UW Whitewater Police

Records Administration		Number: 82.1	No. Pages: 5
CALEA: 82.1.1, 82.1.2, 82.1.3, 82.1.4, 82.1.5, 82.1.6		Date Reviewed: 2/3/26	Date of Next Review: December 2030
Approved By: Chief Kiederlen	Effective Date: 6/9/2004	Revised Date: 2/3/26	Revision number: 4

I. Purpose

The purpose of this general order is to provide procedures for records administration.

II. Definitions

RMS: The Department's computerized police record management system.

III. Policy

The UW-Whitewater Police Department shall conduct records-related functions in accordance with all applicable state statutes, federal and state regulations, and directives.

IV. Procedure

A. Privacy and Security (82.1.1)

1. The privacy and security regulations of the records section are in accordance with the following:
    a. Wisconsin State Statutes 16.61; Records of state offices and other public records
    b. University of Wisconsin Regents policy documents
    c. Wisconsin State Statutes 19.36; Limitations upon access and withholding records
    d. The Freedom of Information Act (FOIA)
    e. The privacy and security of criminal history record information is in accordance with US Department of Justice regulations, Code 28 Part 20, and as governed through the Crime Information Bureau TIME System Manual.
2. Central records shall be maintained securely. Privacy and security shall be ensured through adherence to the following precautions:
    a. Disseminating information in accordance with Wisconsin statutes and Federal regulations.
    b. Completing reports in an accurate and timely manner.
    c. Auditing records.
    d. Securing files.
    e. Limiting access.
    f. Reviewing entered data.

3. Access to electronic files shall be restricted to Department personnel and key stakeholders (Dean of Students, University Housing, etc.). Records are for official use only; under no circumstances shall reports be copied or removed for personal use.
4. Central records information shall be accessible to operations personnel at all times by physical availability and/or technology. If there is a record that personnel are unable to access, they should call the on-call supervisor.
5. In general, any record generated by the Department is considered a public record. A person or organization that desires a record under this section must file a public record request with the Department. The requestor is responsible for any reasonable cost incurred in reproducing the record. The Department is not required to generate records which do not exist.
6. Persons requesting information should be referred to the full-time clerical staff during normal business hours (8:00 am – 4:30 pm Monday-Friday, holidays excluded) or email police@uww.edu. Records may be requested orally or in writing. If an email request is made, an acknowledgment of the request will be replied to the sender within the next business day following receipt of the request.
    a. Accident reports should generally be obtained through the State of Wisconsin Department of Transportation by accessing their website https://app.wi.gov/crashreports or crashdocs.org.
    b. Electronic copies of other reports will normally be available within ten business days after the request is made.
    c. Requests by other law enforcement agencies for immediate release of records shall be referred to a supervisory officer.
7. When making a public records request, Wisconsin statute prohibits asking persons or organizations to identify themselves or state the reason for the request. Requests should be fulfilled as soon as practicable and without delay. Department personnel are not under an obligation to respond immediately to an official public records request.
8. The department has the authority to withhold or deny public record requests based on the balancing test which is inherent in the Wisconsin Public Records law.
9. Once the department has identified the records responsive to a public records request, the below conditions shall be taken into consideration prior to responding to a requester in regards to withholding or redacting records:
    a. Identifying juvenile information.
    b. Sensitive Crimes victim information (such as stalking, harassment, sexual assault.)
    c. Information that would identify an informant and anyone who has requested anonymity.
    d. Information regarding active and ongoing criminal investigations.
    e. Information on police and crime prevention planning, tactics, and techniques.
    f. Any personally identifiable information that cannot be easily obtained by the average person using other more public means (i.e. social security numbers, dates of birth, driver's license numbers.)
    g. Any medical information, whether it is provided as fact or opinion (including the doctor's names, diagnosis, injuries, treatments, medicines, etc.) that is provided by a health care professional.
    h. Cases involving active drug, organized crime, gang, and prostitution investigations are confidential and shall not be released without approval from the Chief of Police or designee.

i. Other cases in which the department believes the strong public interest in non-disclosure significantly outweighs the public interest

10. Report processing fees may be charged in accordance with applicable state statutes and policies.

B. Juvenile Records (82.1.2)

The following shall establish procedures and criteria for the release of Department juvenile records.

