


|   |                   |   |   |
|---|-------------------|---|---|
| <b>ELIZABETH POLICE DEPARTMENT<br/>GENERAL ORDERS</b>                                   |                   |   |  |
| <b>VOLUME: 5</b>  | <b>CHAPTER: 5</b> | <b># OF PAGES: 28</b>   |   |
| <b>SUBJECT: RECORDS ACCESS AND SECURITY</b>   |                   |   |   |
| <b>EFFECTIVE DATE:</b><br><div style="text-align: center;"><b>October 1, 2025</b></div> |                   | <b>ACCREDITATION STANDARDS:</b><br>1.8.1, 1.8.2<br>(NJSACOP LEAP)<br>82.1.1, 82.1.2,<br>(CALEA LE1)<br>(NJCOMS) |   |
| <b>BY THE ORDER OF:</b><br>Chief Giacomo Sacca  |                   |   |   |
| <b>BY AUTHORITY OF:</b><br>Police Director Earl J. Graves                               |                   |   |   |
| <b>SUPERSEDES ORDER #:</b>  |                   |   |   |

**PURPOSE:** The purpose of this directive is to establish and maintain policy and procedures concerning access to and the security of reports and records of this agency, including the use of the field reporting system.

**POLICY:** The records function is necessary to accomplish the Elizabeth Police Department's mission. Therefore, this agency's policy is to maintain accurate and efficient reporting of all activity within the agency's jurisdiction. This agency shall comply with all mandated reporting requirements of the federal government and the State of New Jersey while strictly adhering to the public records law. Furthermore, this agency will protect all agency records, including electronic records and access to shared databases, from unauthorized access, intrusion, theft, destruction, or misuse.

## PROCEDURES:

### I. DEFINITIONS

- A. Cloud Services: Applications and computing resources made available on the internet.
- B. Confidential Record: A public record that contains personal data or other sensitive information which access is restricted.
- C. Criminal Justice Information (CJI): Criminal Justice Information Services (CJIS) data provided for law enforcement agencies to use, including but not limited to biometric, identity history, person, organization, property, and case/incident history data.
- D. Cyber Extortion Threat: A threat against the agency's IT infrastructure, data systems, or other digital assets designed to:
  - 1. Disrupt operations.
  - 2. Alter, damage, or destroy data.
  - 3. Use the network to generate and transmit malware.
  - 4. Deface the official websites, social media, or other public-facing internet outlets.
  - 5. Access personally identifiable information, protected health information, or confidential information stored on the network made by a person or group, whether acting alone or in collusion with others, demanding payment or a series of payments in consideration for the elimination, mitigation, or removal of the threat.
- E. Cyber Incident: A malicious or suspicious event occurring on or conducted through a computer network that jeopardizes the integrity, confidentiality, or availability of an information system or the information the system processes, stores, or transmits. It may be represented by a cyber security breach, cyber extortion threat, data breach, or other cyber events that may include:
  - 1. Attempts from unauthorized sources to access systems or data.
  - 2. Unplanned disruption to a service or denial of service.
  - 3. Unauthorized processing or storage of data.
  - 4. Unauthorized changes to system hardware, access rights, firmware, or software.
  - 5. The presence of a malicious application, such as ransomware or a virus.

- 6. Presence of unexpected/unusual programs.
- 7. Non-malicious or non-unauthorized failures or mistakes of your data, applications, systems, or network.
- F. Cyber Security Breach: Any unauthorized access to, use, or misuse of, modification to the network, and/or denial of network resources by attacks perpetuated through malware, viruses, worms, Trojan horses, spyware, adware, zero-day attack, hacker attack, or denial of service attack.
- G. Data Breach: The actual or reasonably suspected theft, loss, unauthorized acquisition of, or unauthorized access to data that has or may compromise the security, confidentiality, and/or integrity of personally identifiable information, protected health information, or confidential business information.
- H. Mobile Device: Any portable device used to access criminal justice information via a wireless connection (i.e., cellular, WiFi, Bluetooth, etc.)
- I. Public Record or Government Record: Any information that a public agency generates or receives in the transaction of its official duties as outlined in N.J.S.A. 47:1A-1 et seq.
- J. Security Breach: As used in this policy, means an indication of an intrusion, breach, or threat into the agency's central records system, computer system, IT network, or any component or subcomponent of these systems.

## **II. AGENCY RECORDS**

- A. The Records Section falls under the command of the Property and Services Bureau.
- B. The Chief of Police will assign a supervisor to oversee the Records Section of the Police Department. The records supervisor will be responsible for assisting the Records Custodian in complying with the Open Public Records Act regarding records stored with the police department.
- C. The State of New Jersey, Division of Revenue and Enterprise Services, Records Management Services (NJDORES) is the government organization tasked with providing municipalities with compliance information and training regarding public records.
- D. This agency is required by New Jersey law to protect public records.
- E. This agency maintains records in a system that is a combination of electronic records and paper-based records.
- F. The following measures shall be taken and adhered to control access to criminal and quasi-criminal records:

