


ELIZABETH POLICE DEPARTMENT GENERAL ORDERS			
VOLUME: 5	CHAPTER: 5	# OF PAGES: 20	
SUBJECT: RECORDS ACCESS AND SECURITY			
EFFECTIVE DATE: July 30, 2025		ACCREDITATION STANDARDS: 82.1.1, 82.1.2, 82.1.6 (CALEA LE1) 1.8.1, 1.8.2, 1.8.3 (NJLEAP) 1.6.1, 1.6.2 (N.J.C.O.M.S.)	
BY THE ORDER OF: Chief Giacomo Sacca			
BY AUTHORITY OF: Police Director Earl J. Graves			
SUPERSEDES ORDER #:			

PURPOSE The purpose of this directive is to establish and maintain policies and procedures concerning access to and the security of reports and records of this agency.

POLICY The central records function is necessary and vital to the accomplishment of the Elizabeth Police Department's mission. It is, therefore, the policy of this department that an accurate and efficient reporting of all activity within the department's jurisdiction be maintained. It is the policy of this department to comply with all mandated reporting requirements of the federal government and the State of New Jersey while maintaining strict adherence to the public records law.

PROCEDURES:

I. General

- A. Any release of records must be in conformance with the New Jersey Open Public Records Act (O.P.R.A.), New Jersey Court Rules 7:7-7 and 3:13-3 pertaining to discovery requests, applicable Attorney General Guidelines, State Legislation, Statutes, Regulations, and this policy. The Services Commanding Officer shall maintain the complete list of guidelines used to make, manage, and maintain public records.
 - 1. Our organization recognizes the legal and non-legal consequences of failure to respond properly to a public records request. In addition to the distrust in government that failure to comply may cause, failure to comply with a request may result in a court ordering our organization to comply with the law and to pay attorney's fees and damages to the requester.
- B. 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.
 - 1. After the Division authorizes the destruction of a physical or electronic record (paper, CD, tape media, etc.), the record will be destroyed in a way and manner that it will not be discernable again.

II. Public Records Training for Records Personnel

- A. All personnel assigned to the records function shall be trained in each aspect of their responsibilities.
- B. No employee shall release any public record granted by law under the authority of this organization without being trained in the manner in which it is legally allowed.
- C. General training for records personnel shall be performed through the State of New Jersey, Division of Revenue and Enterprise Services, Records Management Services training program listed on their [training web page](#).
- D. Specific O.P.R.A. training for records personnel shall be performed through the State of New Jersey Government Records Council's training program listed on their [training web page](#).
- E. Other supplementary training may be performed by outside vendors who are appropriately credentialed to perform the specific instruction.

III. Controlling Access to Agency Criminal and Quasi-Criminal Records

- A. The following measures shall be taken and adhered to in order to control access to criminal and quasi-criminal records.
- B. The responsibility and accountability for the central record-keeping function shall lie with the records administrator.
- C. All personnel are responsible for maintaining the security and integrity of all records.

- D. Official records are copied for official purposes only, based on an established need to know and right to know the contents of such records.
- E. All personnel who are responsible for copying and releasing official records shall do so in accordance with this policy.
- F. Copies of all official records released under this policy under O.P.R.A. are provided with a clearly marked statement regarding appropriate confidentiality and use of the documents. Sample statement:
 - 1. Under the New Jersey Open Public Records Act (O.P.R.A.), a records custodian must deny access to a person who has been convicted of an indictable offense in New Jersey, any other state, or the United States and who is seeking government records containing personal information pertaining to the person's victim or the victim's family. This includes anonymous requests for said information. If you, the requestor, fit these criteria, then you are not allowed by law (under penalty of N.J.S.A. 2C:28-3) to possess such records. You are also not allowed to provide such records to the victim's assailant, thus circumventing the O.P.R.A. law.
- G. Destruction of official records occurs only during the routinely authorized purging of records (i.e., according to the records retention schedule) or pursuant to a court order.
- H. All electronic records stored on a computer or similar type of device shall be protected by a username-password combination.
- I. Once information from written records is entered into the in-house electronic records management system (R.M.S.), the physical records shall be promptly filed, if necessary. Access to the records filing system is restricted. Personnel with a need to review, inspect and/or copy these records for official purposes may only do so in accordance with this policy. Original records shall not be removed from the records filing system unless signed out and with the permission of the records administrator.
- J. 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.
- K. The department maintains strict privacy and security precautions to ensure the integrity of official records and compliance with applicable laws. The established precautions include the following:
 - 1. **Records privacy and security:** The records filing system is maintained in a secure condition. Only authorized personnel are permitted access to the records filing system.
 - a. **Unlimited access:** Personnel assigned to the records function may access the records filing system at any time.
 - b. **Limited access:** Supervisors may access the records filing system at any time. When personnel assigned to the records function are not

