DIRECTIVE 82.1
CENTRAL RECORDS ADMINISTRATION

Issue Date: 05/28/2020	By Order of Chief of Police
Rescinds: (Issue 03/04/2019) Pages: 8	CALEA Standards Referenced: 82.1.1; 82.1.2; 82.1.3; 82.1.4; 82.1.5 & 82.1.6

This directive consists of the following sections:

POLICY AND PROCEDURE:

The central police records function of the Miami Township Police Department is important to the effective delivery of law enforcement services. This directive addresses those records functions that are basic to meeting the management, operational and information needs of the department. It is the policy of the Miami Township Police Department to provide for the security and privacy of the department's records in accordance with legal mandates.

82.1.1 Privacy and Security

Security and Controlling Access to Agency Files

The Miami Township Police Department records section is staffed by Police Records Clerks who are supervised by a Lieutenant designated by the Chief of Police. The records section is responsible for gathering, indexing, entering, filing and maintaining agency records. Records personnel are responsible for the security and control of access to agency records maintained in the records section.

Only Miami Township Police Department personnel shall have unsupervised access to the records section. Police volunteers may have access to the records section during regular business hours. The records section is secured at all entry points by key card access. No entry point to the records section shall be unlocked or unsecured at any time. Visitors to the records section must always be accompanied by a police department employee.

Accessibility to Operations Personnel after Hours

All police department personnel have access to the records section and all records contained within the section 24/7 through issuance of a police department keycard. Additionally, all police personnel have access to agency records utilizing the in-house records management software. Should an exigent circumstance arise requiring agency records personnel after normal operating hours, the supervisory Lieutenant shall be contacted.

Procedures and Criteria for the Release of Agency Records

The supervisory Lieutenant shall be responsible for the public information function as it relates to authorization and release of public records governed under Ohio Revised Code 149.43.

Records clerks receive advanced training in the Release of the Public Records and are the only authorized employees of the agency that may release records. Records personnel shall complete the Public Records Request Form RC100 in its entirety. While the requestor is not required to complete the form, the clerk releasing the record will complete and sign the form indicating the release to include the checklist provided for why records or portions of records were not provided for inspection or copying.

In instances where members of the Department are either actively involved in or have just concluded a police action, care should be exercised before releasing public records. Records personnel should consult with the supervisory Lieutenant or his/her designee if they have any questions as to what information is appropriate to be released concerning a police record.

Records personnel releasing police records shall redact victim, witness and suspect information as required by ORC 149.43. Redaction means obscuring or deleting information that is exempt from the duty to permit public inspection or copying from an item that otherwise meets the definition of a record in Section 149.011 ORC.

- Personal Identifiers - Personal identifiers means social security numbers, except for the last four digits; driver license numbers, financial account numbers, employer and employee identification numbers and a juvenile's name in an abuse, neglect, or dependency case, except for the juvenile's initials or a generic abbreviation such as 'CV' for Child Victim.
- Medical Records
- Information concerning cause of death shall not be released by members of this agency pending determination by the Coroner's Office, as provided in ORC 313.19.
- Suicide Note – The original suicide note shall be copied and forwarded to the Coroner's office with a copy of the Death Report. Suicide notes are to be handled cautiously as they may be processed for fingerprints, trace evidence and/or handwriting analysis. All original suicide notes will be logged into the MTPD

property room. Any copies of a suicide note are exempt from public record as provided in ORC 313.10. Any requests for copies should be referred to the Coroner's Office. The Coroner's Office may contact the department and request we forward a copy of the suicide note to a family member. Should this occur, it must be documented on a supplemental narrative to the death report.

- If fingerprints or photographic records of juveniles are taken in accordance with ORC 2151.313, they are not public record.
- LEADS/NCIC Records.
- Information on victims, witnesses or suspects as described in Confidential Law Enforcement Investigatory Records.
- Trial Preparation Records – Any record that contains information that is specifically compiled in reasonable anticipation of, or in defense of, a civil or criminal action or proceeding, including the independent thought processes and personal trial preparation of an attorney.

Miami Township Police Department personnel shall not release the following information unless authorized by the Chief of Police.

- Information concerning the prior criminal record, character or reputation of the accused.
- Mug shot of an accused person.
- Information regarding the existence of any confession, admission of guilt, or statement made by the accused or the failure or refusal by the accused to make a statement.
- Excluding OVI tests, results of any examinations or tests conducted or refusal by the accused to submit to these examinations or tests.
- Information concerning the identity, testimony, or credibility of any prospective witness, excluding if such information would not prejudice an investigation or place the witness in danger.
- Opinions regarding the guilt or innocence of the accused shall not be relayed in any manner.
- Opinions regarding the merits of the case or the quality of evidence gathered.