1. All personnel are responsible for maintaining the security and integrity of all records.
2. Access to files stored in the records area is restricted to authorized personnel only.
3. Official records are copied for official purposes only.
4. When personnel assigned to the Records Section are not present or are off duty, the records system shall be secured, protecting it from unauthorized access.
5. Once information from written records is entered into the in-house electronic records management system (RMS), the physical document(s) shall be promptly filed. All ancillary reports and documents shall be added to the electronic record in the RMS system. Ancillary reports and other documents may include handwritten forms, field notes, electronic fillable forms, or other items of record that are part of a case or incident and must be retained per this directive.
6. The agency maintains strict privacy and security precautions to ensure the integrity of official records and compliance with applicable laws. The established precautions include the following:
  - a. **Physical Records:** Access to the records filing system is restricted to records personnel.
    - 1) Other people may only be admitted into the records filing system in specific circumstances.
      - i. Personnel working on active cases in need of specific files and or records that are stored in hard copy format and are not available in RMS may access the records secure area when the Records Section is open.
      - ii. Records personnel have the authority to admit other people to the secure area, provided they are always under the direct supervision of the records personnel and must be in the area.
    - 2) Physical records that must be removed from the filing system for official purposes must be signed out through the records supervisor or designee.
    - 3) Original records released by the records supervisor must be returned as soon as their official purpose has been satisfied.

- b. **Electronic Records:** Electronic records are stored on network servers, records management systems, and in cloud services. Electronic records are partitioned into different levels of access and security.
    - 1) The level of access to electronic records is dependent on personnel assignment. Records may be partitioned based on division, unit, assignment, or other need-to-know factors.
    - 2) The Records Supervisor shall determine the appropriate access levels, groups, or other means based on the security settings of the network architecture, records management software, or cloud services.
  - c. **Copies or Printed Electronic Records:** Copies of records or printed copies of electronic records may be utilized by personnel in the field while conducting authorized duties. When no longer required for their official purpose, the copied records or printed electronic records shall be returned to the Records Section for proper disposal. At no time shall such records be disposed of in public areas, facilities, or other locations where the records can be subject to unauthorized retrieval or use.
- G. **After Hours Access:** When personnel assigned to the records management function are not present or are off duty, the records filing system shall be secured, protecting it from unauthorized access.
  - 1. Personnel requiring access to any reports may access the electronic versions of those reports as stored in the records management system. This access is limited to authorized people with the required records management system (RMS) permissions.
  - 2. In an after-hours emergency, where access to physical records is required, supervisors are authorized to access general records that are not accessible through RMS. Any record removed must be per this policy and returned immediately after use.
- H. **Extra Security Measures:** Extra security measures shall be taken to protect the following types of records:
  - 1. **Juvenile:** All juvenile records shall be secured from unauthorized access.
    - a. Juvenile records will be marked as such to be distinguishable from other records so that they may be protected from inadvertent release or the disclosure of information contained therein.
    - b. Juvenile records shall be generally retained for five years after the age of majority. The NJDRES-RMS records retention schedule shall be followed. In accordance with the records retention section of this

policy, no public record will be destroyed unless proper authorization has been received by NJDRES-RMS by using the approved State of New Jersey online records disposition request via the online Artemis Records Retention and Disposition Management System.

2. **Confidential Records:** All records of a confidential nature shall be marked as such and, depending on their sensitivity, may also be secured in a filing system separate or segregated from the general records management system as determined by the Chief of Police. Access to these files may be regulated to personnel on a need-to-know basis as determined by the Chief of Police. Such files shall be protected from unauthorized access. Confidential records may include:
  - a. Confidential Funds
  - b. Confidential Informants
  - c. Confidential investigations
  - d. Confidential operations
  - e. Early Warning System
  - f. Employee Assistance Program
  - g. Internal Affairs records/reports
  - h. Megan's Law Records
  - i. Underage Alcohol or Marijuana Warning Records
3. **Non-Public Personnel Records:** All non-public personnel records shall be stored securely in their separate filing system in a location determined by the Chief of Police.
  - a. Non-public personnel records may include:
    - 1) Employment application
    - 2) Personnel attendance records
    - 3) Personnel evaluation forms
    - 4) Commendations
    - 5) Promotion resolutions
    - 6) Educational transcripts

- 7) Disciplinary actions
  - 8) Letter of resignation
  - 9) Employee medical records
  - 10) Psychological records
  - 11) Any other pertinent information or material
- b. Securing and Accessing Non-Public Personnel Records
- 1) The Chief of Police shall ensure that all personnel and medical records folders are secured in a locked cabinet and shall only be available to authorized managerial and supervisory personnel on a need-to-know basis.
  - 2) Electronic personnel and medical records shall be protected from unauthorized access.
  - 3) Any employee may review their personnel file in the presence of the Chief of Police or designee upon two business days' notice. Notice shall be in writing.
  - 4) Authorized officials with access to the personnel and medical files or the information contained therein are obligated to keep all such information confidential and disclose such information as may be deemed necessary to other officials solely on a need-to-know basis.
  - 5) Medical information may be disclosed only to the extent described above or upon the employee's written authorization.
  - 6) Any violation of these requirements shall result in disciplinary action, including reprimand, suspension, and/or termination, depending on the severity of the violation.

### III. RELEASE OF AGENCY RECORDS

- A. **Discovery:** Information from the police department needed by defendants and/or their attorneys is available through discovery. All discovery requests shall be submitted, in writing, directly to the municipal prosecutor. The prosecutor must respond to such requests within ten days of their receipt.
1. The preparation of discovery is done by police department records personnel. Requests sent to the municipal court will be forwarded to and subsequently fulfilled by the record personnel once all requirements of the requesting party are satisfied (i.e., forms, payment, etc.).