present, shift supervisors shall log in and out using the "Records Access Log," noting the case number accessed.

- c. **Restricted Access:** Other persons may be admitted into the records filing system only in specific circumstances. Those circumstances are as follows:

1. Personnel working on active cases in need of specific files and or records that are stored in hard copy format. When records personnel are not present, employees with restricted access shall log in and out on the entry log maintained inside the secure area, noting the case number accessed.
2. Records personnel have the authority to admit other people to the secure area (the area not open to the general public) provided such persons so admitted are under the direct supervision of the records personnel at all times and have a need to be in the area.

- L. Procedure for reviewing secured records after-hours.

1. Employees seeking files and records for investigative purposes should first utilize the electronic Records Management System (R.M.S.). The R.M.S. system will contain most of the information personnel will need.
2. In the event of an after-hours emergency, supervisors are authorized to access the records filing system to obtain any additional records they may need in order to perform their duties and responsibilities. Any removal of a record must be in accordance with this policy and necessitates the notification of the records administrator.

- M. Extra security measures shall be taken to protect the following types of records: Juvenile, Confidential, and Non-Public Personnel Records.

1. **Juvenile Records:**

- a. All juvenile records shall be secured from unauthorized access (N.J.S.A. 2A:4A-60).
- b. Juvenile records shall be marked as such to be distinguishable from other records.
- c. Disclosure of juvenile information:
 - 1). 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.
 - 2). Such records shall be made available only in accordance with N.J.S.A. 2A:4A-60a(1-13).

- d. Records of law enforcement agencies may be disclosed for law enforcement purposes or for the purpose of reviewing applications for a permit to purchase a handgun or a firearms purchaser identification card to any law enforcement agency of this State, another state, or the United States, and the identity of a juvenile under warrant for arrest for commission of an act that would constitute a crime if committed by an adult may be disclosed to the public when necessary for the execution of the warrant (N.J.S.A. 2A:4A-60b).
- e. At the time of charge, adjudication, or disposition, information as to the identity of a juvenile charged with an offense, the offense charged, the adjudication and disposition shall, upon request, be disclosed to (N.J.S.A. 2A:4A-60c):
 - 1). The victim or a member of the victim's immediate family,
 - 2). On a confidential basis, the principal of the school where the juvenile is enrolled for use by the principal and such members of the staff and faculty of the school as the principal deems appropriate for maintaining order, safety, or discipline in the school or to planning programs relevant to the juvenile's educational and social development, provided that no record of such information shall be maintained except as authorized by regulation of the Department of Education, or
 - 3). A party in a subsequent legal proceeding involving the juvenile, upon approval by the court.
- f. **School Notification:** A law enforcement or prosecuting agency shall, at the time of a charge, adjudication, or disposition, send a written notice to the principal of the school where the juvenile is enrolled of the identity of the juvenile charged, the offense charged, the adjudication and the disposition if (N.J.S.A. 2A:4A-60d):
 - 1). The offense occurred on school property or a school bus, occurred at a school-sponsored function, or was committed against an employee or official of the school, or
 - 2). The juvenile was taken into custody as a result of information or evidence provided by school officials, or
 - 3). The offense, if committed by an adult, would constitute a crime, and the offense:
 - a). Resulted in death or serious bodily injury or involved an attempt or conspiracy to cause death or serious bodily injury, or
 - b). Involved the unlawful use or possession of a firearm or other weapon, or

- c). Involved the unlawful manufacture, distribution, or possession with intent to distribute a controlled dangerous substance or controlled substance analog, or
- d). Was committed by a juvenile who acted with a purpose to intimidate an individual or group of individuals because of race, color, religion, sexual orientation or ethnicity, or
- e). It would be a crime of the first, second, or third degree.

