19. Maintaining FBI CJI or duplicate copies of official *[NLCRPD]* files in either manual or electronic formats at his or her place of residence or in other physically non-secure locations without express permission.

20. Using *[NLCRPD]*'s technology resources and/or FBI CJIS systems for personal or financial gain.

21. Deliberately failing to report promptly any known technology-related misuse by another employee that may result in criminal prosecution or discipline under this policy.

22. Using personally owned devices on *[NLCRPD]*'s network to include personally-owned thumb drives, CDs, mobile devices, tablets on Wi-Fi, etc. Personally owned devices should not store *[NLCRPD]* data, State data, or FBI CJI.

The above listing is not all-inclusive and any suspected technology resource or FBI CJIS system or FBI CJI misuse will be handled by NLCRPD on a case-by-case basis. Activities will not be considered misuse when authorized by appropriate NLCRPD officials for security or performance testing.

B. Privacy Policy

1. All agency personnel utilizing agency-issued technology resources funded by *[NLCRPD]* expressly acknowledge and agree that such service, whether for business or personal use, shall remove any expectation of privacy.
2. Use of *[NLCRPD]* systems indicate consent to monitoring and recording.
3. The *[NLCRPD]* reserves the right to access and audit any and all communications including electronic and physical media at rest, in transit and at the end of life.
4. *[NLCRPD]* personnel shall not store personal information with an expectation of personal privacy that is under the control and management of *[NLCRPD]*.

C. Personal Use of Agency Technology

1. The computers, electronic media, and services provided by *[NLCRPD]* are primarily for business use to assist personnel in the performance of their jobs. Limited, occasional, or incidental use of electronic media (sending or receiving) for personal, non-business purposes is understandable and acceptable, and all such use should be done in a manner that does not negatively affect the systems' use for their business purposes. However, employees are expected to demonstrate a sense of responsibility and not abuse this privilege.

D. Misuse Notification

Due to the increase in the number of accidental or malicious computer attacks against both government and private agencies, *[NLCRPD]* shall:

(i) Establish an operational incident handling capability for all information systems with access to FBI CJIS systems and data. This includes adequate preparation, detection, analysis, containment, recovery, and user response activities.

(ii) Track, document, and report incidents to appropriate agency officials and/or authorities. ISOs have been identified as the POC on security-related issues for their respective agencies and shall ensure LASOs institute the CSA incident response reporting procedures at the local level.

E. Penalties:

Violation of any of the requirements in this section by any authorized personnel will result in suitable disciplinary action, up to and including loss of access privileges, civil and criminal prosecution and/or termination.

Violation of any of the requirements in this section by any visitor can result in similar disciplinary action against the sponsoring employee and can also result in termination of services with any associated consulting organization or prosecution in the case of criminal activity.

6.2.5 Records maintenance, dissemination, and destruction.

A. Business Records and Correspondence

1. Business records and correspondence related to the business of administering the Department shall be considered confidential and proprietary to the Department, except to the extent that same constitute a part of the "public record" as defined in the Pennsylvania right-to-know statute, 65 P.S. Sec. 66.1 et seq. Copies of these records and correspondence shall not be provided to any persons requesting same, except the other parties to the transaction or correspondence, without the prior approval of the Chief of Police.

2. The "public record" as defined in 65 P.S. Sec. 66.1 is as follows:
Any account, voucher or contract dealing with the receipt or disbursement of funds by an agency or its acquisition, use or disposal of services or of supplies, materials, equipment or other property and any minute, order or decision by an agency fixing the personal or property rights, privileges, immunities, duties or obligations of any person or group of persons: Provided, That the term 'public records' shall not mean any report, communication or other paper, the publication of which would disclose the institution, progress or result of an investigation undertaken by an agency in the performance of its official duties, except those reports filed by agencies pertaining to safety and health in industrial plants; it shall not include any records, document, material, exhibit, pleading, report, memorandum or other paper, access to or the publication of which is prohibited, restricted or forbidden by statute law or order or decree of court, or which would operate to the prejudice or impairment of a person's reputation or personal security, or which would result in the loss by the Commonwealth or any of its political subdivisions or commissions or State or

municipal authorities of Federal funds, excepting there fromhowever the record of any conviction for any criminal act."