2. No personnel other than records personnel are authorized to fulfill or otherwise release information from discovery requests.
3. Discovery requests shall be fulfilled in accordance with New Jersey Court Rule 7:7-1.

- B. **Open Public Records Act (OPRA) Release:** The New Jersey Open Public Records Act (OPRA) (N.J.S.A. 47:1A-1 et seq.) guarantees access to public records in the state in circumstances as defined by the law. Any release of a departmental record will be in accordance with OPRA or other applicable state laws, regulations, court rules, etc. This agency will not release information considered confidential or not included in OPRA.
- a. For any questions related to OPRA, the Government Records Council (GRC) operates a toll-free inquiry hotline to guide requestors of government records and records custodians regarding the Open Public Records Act (OPRA). The toll-free phone number is 1-866-850-0511.
  2. The Records Supervisor shall ensure that the Records Custodian is provided with all information, records, and support necessary to comply with any OPRA request.
  3. Under the New Jersey Open Public Records Act (N.J.S.A. 47:1A-1 et seq.) a government record that is otherwise publicly accessible may contain non-disclosable information that should be redacted. Words, sentences, paragraphs, or whole pages may be subject to redaction.
    - a. Any redaction shall be done so that the redacted information cannot be recovered. Improper redacting may allow information to bleed through to the final copy and be viewable to the requester.
      - 1) The redaction must be accomplished using a visually obvious method that shows the requester the specific location of any redacted material in the record.
      - 2) The use of "White-out" or other marking substantially similar in color to the document's background must be avoided to allow the requester to see the location of the redacted material.
      - 3) If full pages are to be redacted, the custodian should give the requester a visible indication that a particular page of that record is being redacted, such as a blank sheet bearing the words "Page redacted" or a written list of the specific page numbers being withheld. The purpose is to communicate formally to the requester, clarifying that the material was not provided.



- 4) If an electronic document is subject to redaction, such as a PDF, the redaction shall be made using the redaction feature of the software used to prepare the document. For example, most PDF creation software provides a tool for such a purpose to ensure the redacted information cannot be recovered.
- C. **Release through Court Order:** This agency shall abide by any court order to release information. Records personnel shall fill such requests and return them to the employee requesting them as soon as possible. All documents released under a court order shall be reviewed by the Chief of Police or designee before their release to make sure they comply with the court order.
- D. **Disclosure of Juvenile Information:** Social, medical, psychological, legal, and other records of the court and probation division and records of law enforcement agencies pertaining to juveniles charged as delinquent or found to be part of a juvenile-family crisis shall be strictly safeguarded from public inspection. The disclosure of Juvenile Information shall follow N.J.S.A. 2A:4A-60 and other applicable statutes and administrative codes.
- E. **Release or Disclosure of Personnel Records:** Information in an employee's personnel and medical records folders shall be deemed confidential and not released to the public or any third party without the employee's written consent.
1. The following information shall be deemed public information:
    - a. The employee's name, title, position, payroll record, length of service, date of separation from service, and reason, and the amount and type of pension they are receiving; and
    - b. Data contained in information that discloses conformity with specific experiential, educational, or medical qualifications required for government employment or for receipt of a public pension, but in no event shall detailed medical or psychological information be released.
    - c. Major discipline reporting information as required under New Jersey Attorney directive 2021-6.
  2. Internal affairs files and other applicable personnel records may be released to another law enforcement agency requesting such records during an employment background investigation so long as the requesting agency has provided a written acknowledgment to the releasing agency that it will maintain the confidentiality of said files following the Internal Affairs Policy and Procedure Manual (IAPP). If this agency receives such a request, copies of all internal investigative information related to that candidate will be immediately shared per N.J.S.A. 52:17B-247.

#### IV. EXPUNGEMENTS

- A. An expungement is the sealing, impounding, isolation, or removal of all records on file within any court, detention or correctional facility, law enforcement, criminal justice agency, or juvenile justice agency concerning a person's apprehension, arrest, detention, trial, or disposition of an offense within the criminal or juvenile justice system.
- B. Records personnel will conduct daily checks of the Expungement Portal within AOC's eCDR module and comply with any applicable Expungement Orders. Upon completion, the order status within the portal shall be changed to "Expunged."
- C. Expungement orders received by this agency shall be acted upon without delay.
- D. When this agency receives an electronic or paper expungement order, the Records Supervisor shall ensure the following action is taken:
  - 1. Locate all relevant records referenced or contained in the Expungement Order.
  - 2. Electronic records subject to an expungement order shall be isolated or partitioned per the expungement procedure established by the RMS vendor to ensure the records cannot be viewed, referenced, or utilized for any unauthorized purpose.
  - 3. Physical records subject to an expungement order shall be isolated and secure to prevent the records from being viewed, referenced, or utilized for any unauthorized purpose.
  - 4. Expunged records shall not be deleted, shredded, or obliterated. A record of the expunged case, including the Court order, shall be retained for legal and auditing purposes. Storage of such records shall be restricted to the Records custodian or designee and only accessed, reviewed, utilized, or released when authorized.
- E. Where expungement orders contain the names of other people not included in the order, the agency is not obligated to isolate or remove the records that include the names of the other persons. The original record may remain in the agency's general files, with the name(s) contained in the expungement order removed, obliterated, or deleted from those records.
- F. **Use of Expunged Records:** The custodian of records or designee may access, review, utilize, and/or release expunged records in the following circumstances:
  - 1. To ascertain whether the person has had a prior conviction expunged or sealed under prior laws or orders, and may supply information to the court when a motion is pending for a new expungement request.