Information provided to the principal pursuant to N.J.S.A. 2A:4A-60d shall be maintained by the school and shall be treated as confidential but may be made available to such members of the staff and faculty of the school as the principal deems appropriate for maintaining order, safety, or discipline in the school or for planning programs relevant to a juvenile's educational and social development.

- g. Nothing in N.J.S.A. 2A:4A-60 prohibits a law enforcement or prosecuting agency from providing the principal of a school with information identifying one or more juveniles who are under investigation or have been taken into custody for commission of any act that would constitute an offense if committed by an adult when the law enforcement or prosecuting agency determines that the information may be useful to the principal in maintaining order, safety or discipline in the school or in planning programs relevant to the juvenile's educational and social development. Information provided to the principal pursuant to this subsection shall be treated as confidential but may be made available to such members of the staff and faculty of the school as the principal deems appropriate for maintaining order, safety, or discipline in the school or for planning programs relevant to the juvenile's educational and social development. No information provided pursuant to this section shall be maintained (N.J.S.A. 2A:4A-60e).
- h. Information as to the identity of a juvenile adjudicated delinquent, the offense, the adjudication, and the disposition shall be disclosed to the public where the offense for which the juvenile has been adjudicated delinquent, if committed by an adult, would constitute a crime of the first, second or third degree, or aggravated assault, destruction or damage to property to the extent of more than \$500.00 unless upon application at the time of disposition, the juvenile demonstrates a substantial likelihood that specific and extraordinary harm would result from such disclosure in the specific case. Where the court finds that disclosure would be harmful to the juvenile, the reasons, therefore, shall be stated on the record (N.J.S.A. 2A:4A-60f).
- i. **Unauthorized Disclosure of Juvenile Records:** Whoever, except as provided by law, knowingly discloses, publishes, receives, or makes use of or knowingly permits the unauthorized use of information concerning a particular juvenile derived from records

listed in subsection a. or acquired in the course of court proceedings, probation, or police duties, shall, upon conviction thereof, be guilty of a disorderly persons offense (N.J.S.A. 2A:4A-60h)

j. See also Juvenile Operations policy.

2. Confidential Records:

a. Confidential records are considered to be files with sensitive or potentially sensitive information contained within, and access to such files should be protected from unauthorized access:

- 1). Confidential Funds,
- 2). Confidential Informants,
- 3). Confidential investigations,
- 4). Confidential operations,
- 5). Early Warning System,
- 6). Employee Assistance Program,
- 7). Megan's Law Records,
- 8). Restraining Order Records, and
- 9). Victim/Witness Information.

b. Securing of Confidential Records:

- 1). The Chief of Police shall make certain that all confidential records are secured in a locked cabinet or room and shall only be available to authorized personnel on a need-to-know basis.
- 2). Electronic confidential records shall be protected from unauthorized access.
- 3). Any violation of these requirements shall result in disciplinary action, including reprimand, suspension, and/or termination, depending on the severity of the violation.
- 4). Any third-party requests for a confidential record shall be forwarded to the Chief of Police for review and further consideration.

3. Personnel Records:

a. Personnel files will contain the following information, where applicable:

- 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). Any other pertinent information or material, and
- 10). Separate file for medical records.

b. Securing of Personnel Records:

- 1). As personnel files are confidential records, the Chief of Police shall make certain that all personnel and medical records folders are secured in a locked cabinet and shall only be available to approved managerial and supervisory personnel on a need-to-know basis.
- 2). Records relating to any medical condition will be maintained in a separate file folder.
- 3). Electronic personnel and medical records shall be protected from unauthorized access.
- 4). Any employee may review his/her file folders in the presence of the Chief of Police or their designee upon two business days' notice.
- 5). Authorized officials having access to the personnel and medical folders, or the information contained therein, are under an obligation to keep all such information confidential and to disclose such information as may be deemed necessary to other officials solely on a need-to-know basis.
- 6). Medical information may be disclosed only to the extent described above or upon the employee's written authorization.
- 7). Any violation of these requirements shall result in disciplinary action, including reprimand, suspension, and/or termination, depending on the severity of the violation.