3. Documents constituting the "public record" shall be made available for inspection by any citizen at reasonable times, such as regular office hours.

4. Citizens shall be entitled to make copies of documents constituting the "public record", subject to bear the direct and indirect costs of such activities and subject to such other reasonable rules as may be established by the Chief of Police.

B. Criminal Records

1. Governing Law

The dissemination of criminal records and information shall be governed by the provisions of the Criminal History Record Information Act, 18 Pa.C.S. Ch. 91, as may be amended from time to time, and supplemented by this policy.

2. Dissemination of Criminal Records

a. Criminal History Record Information shall not be distributed to any non-law enforcement individual or non-criminal justice agency at any time.

Exception: Title.18 Sec.1. Chap.91 Criminal History record information, providing for crime victim right of access. (See section 6.2.5 B,2,m of this policy)

b. Criminal History Record Information may be distributed to law enforcement agencies and/or personnel for legitimate law enforcement purposes. A record of the dissemination shall be maintained indicating the purpose of release.

c. The LASO will be designated as the Intelligence Officer and will be responsible for the classification, computerization, and dissemination of all “protected information” classified in CHRIA. The LASO may designate other members of the Department to perform this duty on an as-needed basis upon approval from the Chief of Police.

d. No fee shall be charged to a criminal justice agency for such information, nor shall a fee be charged to recruiting officers of the Armed Forces, the Pennsylvania Civil Service Commissioner, or the Governor’s Office of Budget & Administration.

e. Before release of Incident Reports and/or incident related documentation, to

a non-law enforcement individual and/or non-criminal justice agency, all Criminal History Record Information shall be extracted from the record.

f. The expungement of Criminal History Record Information shall be governed by the provisions of 18 Pa. C.S. Sec. 9122, as amended.

g. The destruction of criminal records shall be governed by the record retention and destruction policy contained elsewhere in the Guidebook, as established by resolution of the NLCRPC Board.

h. Collection of protected information by the Department will be done in its automated system only when the following conditions are met.

(1) Information concerns an individual or group which it reasonably suspects of criminal activity.

(2) Information is related to criminal activity that would give use to prosecution for a state offense graded a misdemeanor or felony or for a federal offense for which a penalty is imprisonment for more than one year.

(3) Intelligence information is not collected in violation of state law.

i. Security of protected information will be maintained by ensuring that only those authorized to access protected information are electronically coded or otherwise designated to enter the automated system. A copy of the authorization list will be maintained by the Intelligence Officer or designee. Following department security and maintenance policy to reasonably protect the repository from theft, sabotage, and man-made or natural disasters. Properly selecting, supervising, and training personnel authorized to have access to protected information. There will be three different levels of storage of protected information established for reliability and sensitivity.

(1) Level I - will include all information that has been received froma reliable source and is substantiated.

(2) Level II - will include all information that has been received froma reliable source but is unsubstantiated.

(3) Level III - will include all information that has been received froman unreliable source and is not and cannot be substantiated.

j. Dissemination of protected information by the department's Intelligence Officer or designee may only occur if the following conditions are met.

(1) Requesting criminal justice agency must certify that it hasadopted policies and procedures consistent with this Act. This may be a verbal certification if the agency is known to Intelligence Officer or designee. In the event that agency is unknown, a signed statement of certification will be required before release of information.

(2) Intelligence Officer or designee records on the designated formthe

pertinent information for a proper audit trail of disseminated, protected information. This record is to be maintained separate from the individual's file.

(3) Protected information has been determined to be reliable.