1. According to Wisconsin State Statutes 48.396(1) and 938.396(1)(a) a law enforcement agency's records of juveniles shall be kept separate from the records of adults. Thus, all arrests and identification records pertaining to juveniles shall be marked "juvenile" and maintained separately.
2. Juveniles may also be fingerprinted when arrested or taken into custody as deemed appropriate by the arresting officer. However, photographs, fingerprints, and other forms of identification taken from a juvenile are considered a part of that juvenile's record and subject to the same confidentiality guidelines as other juvenile records.
3. The records supervisor or designee shall be responsible for the collection, dissemination, and retention of Department records pertaining to juveniles.
4. The statutes indicate that the contents of juvenile records may be inspected and their contents disclosed by a law enforcement officer. Officers may have a need for immediate access to juvenile records in the following cases:
    a. Conducting child abuse, neglect, and assault investigation.
    b. Facilitating taking children into protective custody.
    c. Completing referrals to Child Protection for children in need of immediate protection.
    d. Completing referrals to Juvenile Intake for criminal and status offenses.
5. Juvenile records are permanent records and shall remain on file even after the juvenile has become an adult. The juvenile portion of a person's arrest and identification record shall remain restricted, even when the individual reaches adult age. The disposal of all juvenile records shall be accomplished in accordance with guidelines set by the State of Wisconsin after the individual has reached adult age.
6. Expungement of juvenile arrest records can only be accomplished by a valid court order.

C. Records Retention Schedule (82.1.3)

1. The Department follows the Universities of Wisconsin Police and Security records schedule. Adherence to such a schedule shall ensure that electronic data and written documentation are stored and purged in an orderly manner.

D. Incident-Based Reporting System (82.1.4)

1. The Department shall participate in approved state and national crime reporting programs. Such participation assists in effective internal records maintenance and aids in the effort to establish a national database of crime/incident statistics.
2. Department crime data shall be collected via complete incident reports and other resources. Such information shall be entered into electronic systems in a timely manner.

3. Records Staff collects statistical crime data for the FBI required Monthly Report. Monthly reports shall be prepared by Records Staff and shall be sent to the Wisconsin Department of Justice.

E. Report Status Procedure (82.1.5)

1. All calls for service shall be identified through sequential event (control) Computer Aided Dispatch (CAD) generated numbers. In addition to the above-listed event ID, an incident report number shall be assigned for cases involving:
    a. A criminal event
    b. All arrests
    c. Felony, misdemeanor, or non-traffic forfeiture offenses
    d. Death investigations
    e. Potential University liability, such as significant injury caused while on the UW-Whitewater campus, potential release of biological agents, etc.
    f. Incidents as directed by a supervisor,
    g. Incidents that, by their nature, require investigation and documentation.
2. A Field Contact entry shall be done to document contact with identified citizens for incidents that do not meet the criteria for an incident report.
3. Records Staff shall account for the status of initial reports. This tracking may be done through established mechanisms in the RMS database or other reliable means.
4. If a report requires a follow-up investigation by the reporting officer, the officer shall attempt to complete the investigation in a timely fashion. The status of follow-up investigations or reports shall be tracked by the field supervisor. This tracking may be done through electronic mechanisms or other reliable measures.
5. All supplemental reports shall contain the same incident report number as the original investigation and shall receive the same review process as the preliminary case report. The supervisor of the employee responsible for the completion of a supplementary report shall ensure that it is completed in a timely manner.
6. The Assistant Chief or designee is responsible for assigning cases and for investigative case control.
7. Incident reports and supplements shall utilize a classification system to indicate current case status. Such classifications may include: active, inactive, cleared by arrest, unfounded, other, and closed.

F. Computer File Backup and Storage (82.1.6)

The following describes the process for maintaining the security of central records computer systems:

1. RMS files that reside on the RMS database server are backed up on a daily basis. Such backups shall be conducted in accordance with applicable state statutes, record retention schedules, and directives. All backup computer files are secured and stored off-site at the Walworth County Sheriff's Office in Elkhorn, WI. Methods of destruction shall ensure that data is not retrievable from discarded materials.
2. Computer files that reside on the Local Area Network (LAN) (T-Drive) and the records database server are backed up on an hourly, daily, and weekly basis. Such backups shall be conducted in accordance with applicable state statutes, record retention schedules, and directives. All backup computer files are secured and stored off-site. Access to the secure backup computer files is limited to the file owner and select IT staff. Methods of destruction shall ensure that data is not retrievable from discarded materials.

3. Media, disks, drives, or other types of electronic media containing sensitive, confidential, or restricted records that are stored or traveled outside of the physically secured offices of the Department shall be encrypted. Server and workstation hard drives and other media used for central records storage shall be wiped in accordance with CJIS policy, or destroyed.
4. Physical access to the server rooms housing the RMS and central records servers shall be limited to select supervisory and IT personnel. Physical access to workstations connected to the Department network shall be limited to current employees. Electronic access to central records is limited to current Department employees who have passed background checks. Password age and strength levels shall be set and maintained by the server operating system and the FBI's CJIS security policies. Electronic communication or transfer of sensitive, confidential or restricted data outside of the department network shall be encrypted.
5. The department maintains an automated system for verification of passwords, access codes, or access violations.