2. To supply information to the Violent Crimes Compensation Office in conjunction with any claim that has been filed.
  3. When the access, review, or utilization of the expunged records is subject to a court order permitting the inspection of such records.
  4. When the court requests the records to determine whether to grant or deny a person's application for acceptance into a supervisory treatment or diversion program for subsequent charges.
  5. Any other use of expunged records permitted by law.
- G. Information on expunged records shall be revealed by the subject of the expungement order who is seeking employment with a law enforcement agency.
- H. Persons seeking to obtain copies of their own expunged and/or sealed records must apply to the Court for such release.

## **V. CYBERSECURITY AND PROTECTION OF DIGITAL ASSETS**

- A. An employee or a consultant shall be designated as a Network Administrator responsible for ensuring that all the procedures outlined in this policy and any other agency policy related to agency-owned computers and electronic equipment are followed.
- B. The use of all systems, devices, or applications capable of receipt, transmission, or disclosure of any criminal justice information (CJI) shall be in accordance with the latest version of the Criminal Justice Information Services (CJIS) Security Policy.
1. CJIS violations may be subject to criminal and/or civil penalties in addition to any departmental disciplinary actions.
- C. **Asset Management:** The Network Administrator shall maintain records and inventory of all network assets, including;
1. Maintaining an accurate and current network diagram.
  2. Maintaining an accurate and current inventory of hardware to include:
    - a. Workstations
    - b. End-user devices
    - c. Servers
    - d. WiFi Access Points

- e. Other assets connected to agency computer networks or capable of storing agency data.
- 3. Maintaining an accurate and current inventory of software to include:
  - a. Operating systems
  - b. Licensed applications
- D. **Data Storage and Management:** Digital data storage shall consist of all records in the records management system, data stored on the network server, cloud services, or other electronic means of electronic file storage.
  - 1. **Data Sensitivity:** Data containing personally identifiable information (PII), protected health information (PHI), or other Criminal Justice Information (CJI) (including police records, video, audio, etc.) shall be deemed confidential and access shall be protected from theft or unauthorized access through a combination of physical security and passwords or encryption.
  - 2. All data stored on agency networks, devices, or cloud services are the property of this agency.
    - a. Personally owned digital data shall not be stored in any agency electronic storage system.
  - 3. All data retained by this agency will be stored in a manner that complies with the hardware and software manufacturer's recommendations, current best practices in the IT field, the most recent version of the CJIS Security Policy, and applicable laws or regulations.
  - 4. Employees may be provided with a network storage location, cloud storage location, or other specific electronic storage areas. All files that need to be saved concerning your official duties must be saved on an agency's authorized network.
    - a. No agency-owned data or documents will be stored solely on end-user devices such as desktop computers, handheld devices, portable media devices, or any other device that is not included in the daily backup process and may be subject to loss.
      - 1) If portable media is required to transport, store, or use data outside of this agency, the original data shall be stored on a network device subject to the daily backup, and the use of such devices shall be consistent with this directive and the latest version of the CJIS Security Policy.
      - 2) Locations or devices containing PII, PHI, or CJI must be protected from theft. A password or other encryption must

protect any device containing such data to prevent unauthorized access. The data shall be sanitized from the device immediately after its authorized use.

5. Any off-site or cloud-based electronic storage services must comply with FBI CJIS security policies.
  6. The Network Administrator is responsible for keeping an accurate and current inventory of data storage, specifically data containing PII, PHI, and CJI. The inventory will include applications, systems, or locations where agency data is stored.
- E. **Data Backup:** The Network Administrator shall ensure data on all network systems are subject to a full backup at least weekly.
1. Backup data shall be stored off-site to protect against damage from fire, theft, water intrusion, or other means of accidental destruction.
  2. Data backups stored offsite shall be transmitted between the agency and the off-site facility on an encrypted Virtual Private Network (VPN) compliant with the current version of the CJIS Security Policy. Any off-site data storage facility vendor must be approved by the FBI to store and transmit criminal justice information (CJI).
  3. Incremental backups shall be scheduled daily.
- F. **System Physical Security:** Only authorized persons shall access agency computer systems and shared databases.
1. Data storage servers shall be physically secured, preventing unauthorized access. Access to physical servers shall be limited to authorized Information Technology Staff and personnel directly responsible for the Information Technology services of this agency.
  2. Access to locations where workstations or devices capable of accessing agency data shall be protected from use by unauthorized persons.
  3. When personnel are not using their computer or workstation, they will log off the system.
  4. At no time should an employee leave the computer or workstation unattended in a state where unauthorized personnel may use the computer or access agency data.
- G. **Access Security and Account Management:** The agency's computer systems shall control access to restricted information, network locations, data storage, or cloud-based storage based on the personnel assignment, job, or function in the agency.