- 8). Any third-party requests for personnel and/or medical information regarding municipal employees shall be forwarded to the Business Administrator for their review and in consultation with the municipality's personnel and labor attorney.
- c. **Confidentiality of Personnel Records:** Information contained in an employee's personnel and medical records folders shall be deemed confidential and shall not be released to the public or to any third party without the prior written consent of the employee, provided, however, that the following information shall be deemed public information:
 - 1). The employee's name, title, position, payroll record, length of service, date of separation from municipal service, and the reason therefor, and the amount and type of pension he/she is receiving, and
 - 2). Data contained in information that disclose 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.

IV. Off-Site Storage of Public Records

- A. All off-site (outside of the physical confines of the building) public records storage will be performed in accordance with New Jersey law and the administrative policies and procedures outlined by the New Jersey Department of the Treasury, Division of Revenue and Enterprise Services, Records Management Services in the [New Jersey Records Manual](#).

V. Expungements

- A. An expungement is the removal and isolation 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.
 1. Unless otherwise provided by law, if an order for expungement is granted, the adult arrest, the record of law enforcement taking you into custody as a juvenile, conviction, adjudication of delinquency, disposition, and any related proceedings are considered not to have occurred.
- B. The New Jersey expungement law is contained within N.J.S.A. 2C:52
 1. The following records may be expunged:
 - a. **Criminal** records
 - b. **Juvenile** records

- C. **Mandatory Check:** Records personnel will conduct periodic checks of the *Expungement Portal* within eCDR, minimally weekly, and comply with the Expungement Order. Upon completion, the status of the order within the portal shall be changed to "*Expunged*."
- D. When an electronic or paper order is received by this department, it will be honored right away. The applicable records will be moved and isolated with other expunged records this department holds.

VI. Procedures and Criteria for the Release of Agency Records

- A. **Criteria:** The Open Public Records Act, or O.P.R.A., is the name of the New Jersey law guaranteeing access to public records in the State. Any release of a departmental record will be in accordance with O.P.R.A. or other applicable state laws, regulations, court rules, etc.
 - 1. For any questions related to O.P.R.A., the Government Records Council (G.R.C.) operates a toll-free inquiry hotline to provide guidance to requestors of government records and records custodians regarding the Open Public Records Act (O.P.R.A.). The toll-free phone number is 1-866-850-0511. Additionally, the G.R.C. accepts inquiries from requestors of government records and records custodians regarding O.P.R.A. by email at grc@dca.state.nj.us, by fax (609) 633-6337 and by U.S. mail at "N.J. Government Records Council, 101 S. Broad Street, P.O. Box 0819, Trenton, New Jersey 08625-0819."
- B. **Procedures for O.P.R.A. Release:** Requests for access to public records must be made on a form that is in compliance with the Open Public Records Act and approved for use by the Chief of Police.
 - 1. Requests for access to public records shall be in writing and hand-delivered, mailed, transmitted electronically, or otherwise conveyed to the City of Elizabeth Custodian of Records (City Clerk) or to the supervisor of the Services Bureau.
 - 2. Officers shall not release copies of any reports due to privacy and disclosure considerations prior to coordinating with a supervisor from the Services Bureau.
 - 3. The custodian or Services Bureau staff should evaluate each public records request to estimate the length of time required to gather the records.
 - 4. The custodian shall promptly comply with the request to inspect, examine, copy, or provide a copy of a government record.
 - a. If the custodian deems a request significantly beyond routine, such as seeking a voluminous number of copies or requiring extensive research, the acknowledgment must include the following:
 - 1). An estimated number of business days it will take to satisfy the request.
 - 2). An estimated cost if copies are requested.