ORC 149.43 states the following records, concerning confidential agency investigations and operations are not public record and are exempt from release:

- Confidential Law Enforcement Investigatory Record – Any record that pertains to a law enforcement matter of a criminal, quasi-criminal, civil or administrative nature, but only to the extent that the release of the record would create a high probability of disclosure of any of the following:
    - The identity of a suspect who has not been charged with the offense to which the record pertains, or of an information source or witness to whom confidentiality has been reasonably promised.

- Information provided by an information source or witness to whom confidentiality has been reasonably promised, when information would reasonably tend to disclose the source's or witness's identity.
- Specific confidential investigatory techniques or procedures or specific investigatory work product.
- Information that would endanger the life or physical safety of law enforcement personnel, a crime victim, a witness or a confidential information source.

82.1.2 Juvenile Records

Methods to Distinguish Juvenile Records

These records are public and made available if requested. It would be a violation of ORC 149.43 if handled otherwise. Hard copies of public records involving juveniles are not kept separate from the rest of the public records but are tagged as such in the computer files.

Fingerprints, Photographs of Juveniles

Juvenile fingerprints and photographs, if obtained, shall be in accordance with ORC 2151.313 & 109.60. If taken, these records will remain with the investigating officers' case file.

Security and Control of Juvenile Records

Juvenile records are secured and controlled in the same manner as all other records.

Disposition of Juvenile Records upon Reaching Adult Age

Juvenile records maintained by law enforcement agencies in the State of Ohio are treated no differently than adult records, including records identifying a juvenile suspect, victim or witness. Law enforcement agencies in Ohio are not typically permitted by law to redact information about juveniles from their records based simply on the juvenile's age or upon reaching adult age. Specific exemptions to this shall be in accordance with ORC 149.43 and ORC 2151.356. Miami Township Police Department shall maintain juvenile records in accordance with the Schedule of Records Retention and Disposition.

Court Ordered Expungements

The Clermont County Juvenile Court may order an expungement or sealing of a record of a juvenile after conducting a hearing in accordance with ORC 2151.358. Upon receiving notification of an expungement or sealing of a record, the supervisory Lieutenant or their designee shall be responsible for removing all record of the person from hard copies of records held by the agency and removing the record from all computerized records of the department.

82.1.3 Records Retention Schedule

In accordance with ORC 149.39, the Miami Township Police Department has established and maintains a schedule for retention and destruction of agency records. No records shall be destroyed, transferred or otherwise disposed of in violation of this schedule. The records covered by the schedule, upon expiration of the retention period, may be deemed of no continuing value to the department. No records shall be destroyed so long as in the opinion of the department, it pertains to any pending case, claim or action. The supervisory Lieutenant or their designee shall be responsible for the retention and destruction of agency records.

82.1.4 Crime Reporting

Miami Township does participate in the submission of crime information to the Ohio Office of Criminal Justice Services through monthly OIBRS submissions. The Ohio Incident-Based Reporting System (OIBRS) is Ohio's version of the FBI's National Incident-Based Reporting System (NIBRS). OIBRS is a voluntary crime reporting program in which Ohio law enforcement agencies can submit crime statistics directly to the state and federal government in an automated format.

The information shall be derived from the department's records and submitted in accordance with the requirements of the OIBRS program.

Records personnel shall also complete a monthly Domestic Dispute/Domestic Violence Summary and submit the document to the Bureau of Criminal Identification and Investigation.

82.1.5 Report Accounting System

Each incident of law enforcement service which creates a record shall be assigned a unique number upon entry in the in-house computerized records management software. This number is assigned by the software program and will not be repeated.

Personnel entering the record shall record this unique number on any attachments to the report, i.e. Commitment Forms, Handwritten Statements, etc. The report and all attachments shall be maintained in records.

The Investigations Supervisor shall be responsible for the case screening/management system. A copy of all criminal offense reports taken shall be given to the Investigations Supervisor. Upon receipt of an offense report, the Investigations Supervisor may assign the case for follow-up investigation.

Case investigators shall work from the copy assigned. Should the investigating officer generate additional paperwork versus software data entry, the officer will be responsible to maintain all additional documents pertaining to the case under investigation in the case file. Follow up reporting shall be in accordance with Directive 42.1.3.

When the case is closed or inactivated, the case file will be forwarded to the records section. Upon receipt of the case file, records personnel shall verify all hard copy attachments are scanned to the computerized record, numbered with the case number and that the case status is updated in the records management software.

82.1.6 Computer File Backup and Storage

Data Backup

Miami Township's servers store all user and system data and are in a secure climate-controlled room in the Township Civic Center. Modified file backups are performed every hour with full backups being performed as needed.