(4) Requesting criminal justice agency justifies its request based on name, fingerprints, modus operandi, genetic typing, voice print or other identifying characteristics.

(5) Intelligence officer or designee lists on the individual's file the date, the purpose, and agency requesting the information.

(6) in the event the Intelligence Officer or designee becomesaware of/by any means that previously disseminated information is misleading, obsolete, and/or unreliable, the information is to be corrected and the recipient agencies notified of the change within a reasonable time period. Notification of correction or change made to agencies must be documented on the dissemination log (Attachment B)

(7) Protected information in the department's possession but whichwas not obtained through our sources may not be disseminated to another agency except if requesting agency and our department are investigating or prosecuting a criminal matter jointly. The Intelligence Officer or designee must, however, refer the requesting agency to the agency which was the source of the information.

(8) Intelligence Officer or designee when requesting protected information from another agency must certify, in writing, thatthis department complies with CHRIA (Attachment A).

k. Protected information will be maintained and will be purged only with the written approval from the Chief of Police and only under the following conditions:

(1) Data is no longer relevant or necessary to meet the goals and objectives of this agency.

(2) Data is obsolete, making it unreliable for present purposes and updating it would be worthless.

(3) Data cannot be used for strategic or tactical purposes associated with the duties of this agency.

l. All CHRIA information will be stored in the NLCRPD Records Section. The only exception to this policy will be the collection, possession, and temporary storage of CHRIA information during an officer's scheduled duty tour and/or scheduled court appearances.

m. **Crime Victims: Title.18 Sec.1. Chap.91 Criminal History record information, providing for crime victim right of access.**

(1) General Rule

i. A requesting party may request the dissemination of criminal history investigative information that is directly related to a civil action pending in a court in this Commonwealth (PA).

ii. A crime victim OR THE CRIME VICTIM'S REPRESENTATIVE may request the dissemination of criminal history investigative information that is material and necessary to the investigation or preparation of a civil action IN THIS COMMONWEALTH (PA).

(2) Request(s) for dissemination shall include:

i. An unsworn statement by the requesting party or party's legal representation. (Subject to penalties of section 4904 - falsification to authorities).
ii. Be directly related to a civil action pending in PA.
iii. Be material and necessary for the investigation or preparation of the civil action in PA.
iv. Shall identify or describe the information sought.
v. Be served on the records information officer (LASO) or Chief of Police in person or by certified mail with receipt.

(3) Dissemination:

i. Shall be completed within 60 days of receipt of the request. (Or by the date returnable on the request, whichever is later).
ii. The NLCRPD shall impose (reasonable) fees for associated costs in conjunction with the NLCRPD fee structure for the dissemination of records.

(4) Denial of request: The NLCRPD shall deny a request for dissemination:

i. Absent reasonable redactions, the information requested endangers a person or public safety, adversely affects an investigation or ongoing prosecution, or relates to a law enforcement's use of confidential informants or discloses investigative techniques or procedures.
ii. The criminal history is <u>not</u> directly related to a civil action pending in a PA court, or material and necessary to the investigatory civil action.
iii. Dissemination of the information would identify a third-party victim of child abuse, domestic violence, or sexual abuse (unless prevented through redaction).

(5) Service of denial: In the event request for dissemination for criminal history is denied on the grounds listed in (4), the NLCRPD shall:

i. Serve a denial in writing to the requesting party within 60 days of the request and identify the grounds for the denial.
ii. Judicial Review: A requesting party may file a petition for review appealing the denial before the court of common pleas. The appeal must be filed within 45 days of service of the denial.

(6) Redactions and or information <u>not to be disseminated</u> under this section:

i. Grand Jury investigative materials
ii. Medical, mental health, or treatment information
iii. Materials protected by 42. Pa.C.S. Ch. 63 related to juvenile matters.
iv. Materials subject to 42. Pa.C.S. Ch. 67A related to recordings by law enforcement. (BWC/MVR)
v. Other information is prohibited or protected by Federal or state law.
vi. A person's social security number
vii. A person's driver's license number
viii. Personal financial information
ix. A person's home or cell phone number
x. A person's email address, employee number, or other person ID information.

