BLOOMFIELD POLICE DEPARTMENT
GENERAL ORDERS

VOLUME: 5	**CHAPTER: 5**	**# OF PAGES: 9**

SUBJECT: RECORDS ACCESS AND SECURITY

BY THE ORDER OF: **Public Safety Director Samuel A. DeMaio**	**ACCREDITATION STANDARDS:** **1.8.1, 1.8.2**
Effective Date: **December 4, 2015**	**SUPERSEDES ORDER #:**

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.

POLICY The central records function is necessary and vital to the accomplishment of the Bloomfield 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 (OPRA), New Jersey Court Rules 7:7-7 and 3:13-3 pertaining to discovery requests, applicable Attorney General Guidelines, and this policy.

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 Archives and Records Management.

1. After the New Jersey Division of Archives and Records Management authorizes the destruction of a physical record (paper, CD, tape media, etc…) it will be the responsibility of the Services Division Commander to make sure the record will be destroyed in a way and manner that it will not be discernable again.

II. 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 Records.

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 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 OPRA 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 (OPRA), 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 this 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 OPRA law.

G. Destruction of official records occurs only during the routine 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 device, shall be protected by a username password combination.

I. Once information from written records are entered into the in-house electronic records management system (RMS), the physical record 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.

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 assure 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 actives cases or need specific files and or records that are stored in hard copy format in records. 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, 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. The electronic Records Management System (RMS) contains most of the information personnel will need to gain access to when the records filing system is secured.

2. In the event of an after-hours emergency, supervisors are authorized to recall Administrative Bureau personnel to obtain any additional records they may need to in order to perform their duties and responsibilities. Any removal of a record must be in accordance with this policy.

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

1. **Juvenile**: Juvenile records will be marked as such so that they may be protected from inadvertent release or from the disclosure of information about the case or juvenile that is prohibited under other related regulations or laws.

2. **Confidential**: All records of a confidential nature shall be clearly 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 Public Safety Director. Access to these types of files may be regulated to personnel with a need to know basis as determined by the Public Safety Director.

3. **Non-Public Personnel Records**: All non-public personnel records shall be stored in a secure manner in its own separate filing system in a location determined by the Public Safety Director. Access to these types of files will be regulated to personnel with a need to know basis as regulated by the Public Safety Director.

III. Procedures and Criteria for the Release of Agency Records.

A. **Criteria**: The Open Public Records Act, or OPRA, 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 OPRA or other applicable state laws, regulations, court rules, etc.

1. For any questions related to OPRA, the Government Records Council (GRC) operates a toll-free inquiry hotline to provide guidance to requestors of government records and records custodians regarding the Open Public Records Act (OPRA). The toll-free phone number is 1-866-850-0511. Additionally, the GRC accepts inquiries from requestors of government records and records custodians regarding OPRA by e-mail at grc@dca.state.nj.us, by fax (609) 633-6337, and by US mail at "NJ Government Records Council, 101 S. Broad Street, P.O. Box 0819, Trenton, New Jersey 08625-0819."

B. **Procedures for Records Release under the NJ Open Public Records Act**: Requests for access to public records should be made on a form that is in compliance with the Open Public Records Act and approved for use by the Public Safety Director. However, the New Jersey Open Public Records Act does not require the form to be used just that the request be submitted in writing.

1. The recipient of any OPRA request brings that request to the Township's OPRA Clerk located in the Town Clerk's Office.

2. The OPRA Clerk assigns the request a unique number and a due date.

3. The request is then forwarded to the Public Safety Director.

4. The Public Safety Director or their designee determines where the requested record is located within the police department.

5. The Public Safety Director's designee forwards the request to the appropriate commander of the division where the record is kept.

6. If the record exists, the division commander makes a copy of the requested record and provides the copy to the Public Safety Director's designee.

7. If the record does not exist or the record cannot be released, the Division Commander will provide the Public Safety Director's designee, in writing, the reason for not providing the record.

8. The completed OPRA request, or the reason for not producing the record is provided to the Township's OPRA Clerk prior to the due date.

C. **Criteria and Procedures for Release through Discovery**: Records Section personnel shall follow New Jersey Court Rule 7:7-7 in releasing any department record in a discovery request. If there is a question as to the release of a specific document Records 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 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 Public Safety Director before its 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 Public Safety Director.

F. Under OPRA, 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, custodian's should:

1). Make a paper copy of the original record and manually "black out" 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 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 word "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 OPRA 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 black out 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.

IV. 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 is adhered to.

B. **Data Back-Up**: The network administrator shall provide for a daily back-up of the electronic records management system. This will assure continual continuity of data integrity and retrieval in case of a catastrophic failure of the system. The back up or a copy shall be securely stored on site.

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 IT 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 user name 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 on-line. Ideal passwords are not only hard to guess but also easily memorized. Passwords are not to be shared with anyone. They should be considered as 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.

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

1. **Annual Security Audit**: On an annual basis the network administrator will perform an audit of our RMS 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 absences are temporarily removed from having access rights;

d. Any violations or discrepancies shall be immediately reported in writing to the Public Safety Director through the chain of command; and

e. The network administrator shall report their findings in writing to the Public Safety Director using the Annual Computerized Records Security Audit form.

2. **Security Breach Procedures**:

a. An immediate audit of the RMS system will be conducted at any time a breach, violation, or similar type of situation is determined to have occurred or exists.

b. The audit will be conducted concurrently by the network administrator and Internal Affairs unless it is determined that another course of action is needed by the Public Safety Director.

c. The investigative team conducting the audit will keep the Public Safety Director informed regarding progress made.

3. **Annual Password Audit of Shared Databases**: On an annual basis an audit will be performed of all user names 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 absences are temporarily removed from having access rights;

d. Any violations or discrepancies shall be immediately reported in writing to the Public Safety Director through the chain of command; and

e. The network administrator shall report their findings in writing to the Public Safety Director using the Annual Computerized Records Security Audit form.

f. Shared databases include, but are not limited to the following:

1). NJCJIS (audited in accordance with the NJSP CJIS User Agreement); and

2). AOC applications.

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 will be scanned utilizing an antivirus program on each computer. 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.