1. Administrative access to servers, operating systems, cloud services, and other agency applications shall be restricted to only those individuals who require such access to manage those systems.
  2. Access levels and privileges for user accounts shall be restricted to the lowest level of access required for that user's assignment, job, or function relative to that system.
  3. Multi-factor Authentication shall be activated on all cloud-based applications where available.
  4. User accounts that remain inactive for 45 days shall be disabled.
  5. Supervisor shall review their subordinate's access to systems every six (6) months to ensure they have access appropriate to their function.
  6. Access rights to systems shall be updated upon personnel status changes. Employees who are suspended or terminated from employment shall have their access revoked on all agency systems immediately.
  7. Using any default accounts or passwords provided by any hardware or software provider is strictly prohibited and shall be disabled.
  8. The Network Administrator shall maintain an inventory of current accounts, including:
    - a. Users.
    - b. Administrators and Elevated Privilege Users.
    - c. Service Accounts.
    - d. Shared Accounts.
  9. **Visitor Control:** The agency shall control physical access to all areas where access to the agency's computer network is present. Visitors shall be escorted at all times and monitored while visiting this facility.
  10. All contractors and vendors performing work within the agency shall be escorted and monitored to ensure they do not access network servers, devices, access points, or other data sources. This does not apply to authorized Information Technology vendors conducting work as authorized by the NJSP CJIS Unit.
- H. **Password Protection:** Only appropriate personnel are given access to the office computers regardless of location, whether in the office or off-site on mobile systems. The electronic records management system has a password-protected access control system. Personnel shall change their Password for the records management system as determined by the system administrator.

1. The system shall lock a user account or access point for no less than 30 minutes after five (5) consecutive invalid access attempts by a user. An authorized network administrator may release this account lockout.
- I. **Password Strength and Security:** All networks with access to Criminal Justice Information (CJI), including all servers and client terminals (workstation computers), shall be secured by a username ID and password access control system that complies with the FBI CJIS Security Policy.
1. All personnel shall comply with the following password standards.
    - a. Expire within a maximum of ninety (90) calendar days.
    - b. Be a minimum of ten (10) characters on all systems.
    - c. Must contain both upper-case and lower-case characters.
    - d. Passwords must be unique from those used on all other programs, websites, devices, etc., both personal and work.
    - e. Not be the same as the User ID.
    - f. Not be identical to the previous ten (10) passwords.
    - g. Shall not contain sequential or repetitive characters of more than two in succession. Examples include: "123," "AAA," "987," etc.
    - h. Not be a dictionary word or proper name.
    - i. It should not be a commonly used password, such as those published on various "commonly used password lists:" (Full lists of commonly used passwords can be found in various cybersecurity reports.)
      - 1) NordPass's top 200 commonly used passwords
      - 2) NCSC.gov.uk top 10,000 commonly used passwords
    - j. Not be easy to memorize, such as:
      - 1) Names of your children or pets.
      - 2) Single words or phrases. (i.e. iloveyou)
      - 3) Dates or phrases that can easily be guessed or learned about you, such as anniversary dates, birthdays, children's birthdays, favorite sports teams, favorite bands, etc.

- k. It should not be context-specific, such as the application's name or website being logged into.
    - l. Not be transmitted in the clear outside the secure location. (Must be sent over an encrypted network connection)
    - m. Not be displayed when being entered.
  - 2. Passwords should be compared against a breach corpus or "blacklist" of unacceptable passwords by checking your username or email address against the list to ensure previously breached passwords are not used.
    - 1) [breachdirectory.org](https://breachdirectory.org)
  - 3. Passwords should never be written down or stored online (except in secure, encrypted password vaults).
  - 4. Passwords are not to be shared with anyone. They should be considered sensitive, confidential information belonging to the organization.
  - 5. Passwords should not be included in an email message or revealed to co-workers or family members.
  - 6. All servers and client terminals (computers) with access to CJI shall have their Windows password default settings configured by the Network Administrator to comply with FBI CJIS Security Policy requirements.
  - 7. Two-factor authentication shall be used when accessing any shared database or service where that level of authentication is available
- J. **Unauthorized Downloading:** Personnel shall not download or open any information from an unknown source. The Network Administrator must approve all software installed on agency devices.
- K. **Email System:** The agency shall provide official email services for personnel to use for official communications.
- 1. **Email Usage:** All employees shall use the official agency-provided email accounts for all official communications. Employees are prohibited from using unapproved email addresses or services on agency-owned devices.
  - 2. **Anti-Phishing Measures:** Phishing is sending emails that appear or purport from a reputable company or person to induce the receiver to reveal personal or agency information, such as passwords or other sensitive information. The network administrator shall implement anti-phishing measures to detect and mitigate any phishing attempt.
    - a. Measures may include email filtering solutions that identify and quarantine suspicious emails.



- b. All employees shall report any suspicious email believed to be a phishing attack to the network administrator.
- 3. **Anti-Malware and Anti-Spam:** Malware and spam significantly threaten the security of the agency's digital assets. Viruses, worms, or ransomware can infiltrate the agency's network through the email system. The Network Administrator shall ensure that malware and spam scanning measures are implemented. Such measures shall be enabled on the email server, and incoming messages shall be inspected to prevent malware or malicious content from reaching a user's inbox.
- 4. **Encryption:** Sensitive and confidential information sent or received via email shall be encrypted to ensure the content of those messages remains secure during the transmission and can only be seen or decrypted by the intended receiver.
- 5. Only fully supported web browsers and email clients may be used.
- 6. Emails from outside the agency shall be marked as such.
- L. **Endpoint Protection:** All agency-owned endpoint devices, including but not limited to computer workstations, laptops, tablets, mobile devices, and servers, shall have endpoint security software installed.
  - 1. **Endpoint Security Software:** The Network Administrator shall ensure the deployment of endpoint security software, including:
    - a. Antivirus Protection
    - b. Anti-Malware Protection
    - c. Firewalls
    - d. Endpoint Detection and Response Software or services.
  - 2. Endpoint protection software shall be reviewed and updated, if necessary, at least semi-annually.
  - 3. Autorun shall be disabled for all removable media.
  - 4. Microsoft Office applications shall be set to open downloaded files in "Protected Mode."
  - 5. All removable media will undergo a virus scan before permitting a connection or accessing files.
  - 6. The Network Administrator will ensure that any unused network ports are disabled.