3. <u>Motor Vehicle Accident Reports/Investigations</u>

a. Distribution of accident reports/investigations shall be governed by the Motor Vehicle Code, 75 Pa. C.S.A. Sec. 3750 as amended hereafter. Copies of same shall be provided upon written request only to the federal government, branches of the military service, Commonwealth agencies, agencies of other states and nations and their political subdivisions, attorneys or insurers of accident participants who offer written verification of their representation of the participant, and the accident participants themselves, unless the participant has been charged criminally in connection with the accident, in which case copies of same will not be provided unless required by the Pennsylvania Rules of Criminal Procedure.

b. The maximum charge permitted by law shall be made for the cost of copying and providing such vehicle accident reports/investigations. At the present time, this fee is $15.00. There may be an additional charge as determined by the Chief of Police or his designee and is subject to review from time to time and on a case-by-case basis, i.e., an accident investigated by a deconstructionist.

6.2.6 Use and dissemination of Penn DOT Images

A. Disseminations of Penn DOT images may only be used for posting on social media or press under the following limited circumstances:

1) The individual has an active warrant for their arrest (minors excluded in NLCRPD utilization unless exigent circumstances apply)
2) The individual is deemed as a missing person and meets criteria for NCIC entry.

B. Recalls and Destruction requirements specify the NLCRPD officer / agency is ***required*** to contact all social media and press outlets to whom theimage was disseminated whenever one or more of the following requirements exist:

1) The wanted individual has been apprehended.
2) The warrant has been canceled.
3) The person has been found / located.

C. Dissemination Log Requirement requires that NLCRPD officers completeand file a dissemination log for all Penn DOT images**.** Minimum requirements include the following:

1) Five-year mandatory NLCRPD agency retention period (DPPA – 18 U.S.C. § 2721).
2) Availability of forms on JNET website.
3) Availability of forms **(See "Attachment B")**
4) Completion of all required blocks of information including.
    a) Social media distribution
    b) Press distribution.
    c) Recall efforts.
    d) Destroy efforts.
5) Procedures for removal of Facebook posts, or tweets, etc. are available via Google search.
6) Be certain to log all efforts and actions.

D. Misuse Penn DOT photographs are NOT PERMITTED to be used or disseminated to any media outlet or social networking site for:

1) Arrest reporting – NLCRPD officers shall not export or utilize any PENNDOT image for population of arrest or booking reports, these images must be imported from JNET or CPIN.
2) Found person reporting.
3) Deceased individual reporting.

4) Conviction, sentencing, and appeal reporting.

E. Other Unauthorized activities and practices, Penn DOT retains exclusive ownership of all driver records including photographs. The following acts are prohibited:

1) To combine or link data to/on any other database except as may be required by law.
2) To electronically store Penn DOT photographs outside of the Official Penn DOT Repository (this includes as prohibited storage venues) :
    a) RMS systems
    b) Email
    c) SMS messages
    d) Hard disk drives
    e) Smart phones
    f) Other media
    g) Use of Penn DOT images for photo identification badges.

F. Sanctions for misuse of Penn DOT could include the flowing limitations on all source forms of access to Penn DOT data: (JNET, and or 911 and or viaCLEAN)

1) Short term suspension.
2) Long term suspension.
3) Up to 1-year suspension of general access to JNET.
4) Permanent loss of access to JNET resources.
5) Civil litigation and fines.

6.2.7 Destruction of obsolete, retired, unusable, or otherwise discarded CJIS components and authorized disposal vendors.

The NLCRPD adheres to the practice of the utilization of approved vendors for services associated with the component destruction function. These vendors adhere to the best industry practices associated with this policy.