- 3). Any items within the request that may be exempt from disclosure.
5. If the custodian is unable to comply with a request for access, the custodian shall indicate the specific basis on the request form and promptly return it to the requestor. The custodian shall sign and date the form and provide the requestor with a copy.
- C. **Criteria and Procedures for Release through Discovery:** Services Bureau Records Section personnel supervisors shall follow New Jersey Court Rule 7:7-7 in releasing any department record in a discovery request. Services Bureau personnel may assist in gathering documents, but the final release must be completed by a supervisor. If there is a question as to the release of a specific document, personnel shall seek clarification from their supervisor. Any decision that has to be made that is not outlined in rule 7:7-7 shall be made under the advice of the appropriate prosecutor or their designee.
- D. **Criteria and Procedures for Release through Court Order or Subpoena:** This department shall abide by any court order for the release of any information. Records personnel shall fill such a request and return it to the employee requesting it as soon as possible. All documents released under a court order shall be reviewed by the Chief of Police or his/her designee before their release to make sure it complies with the court order.
- E. Any other records release not covered under this policy shall require approval by the Records Custodian and the Chief of Police.
- F. Under O.P.R.A., a government record that is otherwise publicly accessible may contain non-disclosable information that should be redacted. Redaction means editing a record to prevent public viewing of material that should not be disclosed. Words, sentences, paragraphs, or whole pages may be subject to redaction.
 1. How to Redact:
 - a. If a record contains material that must be redacted, such as a social security number or unlisted phone number, redaction may be accomplished by using a visually obvious method that shows the requester the specific location of any redacted material in the record. For example, if redacting a social security number or similar type of small-scale redaction, custodians should:
 - 1). Make a paper copy of the original record and manually "blackout" the information on the copy with a dark-colored marker,
 - 2). Then provide a copy of the blacked-out record to the requester.
 - b. The blacked-out area shows where information was redacted, while the double copying ensures that the requester will not be able to "see-through" to the original, non-accessible text. If "white-out" correction fluid is used to redact material, some visual symbol should be placed

in the space formerly occupied by the redacted material to show the location of the redacted material.

- c. 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 provide formal communication to the requester, making it clear that material was not provided.
 - d. If an electronic document is subject to redaction (i.e., word processing or Adobe Acrobat files), custodians should be sure to delete the material being redacted. Techniques such as "hiding" text or changing its color so it is invisible should not be used as sophisticated users can detect the changes.
2. Explaining why a redaction is made.
- a. When redactions are made to a record, the custodian can use either the request form to explain why those elements of a record are redacted or use a separate document, depending on the circumstances, but also referring to the O.P.R.A. exception being claimed. This principle also applies if pages of information are redacted. Sometimes it is clear from inspection (an entry called "Social Security Number" has a blackout over where the number would appear). The bottom line is that the requester has a right to know the reason for the redaction, and the custodian has the responsibility to provide a reasonable explanation.

VII. Security of Central Records Computer Systems

- A. One employee, or a consultant, shall be designated as a Network Administrator who will be responsible for ensuring all the procedures outlined in this policy and any other agency policy related to agency-owned computers and electronic equipment are adhered to.
- B. **Data Backup:** The Network Administrator shall make a daily backup of the electronic records management system. This will ensure continual continuity of data integrity and retrieval in case of a catastrophic failure of the system. The backup or a copy should be securely stored off-site, if possible.
- C. **Data Storage:** All data from the central records computer records management system will be stored in a manner compliant with the hardware and software manufacturer's recommendations as well as what is considered to be the current best practices in the I.T. field. All data will be stored in the records management system. The storage of any electronic files or other forms of electronic data not the property of the agency on computers owned by the agency is strictly prohibited. All data will be stored on network resources that are backed up daily. No unauthorized data or documents will be stored on desktop computer media.
- D. **Password Protection and Access Security:** Physical security of our computer systems must be maintained at all times. Only appropriate personnel are to be given access to the office computers regardless of their location, whether that is in the

office or off-site on mobile systems. The electronic records management system has a password-protected access control system. Only personnel with a need to access the system will be assigned a username and password. Personnel are required to change their password for the records management system at least every six (6) months.