7. Employees are responsible for ensuring their assigned device remains protected and is up to date. If an employee is unable to update the software or determines they are not capable of keeping the device protection running or up to date, they shall discontinue the use of the device and notify the Network Administrator as soon as practical.
- M. **Patch Management:** Software and hardware providers regularly deploy security patches or firmware updates to address known vulnerabilities. All operating and application software and infrastructure equipment shall be updated to the latest versions. Patches and firmware updates shall be installed based on risk and operational impact as soon as practicable.
1. Patches or firmware updates for high and critical vulnerabilities shall be completed within one month of release.
  2. For high and critical vulnerabilities that cannot be patched in a month, create an exception process that documents the vulnerability and plans to remediate or otherwise compensate for the risk.
  3. The use of software and hardware no longer being supported by the publisher or manufacturer, or reaching its end-of-life, is strictly prohibited. Such software or hardware shall be removed from service immediately after being notified of the end-of-life by the publisher or manufacturer.
- N. **Use of Mobile Devices:** The agency shall authorize, monitor, and control all remote access methods to agency data systems and shared databases.
1. Personally owned mobile devices or other remote access devices are not permitted to access the agency's network or CJI.
    - a. This prohibition does not apply to the access of agency web-based services that do not support access to CJI, such as scheduling software, email services, policy management systems, or other non-CJI services that may be authorized by the Chief of Police or other information systems that are intended for public access.
  2. Mobile devices used by employees for official business or can connect to agency accounts or networks must be capable of being encrypted and disabled, locked, or returned to the factory setting remotely if they should become lost or stolen.
  3. Any device or workstation that provides CJI through remote access owned and authorized by this agency shall comply with the most recent version of the CJIS Security Policy.
  4. A Virtual Private Network (VPN) and Multi-Factor Authentication (MFA) shall be used for all remote connections to agency network(s).

- O. **WiFi Access Points:** WiFi access is provided to agency members and guests throughout the facility. The Network Administration shall ensure the following controls to ensure the security of the WiFi system:
1. All WiFi access points shall be secured with WiFi Protected Access cryptographic algorithms.
  2. All access points shall be mounted or placed in areas that prevent unauthorized physical access to user manipulation.
  3. Ensure all access points have strong administrative passwords.
  4. Change the default SSID of all access points.
  5. Provide separate "guest" access for non-agency personnel who need internet access but are insulated from access to the agency's network data and CJI.
  6. Perform periodic testing to ensure a rogue access point or "pineapple" device is not present.
  7. Test the access point range boundaries to determine the extent of wireless coverage.
  8. Ensure all access points comply with the latest CJIS Security Policy.
- P. **Retirement of IT components:** No server, workstation, computer, hard drive, CD, DVD, cellular phone, portable media, or other remotely related electronic data storage device owned by this agency shall be released from custody and control of this agency until it can be cleared of all data and software and sanitize it in a way that no one will be able to retrieve any data from any type of storage device at any later date.
- Q. **Software Licensing:** All software installed on agency computers, workstations, or servers shall be properly licensed.
- R. **3rd Party Vendors:** All 3rd party vendors shall be vetted. Security, insurance, and other compliance requirements shall be verified before the execution or renewal of contracts.
1. A 3rd Party Risk Assessment Tool should be utilized for any vendor not previously approved by the FBI CJIS or NJSP CJIS Unit that will have access to or perform work on the agency network.
  2. The Network Administrator shall maintain an inventory of all 3rd party vendors with access to any component of the agency's systems. The inventory shall include current emergency contact information.

- S. **Information Sharing:** The Network Administrator shall register with the Multi-State Information Sharing & Analysis Center (MS-ISAC) and New Jersey Cybersecurity Communication and Integration Cell (NJCCIC).
- T. **Social Engineering:** Manipulating people into performing actions or divulging confidential information threatens the security of agency data systems.
  - 1. Hackers may use various means of social engineering to access secure data.
  - 2. Hackers may pose as supervisors, IT staff, or other authorized persons to obtain access to the agency computer system.
  - 3. Employees receiving requests for sensitive information via email or phone shall verify the request's source. At no time shall any employee ask another employee for passwords or access information.
    - a. Verification should be through independently obtained communication channels. For example, if a request is made via email, do not use a phone number in the email for verification. Verify the request by obtaining contact information from a source outside the original request.