1) Equipment containing storage media with embedded Criminal Justice Data shall be subject to the specific handling requirements upon removal from the NLCRPD RMS or other interfaced criminal justice restricted networks.

2) Storage media shall be retained in a secure storage environment located in the secured portion of the Support Services Unit Supervisor.

3) Items shall be within the control of a sworn NLCRPD staff member from the time of removal from secure storage until final destruction and disposition is witnessed by the designated agency member.

4) A record of destruction of the hardware shall be retained by the support services supervisor / agency JTAC. The record shall contain information related to the destruction of the device and is required to be witnessed by at least one additional person **(see "Attachment A).**

5) Authorized disposal vendors
   - MOOREFIELD COMMUNICATIONS

6.2.8 Cyber Security Incident Response.

I. Scope of requirements

This section applies to every individual—contractor, private entity, noncriminal justice agency representative, or member of a criminal justice entity—with access to, or who operate in support of, criminal justice services and information This policy applies to all *[NLCRPD]* employees, contractors, temporary staff, and other workers at *[NLCRPD]*, with access to FBI CJIS systems and/or data, sensitive and classified data, and media. This policy applies to all equipment that processes, stores, and/or transmits FBI CJI and classified and sensitive data that is owned or leased by *[NLCRPD]*.

II. Policy

All users of the NLCRPD automated data systems shall adhere to this policy.

III. Procedures

An incident, as defined in National Institute of Standards and Technology (NIST) Special Publication 800-61, is a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard computer security practices. An incident response capability is necessary for rapidly detecting incidents, minimizing loss and destruction, mitigating the weaknesses that were exploited, and restoring computing services.

A. RESPONSIBILITIES:

1) Individual Information Technology User:

All users of NLCRPD computing resources shall be aware of what constitutes a cyber security incident and shall understand incident reporting procedures.

Information Services Division (ISD) (Moorefield Communications) Provide incident response support resources that offer advice and assistance with handling and reporting of security incidents for users of ISD information systems. Incident response

support resources may include, for example, the ISD Help Desk, a response team (described below), and access to forensics services.

Establish a Cyber Security Incident Response Team (CSIRT) to ensure appropriate response to cyber security incidents. The CSIRT shall consist of members of the State IT Security Council and key personnel from other agencies as required. CSIRT responsibilities shall be defined in the Cyber Security Incident Reporting Procedures.

B. Agency Management, Information Technology Organization:

1) Private Vendors
2) Other Authorities

Develop organizational and system-level cyber security incident response procedures to ensure management and key personnel are notified of cyber security incidents as required. Organizations that support information systems shall develop incident response plans and/or procedures that:

1) Provides the organization with a roadmap for implementing its incident response capability.
2) Describes the structure and organization of the incident response capability.
3) Provides a high-level approach for how the incident response capability fits into the overall
4) organization
5) Meets the unique requirements of the organization, which relate to mission, size, structure, and
6) functions
7) Defines reportable incidents.
8) Provides metrics for measuring the incident response capability within the organization.
9) Defines the resources and management support needed to effectively maintain and mature an incident response capability.

10) Is reviewed and approved by designated officials within the organization.

a. Review incident response plans and procedures at least annually.
b. Revise the incident response plan/procedures to address system/organizational changes or problems encountered during implementation, execution, or testing.

c. Distribute copies of the incident response plan/procedures to incident response personnel.

d. Communicate incident response plan/procedure changes to incident response personnel and other organizational elements as needed.

e. Provide incident response training to information system users consistent with assigned roles and responsibilities before authorizing access to the information system or performing assigned duties,

f. when required by information system changes; and annually thereafter.

g. Organizations shall test the incident response capability for the information systems they support at least annually.

h. Use organization-defined tests and/or exercises to determine incident response effectiveness. Document the results.

i. Organizations that support information systems shall implement an incident handling capability for cyber security incidents that includes preparation, detection and analysis, containment, eradication, and recovery.

j. Coordinate incident handling activities with contingency planning activities.

k. Incorporate the lessons learned from prior and ongoing incident handling activities into incident response procedures, training, and testing/exercises.

l. Track and document information system security incidents. Retain and safeguard cyber security incident documentation as evidence for investigation, corrective actions, potential disciplinary actions, and/or prosecution.