1. **Password Strength and Security.** All personnel shall have a strong password. Strong passwords should be at least eight alphanumeric characters long and contain both upper and lower-case characters. Passwords should never be written down or stored online. Ideal passwords are not only hard to guess but also easily memorized. Passwords are not to be shared with anyone. They should be considered sensitive, confidential information that belongs to the organization. Passwords should not be included in an email message, revealed to co-workers or family members.
2. **Internet Access.** All computers that allow Internet access are secured with an industry-standard firewall to prevent unauthorized access to the central electronic records management system. Even with this level of protection, internet use is for mission-critical requirements only.
3. **Inactivity.** When personnel are not using their computer or a workstation, they will log off the system and not leave it unattended.
4. **Unauthorized Downloading.** Personnel shall not download or open any information from an unknown source. This is required to protect the network from intrusive programs such as viruses, malware, and spyware.
5. Personnel shall not email their username or password.

E. **R.M.S. System Integrity Measures:** The following internal controls will be strictly adhered to in order to maintain R.M.S. integrity:

1. **Annual Security Audit:** On an annual basis, the Network Administrator will perform an audit of our R.M.S. system of all user names and passwords to determine the following:
 - a. Only currently employed personnel have access,
 - b. All users' access rights are for their specific duties and responsibilities,
 - c. Any personnel on suspension or other related leave of absence are temporarily removed from having access rights,
 - d. Any violations or discrepancies shall be immediately reported in writing to the Chief of Police through the chain of command, and
 - e. The Network Administrator shall report their findings in writing to the Chief of Police using the Annual Computerized Records Security Audit form.
2. **Security Breach Identification and Response Procedures:**

- a. Personnel are required to watch for indications our network has been breached and compromised by unauthorized users. When an employee believes their computer may be breached, they are to immediately notify their supervisor, who will, in turn, contact the department's Network Administrator. Some indications a computer may be breached are as follows:
 - 1) The system becomes locked and unresponsive,
 - 2) A ransom message is observed,
 - 3) Fake antivirus messages pop-up,
 - 4) Frequent random pop-ups,
 - 5) Unwanted browser toolbars appear in your web browser,
 - 6) Redirection from one website to another,
 - 7) One of your email contacts received an email from you that you didn't send,
 - 8) Your password suddenly stops working,
 - 9) Unexpected software loads onto your computer,
 - 10) Your mouse pointer moves in ways you are not moving it, and
 - 11) Your anti-malware software, Task Manager or Registry Editor is disabled and can't be restarted.
- b. Personnel are not authorized to perform any investigative or diagnostic work on a suspected computer without authorization from the Network Administrator.
- c. When the Network Administrator has reason to believe a network has been breached, he/she shall immediately terminate any and all remote communication connections to and from it in order to isolate the potentially affected system. The Network Administrator shall then make the following notifications:
 - 1) Chief of Police through the chain of command,
 - 2) The Union County Prosecutor, and
 - 3) Any vendors whose software or hardware are potentially involved in the breach.
- d. The Network Administrator will facilitate an investigation into the potential breach in coordination with the prosecutor's office and applicable vendors. An immediate audit of the R.M.S. system will be conducted at any time a breach, violation, or similar type of situation

is determined to have occurred or existed. The investigative direction will be taken from the prosecutor's office as to how the investigation will proceed and how/what related criminal charges are to be filed. Investigations into a potential breach can range from simple to incredibly complex, depending upon the method the breach was able to penetrate the network and the level of commitment the breaching party had to gain access to it.