## VI. RECORDS SECURITY AND PASSWORD AUDIT

- A. **Records Security and Password Audit:** The Records Supervisor or designee(s) shall conduct a security audit of the agency's records system, including physical and digital records. Simultaneously, password and access audits shall be conducted on all of the agency's electronic networks and shared databases.
- B. **Audit Frequency:** The records security and password audit shall be conducted annually.
- C. **Audit Scope:** The audit shall encompass the entire records system, including but not limited to physical records storage and security, electronic data storage and security, access controls (usernames and passwords), network security, compliance with applicable laws, regulations, CJIS Security Policy, and agency policy.
- D. The execution of the audit should determine the following:
  - 1. Policies regarding access, security, and release of agency records are being followed.
  - 2. All physical records are properly secure and are not accessible by unauthorized persons.
  - 3. Only currently employed personnel have access.

4. All users' access rights are for specific duties and responsibilities.
  5. Any personnel on suspension or other related leave of absence are temporarily removed from having access rights.
  6. Agency networks and endpoints are adequately protected by up-to-date protection software.
  7. All agency hardware is currently running the most up-to-date firmware.
  8. If there was any attempt by unauthorized persons to access any of the agency's networks.
  9. Mobile devices assigned to employees are being used following this policy.
  10. Inventories of all hardware, software, user accounts, 3rd party vendors, and data storage services/locations are current.
  11. The network diagram is current.
  12. Applications are reviewed, and those nearing end-of-life are identified for replacement or upgrade if required.
  13. Any violations or discrepancies shall be immediately reported to the Chief of Police in writing.
- E. The audit findings shall be submitted to the Chief of Police in writing using the Annual Computer System Security Audit form.

## **VII. BREACH OF SECURITY – INCIDENT RESPONSE PLAN**

- A. **Incident Response Manager:** The Chief of Police shall designate an Incident Response Manager. Ideally, the Incident Response Manager should be a command-level staff member familiar with the records systems and the agency's information technology systems and is readily available to respond to security breaches or cybersecurity incidents or events. The Incident Response Manager's responsibilities:
1. Respond to a security breach or cyber event and oversee the subsequent investigation.
  2. Ensure the policy is followed during a security breach or cyber event.
  3. Establish an Incident Response Team to support the execution of the Incident Response Plan.
  4. Coordinate a security breach or cyber event investigation.

5. Liaison with Incident Response Team members and partner agencies during a response and investigation into a security breach or cyber event.
  6. Coordination of inventories or audits associated with a response to a security breach or cyber event.
  7. Direct the annual review of this policy and associated procedures and recommend any adjustments considering new risks and security best practices. Any recommendations shall be in writing to the Chief of Police.
- B. **Incident Response Team:** An incident response team shall be established to respond to security breaches or cyber incidents quickly. The team should be comprised of administrative, investigative, and technical resources required to effectively respond to, analyze, contain, and investigate security breaches or cyber incidents.
- C. **Incident Detection and Reporting:** All personnel are required to watch for indications our records system or network has been breached and compromised by unauthorized users.
1. If an employee discovers an indication or is aware of a security breach or cyber event, they shall notify their supervisor immediately.
  2. Personnel are not authorized to perform investigative, diagnostic, or containment work on a suspected workstation, computer, or system without the expressed permission and instruction from the Incident Response Manager or technical expert activated in response to the incident.
  3. The supervisor shall make immediate notification to the Incident Response Manager.
  4. If the Incident Response Manager is unavailable, the Chief of Police shall be notified.
  5. **Isolation of Threat:** The Incident Response Manager should determine if the threat is contained to a single or a limited number of devices and advise on steps to isolate the device from the rest of the network.
    - a. If the Incident Response Manager is unavailable, the user discovering the potential security breach or cyber incident should isolate the affected device(s) from the network or internet by removing the network cable. If the device is operating via a wireless connection, turn off the wireless connection. If isolation of the device is not possible, disconnect the power source.
  6. The Incident Response Manager should attempt to identify the scope of the incident and notify the Chief of Police regarding its severity and action plan.

- D. **Notifications and Response:** The Incident Response Manager shall direct the following notification and any required response upon confirmation of a security breach or cyber incident:
1. **Chief of Police:** Advised of the incident scope, severity, and action plan.
  2. **The Incident Response Team:** Key team members required for the containment, investigation, and recovery.
  3. **CJIS Unit of the New Jersey State Police:** Mandatory Notification to the CJIS Unit is required within 1 hour after the attack is first.
    - a. Email: r038@njsp.gov
    - b. Phone - Enterprise Service Desk: 1-800-NCC-HELP
  4. **New Jersey Cybersecurity and Communication Integration Cell (NJCCIC):** Online (NJCCIC) must be completed within 72 hours after the attack was first identified.
    - a. Online NJCCIC Reporting Portal
  5. **Cyber Security Breach, Cyber Extortion Threat, or Data Breach:** Notification to the 24/7 Data Breach Hotline is mandatory. Do not delay in making the notification
    - a. Cyber JIF Data Breach Hotline: 855-566-4724
    - b. If the hotline does not immediately answer, leave a message describing the incident and leave contact information.
    - c. The Data Beach Hotline will refer the matter to a "Breach Advisor/Counsel" who will coordinate the response.
    - d. The Incident Response Manager shall follow the instructions of the Data Breach Hotline or the Breach Advisor.
    - e. The Breach Advisor will gather information about the incident and work with the Incident Response Manager to determine an action plan.
    - f. Advice and instructions from the Data Breach Hotline and/or the Breach Advisor shall be followed until the issue is resolved.
  6. **Other required breach notifications:**
    - a. FBI Internet Crime Complaint Center