Storage

A full backup is completed as needed to accommodate new servers/storage repositories or to consolidate backup chains. Copies of all backups are sent securely via internet connection to a secure, offsite facility.

Access Security

Invalid login attempts are audited and logged on all workstations and servers and checked on a regular basis, at least quarterly.

A multi-factor authentication system has been implemented that will require personnel to enter additional credentials when logging onto a new compter.

Webroot Secure Anywhere is used to protect all workstations, servers and email from virus and spyware infections and activity is alerted automatically.

The Township shared Internet connection is protected by a Cisco ASA firewall and all activity controlled and monitored using a hosted web filter.

All user accounts are created on the network servers (Domain Controllers) and there are no user accounts available on any local workstation for users to login to.

Patches for the core operating systems on all systems are reviewed and updated automatically.

Password Audits

All Township employees that have user accounts within the Township network are required to have a password that is a minimum of 7 characters and must contain three of the four following character sets: Capital letter, lower case letter, alphanumeric or symbol. Passwords are effective for 180 days, after which they must be changed. The last 12 passwords used are not eligible to be re-used.

If five attempts are made to access a user's account with the wrong password, the account is automatically locked and remains locked for 30 minutes.

User accounts are audited every six months for terminated employees or infrequently used accounts, which are suspended until authorization from the department is granted again. When an employee is terminated, the department head or designee is required to notify the network administrator of the departure so that their account can be suspended or deleted.

Computerized Security Protocol of Criminal History Records

The Miami Township Police Department does not keep Criminal History Records. The department does keep original arrest reports and offense reports, both are public records regardless of the outcome of any trial and regardless of age of the defendant.

Conviction records are kept by the courts involved. Adult convictions are public records and juvenile convictions are controlled by the Juvenile Court. The Miami Township Police Department has no control over these records.

LEADS

Computerized Criminal Histories (CCH) are controlled by LEADS and BCI&I. The Miami Township Police Department has entered into a Participation Agreement to gain access to these computerized files. A copy of the participation agreement is maintained by the department. A LEADS Administrative Rules Manual is located on the Miami Township police computer system in PowerDMS.

All LEADS security policies apply to agency owned LEADS equipment. All LEADS certified operators have access to terminals. Terminals are only used by members of the Miami Township Police Department with LEADS training and certification. Access to the LEADS system is controlled by user state issued identification number and password, which are set by LEADS. LEADS terminals are not capable of connecting to the Township network and/or the internet. Terminals will only be connected to the LEADS network.

LEADS printouts are exempt from public record and shall not be released except as required to Criminal Justice Agencies, i.e. Courts, Prosecutor. In the event a LEADS security violation occurs, resulting in disclosure of sensitive or classified information to unauthorized individuals, consideration will be given to the extent of loss or injury to the system, agency, or the person, and if the act was intentional or accidental. The Chief of Police will formulate a plan to take action regarding the employee following the disciplinary guidelines established in Directive 26.1.4. In cases where restricted LEADS-obtained Criminal Justice Information is improperly disseminated, the Data Security Officer at the LEADS Control Center will be notified.

Unauthorized modification or destruction of LEADS system data, loss of computer system processing, capability or loss by theft of any LEADS computer system media including: memory chips, optical or magnetic storage medium, hardcopy printout, etc. shall result in the employee being charged with theft as outlined in the Ohio Revised Code 2913.01 and termination of employment with the Miami Township Police Department.

OHLEG

OHLEG (Ohio Law Enforcement Gateway) allows law enforcement personnel access to Computerized Criminal Histories. OHLEG is a secure web-based platform that increases and strengthens law enforcement efforts by promoting open communication and cooperation among the criminal justice community. Through a variety of electronic databases containing a vast array of information, OHLEG allows agencies to share data to prevent and solve crimes. OHLEG does access Computerized Criminal History files.

Law enforcement agencies are provided access under the terms and conditions of OHLEG policies. Participants are required to only use the network to carry out their law enforcement responsibilities, not for personal use or gain. The Chief of Police shall grant authority to employees within the Miami Township Police Department to access the network. Access to the OHLEG system is controlled by username and password, which are set by OHLEG. Improper use by those who are granted access to the Network may result in violation of public records laws, invasion of privacy, lost productivity, or may jeopardize the security of the network.

OHLEG printouts are exempt from public record. In the event an OHLEG security violation occurs, resulting in disclosure of sensitive or classified information to unauthorized individuals, consideration will be given to the extent of loss or injury to the system, agency, or the person, and if the act was intentional or accidental. The Chief of Police will formulate a plan to take action regarding the employee following the disciplinary guidelines established in Directive 26.1.4.