- 1) Random breach: a random breach is where malware is used in a random fashion to identify weaknesses in random networks, and when one is discovered, it is exploited. Depending upon the level of sophistication behind this type of breach, the Network Administrator may have some time to secure the network from further intrusion and potential data destruction or theft. Various types of commercial-grade anti-malware software, along with network physical and virtual configurations, will help in preventing/limiting these kinds of breaches.
- 2) Directed breach: directed breaches are the most dangerous and, in an ever-increasing amount of occurrences, are difficult even to detect. Direct breaches are when a network is specifically targeted by a sophisticated adversary with the intended purpose of breaching the network for an identified purpose. These types of breaches are difficult, if literally impossible, to prevent, but they can be limited by having a robust layered defense system in place, including:
 - a) User education.
 - b) Robust Information Assurance (Cyber Security) policies in place.
 - c) Software specially designed and appropriately updated to identify and prevent spyware, malware, ransomware, etc., from being able to operate on a computer or network.
 - d) Real-time monitoring of network health to identify outlier activity that could potentially indicate a breach attempt in progress or an actual breach working its way through the network
- e. The Network Administrator is not permitted to reconnect the potentially affected network until he/she reasonably believes there was no breach or that the breach that did occur was stopped and the method used closed to unauthorized access.
- f. The Network Administrator will provide the Chief of Police with a detailed report of facts and actions taken for any suspected or confirmed breach of a police department network.

3. **Annual Password Audit of Shared Databases:** on a yearly (annual) basis, an audit will be performed of all usernames and passwords for any shared database to determine the following:
 - a. Only currently employed personnel have access,
 - b. All users' access rights are for their specific duties and responsibilities,
 - c. Any personnel on suspension or other related leave of absence are temporarily removed from having access rights,
 - d. Any violations or discrepancies shall be immediately reported in writing to the Chief of Police through the chain of command, and
 - e. The Network Administrator shall report their findings in writing to the Chief of Police using the Annual Computerized Records Security Audit form.
 - f. Shared databases include, but are not limited to, the following:
 - 1). CJIS/NCIC (audited in accordance with the NJSP CJIS User Agreement),
 - 2). AOC (ATS/ACS) applications,
 - 3). CAD/RMS,
 - 4). eCDR / Etro,
 - 5). NJLearn,
 - 6). Guardian Tracking,
 - 7). Power D.M.S,
 - 8). Network/Email,
 - 9). M.V.R (Mobile Vision, and
 - 10). Live Scan
- F. **Clearing, Sanitizing, and Releasing Computer Components:** No computer, hard drive, CD, DVD, cellular phone, or other remotely related electronic data storage device owned by this agency shall be released from custody and control of this agency until such time as 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.
- G. **Virus Protection:** Due to the possibility of computer virus infection, all outside software, discs, or other electronic data storage devices are to be used only with the prior approval of the Network Administrator. Should anyone need assistance with

this process, they will contact the Network Administrator before using or connecting the device to any computer.

- H. All software shall be properly licensed.

VIII. Field Reporting and Management System

- A. A standardized process is required to memorialize police activity for future reference. CAD records shall be completed as thoroughly as possible, including as much information as possible to provide future investigative leads. Information to be included may be received by phone, in-person, or other electronic means. At a minimum, a CAD record will be generated for the following:
 - 1. Citizen reports of crimes,
 - 2. Citizen complaints,
 - 3. Citizen requests for services when:
 - a. An officer is dispatched,
 - b. An officer is assigned to investigate, or
 - c. An officer is assigned to take action now or at a later time.
 - 4. Criminal and non-criminal investigations or incidents initiated by law enforcement members,
 - 5. All incidents involving arrests, complaints, summonses, or
 - 6. Any report of an incident(s) requiring a police response.
- B. A CAD entry with an accompanying narrative by an officer or dispatcher is required in all of the following, but not limited to, incidents/events occurring within this agency's service area:
 - 1. Citizen reports of crimes or alleged criminal activity,
 - 2. Criminal investigations (assigned or self-initiated),
 - 3. Arrests,
 - 4. Issuance of C.D.R. warrants or summonses and special complaints,
 - 5. Domestic Violence,
 - 6. Motor vehicle stops,
 - 7. Field interviews/investigative detentions,
 - 8. Found/recovered property or vehicles,
 - 9. Injured persons,

10. Vehicle crashes,
11. Building entry,
12. Property damage,
13. Firearms discharges,
14. Missing/Located/Unidentified Person investigations,
15. Mutual aid assistance to other law enforcement agencies, and
16. Any incident that could generate publicity.