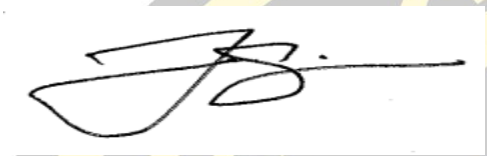
m. Promptly report cyber security incident information to appropriate authorities in accordance with State, Federal, or organization incident reporting procedures.

n. Organizations that support information systems shall provide an incident response support resource integral to the organizational incident response capability that offers advice and assistance to users of the information system for the handling and reporting of security incidents.

o. Possible implementations of incident response support resources in an organization include a help desk or an assistance group and, when required, access to forensics services.

Effective: September 17, 2024

By order of



Joshua P. Kilgore
Chief of Police

Attachments:

A – 6.2.7 Record of Destruction

B – 6.2.6 Dissemination Log

C – 6.2.3 System Diagram

S.O. 6.2.0.1 – Designation and Assignment of NLCRPD Agency Intelligence Officer

Attachment A: 6.2.7 Record of Destruction of obsolete, retired, unusable, or otherwise discarded CJIS components.

Date of removal of service:

Storage location:

Date of destruction:

Time:

Service Tag Number:

Hard drive number:

Method of destruction

- ☐ Drilling of multiple holes
- ☐ Application of magnet
- ☐ Shredded by vendor

Destroyed by: Signature:

Witnessed by: Signature:

ATTACHMENT B

6.2.0 Attachment B

PennDot Secondary Dissemination Log

Date	Subjects Name	Given to	Released By	Reason for dissemination	Information disseminated	PennDot photo for press release
		☐ MDJ ☐ Other ________		☐ Arraignment ☐ Other ________________	☐ Certified OLN ☐ Certified Reg.	☐ YES ☐ NO
		☐ MDJ ☐ Other ________		☐ Arraignment ☐ Other ________________	☐ Certified OLN ☐ Certified Reg.	☐ YES ☐ NO
		☐ MDJ ☐ Other ________		☐ Arraignment ☐ Other ________________	☐ Certified OLN ☐ Certified Reg.	☐ YES ☐ NO
		☐ MDJ ☐ Other ________		☐ Arraignment ☐ Other ________________	☐ Certified OLN ☐ Certified Reg.	☐ YES ☐ NO
		☐ MDJ ☐ Other ________		☐ Arraignment ☐ Other ________________	☐ Certified OLN ☐ Certified Reg.	☐ YES ☐ NO
		☐ MDJ ☐ Other ________		☐ Arraignment ☐ Other ________________	☐ Certified OLN ☐ Certified Reg.	☐ YES ☐ NO
		☐ MDJ ☐ Other ________		☐ Arraignment ☐ Other ________________	☐ Certified OLN ☐ Certified Reg.	☐ YES ☐ NO
		☐ MDJ ☐ Other ________		☐ Arraignment ☐ Other ________________	☐ Certified OLN ☐ Certified Reg.	☐ YES ☐ NO
		☐ MDJ ☐ Other ________		☐ Arraignment ☐ Other ________________	☐ Certified OLN ☐ Certified Reg.	☐ YES ☐ NO
		☐ MDJ ☐ Other ________		☐ Arraignment ☐ Other ________________	☐ Certified OLN ☐ Certified Reg.	☐ YES ☐ NO

6.2.0 Criminal Justice Information and Criminal History Records – 2/26/21

ATTACHMENT C – Clean System Diagram