- b. Any vendors controlling or supplying software or hardware involved in the breach.
- E. **Containment, Eradication, and Recovery:** The Incident Response Manager ensures actions are taken by agency personnel to limit the scope and magnitude of the incident as quickly as possible.
  - 1. **Immediate Triage:**
    - a. Immediately contact the technology expert or vendor(s) who has knowledge of the affected device(s), system(s), or application(s) and follow instructions.
    - b. Isolate the affected device(s) from the network or internet by removing the network cable from the service.
      - 1) If operating via wireless, turn off the wireless connection if possible.
    - c. Assemble the Incident Response Team and assess if the incident is a cybersecurity breach, cyber extortion threat, or data breach.
    - d. Document all actions taken.
    - e. Determine the scope of the incident to include:
      - 1) List of Devices Involved.
      - 2) List of Applications Affected.
      - 3) List of IP Addresses Involved.
      - 4) Compile access logs or other application logs from affected systems.
      - 5) Determine any user accounts that were compromised.
  - 2. **Eradication:** Removing malicious code, accounts, or inappropriate access and repairing vulnerabilities that may have been the root cause of the compromise is part of the eradication process.
    - a. The Incident Response Manager will liaison with representatives from all affected systems, applications, or devices to develop a plan for eradication.
    - b. A complete reinstallation of the operating system and any affected application is preferred.



3. **Recovery:** Allows the processes affected by the incident to recover and resume operations. It generally includes:
  - a. Reinstall and patch the OS and applications.
  - b. Change all user and system credentials.
  - c. Restore data to the system.
  - d. Return affected systems to an operationally ready state.
  - e. Confirm that the affected systems are functioning normally.
- F. **Investigation:** The Incident Response Manager, in conjunction with the Union County Prosecutor's Office or other investigatory agency, will facilitate an investigation into the potential breach.
  1. During the investigation, evidence shall be collected, retained, and stored in compliance with this agency's Evidence and Property directive.
  2. **Forensics:** Security incidents of a significant magnitude may require a forensics investigation. Once that need has been established, all additional investigation/containment activities must be directed and/or performed by a forensics specialist to maintain the evidence and chain of custody.
  3. Any personally owned devices, such as cell phones, wireless devices, or other electronic devices used to access organizational data and are determined to be relevant to an Incident, may be subject to retention until the Incident has been eradicated.
  4. **Immediate Audit:** As part of the investigation, the Incident Response Manager shall direct an immediate audit of the records system as follows:
    - a. The extent of the security breach to include what records were accessed without authorization.
    - b. The usernames or passwords used when the breach occurred.
    - c. Accounting of all keys to the physical records storage areas.
    - d. The audit also follows the scope of an annual security audit.
  5. The final results of the investigation and audit shall be reported in writing to the Chief of Police and include:
    - a. Information about the Incident type.
    - b. A description of how the Incident was discovered.

- c. Information about the systems that were affected.
  - d. Information about who was responsible for the system and its data.
  - e. A description of what caused the Incident.
  - f. A description of the response to the Incident and whether it was effective.
  - g. A timeline of events, from detection to Incident closure.
  - h. Recommendations to prevent future Incidents include:
    - 1) Policy Changes
    - 2) Training Needs
    - 3) Equipment or Software Needs
    - 4) Security Needs
  - i. A discussion of lessons learned that will improve future responses.
6. If it is found that any security breach occurred by an employee of this agency or through actions by an employee contrary to any agency directive, the violation shall be reported to the Internal Affairs function.
- G. **Loss, Theft, or Mishandling of Mobile Devices:** Rapid response to mobile device-related incidents can significantly mitigate the risks associated with illicit data access through the device itself or within online data resources associated with the device.
- 1. A mobile device's loss, theft, or misplacement must be reported immediately.
  - 2. If a mobile device or other device capable of remotely accessing CJI is reported lost, stolen, or misplaced, the device must be remotely locked or disabled to prevent access to network resources or data.

## VIII. RETENTION AND DISPOSAL OF AGENCY RECORDS

- A. Physical and digital records shall be retained and destroyed in strict accordance with the applicable schedules promulgated by the New Jersey Division of Revenue and Enterprise Services – Records Management Services (NJDRES-RMS). No public record will be destroyed unless proper authorization has been received by NJDRES-RMS by using the approved State of New Jersey online records disposition request via the online Artemis Records Retention and Disposition Management System.

1. After NJDRES-RMS authorizes the destruction of an agency record (paper, digital, CD, tape media, etc.), the record will be destroyed so that it will not be discernable again.
- B. Regularly, but no longer than on a triennial basis, the Custodian of Records or designee shall audit files currently being retained by the department and make a written determination to the Chief of Police of documents that can be destroyed per the records retention schedule.
- C. Any questions regarding records not found on the Records Retention Schedule shall be directed to the NJDRES-RMS through the contact information listed on their website.

## IX. TRAINING

- A. **CJIS Security Awareness Training:** All agency personnel with access to CJI shall complete CJIS Security Awareness training as required by the current version of the CJIS Security Policy.
- B. **Cybersecurity Training:** Employees shall receive at least one hour of cybersecurity training annually. Training shall include:
  1. A phishing exercise.
  2. Malware Identification.
  3. Password Construction.
  4. Identification and responding to security incidents.
  5. Social Engineering attacks.
- C. All personnel assigned to the Records Section shall be trained in each aspect of their responsibilities.