C. The following forms are typically utilized to record actions or police investigations:

1. CAD,
2. Incident Data Sheet,
3. Continuation/Supplemental Report,
4. Pedigree Information Form,
5. Arrest Checklist,
6. Arrest Report,
7. Miranda Rights Form,
8. D.W.I. Reports:
 - a. D.W.I. Questionnaire,
 - b. Alcotest,
 - c. Drinking-Driving Report w/continuation.
9. Motor Vehicle Crash Report (NJTR-1),
10. Towed Vehicle Report (Impound Sheet),
11. Property Evidence Release Forms,
12. Missing Person Forms,
13. Unidentified Person Forms,
14. Consent to Search Forms,
15. Use of Force Report,

16. Pursuit Incident Report, and
 17. Victim Notification Form,
- D. Some reports will require a great deal of information and involvement(s), while others may only require a short narrative to memorialize a particular incident. The primary officer ensures all applicable information is added to the initial report. All reports shall include the following:
1. All principal and relevant data fields on the RMS report pertaining to the incident shall be completed.
 2. A narrative describing, at a minimum, the incident and the officer's role.
 3. All principal and relevant individuals involved in the incident.
 4. All offenses committed or attempted as a result of the incident.
 5. All reports, forms, or other statistical data required by law, regulation, or directives.
- E. Most forms are self-explanatory concerning the information required. Personnel are responsible for completing these forms accurately and thoroughly. For questions regarding CAD and/or Records Management Software forms, please refer to the software manual.
- F. Reports containing descriptions of hazardous or dangerous conditions that are under the purview of other governmental agencies shall be forwarded to the appropriate government agency with jurisdiction without undue delay. Notification may be made by phone, fax, radio, or other electronic submission. Information within the report that is not subject to public disclosure shall be redacted. These governmental agencies include, but are not limited to, municipal, county, and State:
1. Public works departments,
 2. Zoning, property maintenance, city engineer and other code officials,
 3. Fire department,
 4. Public health officials,
 5. Board of Education/educational institutions, and
 6. Parks and or recreation.

IX. Procedures for the Writing, Submitting, Inspecting, and Dissemination of Reports

- A. The Elizabeth Police Department uses the LawSoft electronic records management system for memorializing law enforcement activities in the city of Elizabeth.
- B. All personnel are required to complete and submit their work electronically through LawSoft as soon as possible but no later than the end of the shift. Supervisory approval is required to deviate from this.

- C. The Desk Lieutenant shall review and approve any outstanding reports in LawSoft during their tour of duty. This shall be performed on an ongoing basis throughout their shift.
- D. Supervisory Responsibilities for the Review and Approval of Records:
1. Supervisors are responsible for reviewing reports submitted by subordinates to ensure that they were completed in compliance with this directive.
 2. Supervisors will ensure that reports are completed accurately, thoroughly, and in a timely manner.
 3. Supervisors must approve any delay in the submission of a subordinate's report. All approvals to extend the time to submit a report should be based on manpower, call volume, and/or complexity of the investigation. Delays based on poor time management or organizational skills are not acceptable. Additional training and/or counseling may be necessary to avoid such delays.
 4. Supervisors should review reports prior to the end of the officer's shift. Reports for incidents occurring late in a shift should be reviewed as soon as possible, but generally no later than the supervisor's next assigned shift.
 5. Supervisors are responsible for the quality of reports prepared by their subordinates. Reports containing errors or deficiencies shall be returned to the authoring person for correction. When the reviewing supervisor finds deficiencies in a report, he/she will counsel the reporting officer prior to obtaining the necessary corrections.
 6. Supervisors have a responsibility to train and counsel subordinates on proper report-writing techniques and should offer advice and constructive criticism when appropriate. However, reports containing alternative writing styles should be distinguished from reports that contain deficient content, poor grammar, and/or spelling errors. Supervisors should not immediately discount an alternative writing style if the report is thorough and accurately describes the incident.
 7. Supervisors will indicate that they reviewed the report and determined it to be satisfactory by "approving" the report in the appropriate field.
 8. Reports authored by supervisors should be reviewed by a supervisor in the next level of command when possible. However, another supervisor of equal or lesser rank may review the report for accuracy and completeness.