ACCREDITATION 1.8.1-3
REPORTS AND RECORDS
09/11/2024

GENERAL ORDERS MANUAL
WESTERN MICHIGAN UNIVERSITY
DEPARTMENT OF PUBLIC SAFETY

I. PURPOSE

The purpose of this general order is to establish guidelines for the report writing and review process. This general order also establishes rules for storage, retention and disposal of investigative documents held by the records division or saved electronically in the department's Reports Management System (RMS). Additionally, it will detail the access and security requirements for these documents and software.

II. FIELD REPORTING AND REPORT REVIEW PROCESS (1.8.3)

A. Patrol units use a mobile CAD (computer aided dispatch) software provided by Kalamazoo County Consolidated Dispatch Authority (KCCDA) to document activity, citizen contacts, and initial investigative information. These are logged as CAD events.

B. When a CAD event requires a more detailed report, officers will create a new entry in the department's RMS system, generally as follows:

1. Non-criminal reports (e.g. traffic accidents, suspicious activity, trouble with subject, etc), along with some misdemeanors that result in subjects being released following a citation, are created in a WMU Incident Supp in Mobile Field Reporting

2. Criminal reports, or lengthy reports that could be related to criminal activity, are added to the WMU Case module in Mobile Field Reporting.

C. A supervisor will review each WMU Incident Supp and WMU Case report. Reports are also reviewed by command staff. The reports may be approved or rejected upon review. Supervisors may opt to correct a minor error for the reporting officer. Rejected reports are marked with issues detailing the needed corrections or clarifications. The original reporting officer shall respond to and/or correct the issues then resubmit the report for review.

D. Supplemental reports may be submitted through Mobile Field Reporting by any sworn officer to provide follow-up or additional information not listed in the original report. The reports may be submitted to front-line supervisors or command staff for review. These may be approved or rejected and sent back to the reporting officer for correction and resubmission.

III. LATE REPORTS

A. Officers shall complete all their assigned reports prior to going off duty. Officers shall complete their reports as soon as possible following the initial investigation. If an officer is unable to complete a report prior to going off duty, a supervisor must approve the delay of completing the report. If approved, the officer must complete the late report submission on the 511 website, including the expected date of completion.

B. In the following cases the officer shall complete their incident report prior to going off duty. Overtime is authorized for completing these reports.

1. If an investigating officer is going off duty for more than 3 days.

2. Any serious felony case except property crimes. (e.g., sexual assaults, a death investigation, armed robbery, etc.)

3. A child abuse and neglect case.

4. If a suspect is in custody and an appearance citation has not been issued, and the incident report is needed for prosecutorial or judicial review for a warrant request or bond violation. (e.g., OWI-3RD offense, resisting and obstructing police, domestic violence, etc.)

IV. RECORDS ACCESS AND CONTROL

A. Any paperwork related to case files, including criminal investigations, is to be maintained and secured in a locked cabinet in the records room (room 1313) within the detective bureau. Reports documented in New World CAD or the IDNetworks records management system will be electronically stored. Only department personnel trained in the RMS and CAD system will have access to reports. (1.8.1.a)

B. Detectives, Records Division staff, and supervisors have after-hours access to stored/secured case files. Case files stored in the secured cabinet and room may not be removed without the authorization of the administrative lieutenant in charge of records or the operations administrative lieutenant. (1.8.1.b)

C. Any reports or information pertaining to juveniles, or marked as non-public, are collected, saved, and disseminated only to and by authorized personnel. Incident reports with juvenile involvement with be marked “sealed” in LERMS. When an incident report becomes non-public information, Records Division staff will indicate this in the Related Case Notes field within the report. (1.8.1.c, 1.8.1.d)

D. Release of records must be made in accordance with the Michigan FOIA and applicable court rules pertaining to discovery. (1.8.1.e)

E. It is the responsibility of the Records Division staff to maintain records in accordance with State Archives Certified Retention and Disposal schedule. The State of Michigan General Schedule 11 for Law Enforcement Agencies has been adopted by Western Michigan University Department of Public Safety and can be found in the department’s PowerDMS software. Any disposal of these records must be approved by the Administrative Lieutenant in charge of the WMU PD Records Division, prior to destruction of the materials. (1.8.1.f)

V. INFORMATION TECHNOLOGY SECURITY OF RECORDS DATA

A. The agency RMS contains CJIS data and follows the same FBI/CJIS rules that apply to LEIN and all other CJIS data, as detailed in COM-4.

B. The server hosting the agency RMS is fully backed up every two weeks, with daily incremental backups in between. This backup process includes the database. The server and backup server are separate physical units. (1.8.2.a)

C. The server and backup server are secured in the department server room with access limited to only authorized personnel. Electronic access to the servers is limited to server and software administrators with authorized password access. (1.8.2.b)

D. All RMS users and system administrators have individually identifiable accounts with password protection as required by FBI/CJIS rules. (1.8.2.c)

E. At least once per calendar year a system administrator shall audit the RMS user accounts to confirm each user has proper access and rights. In addition, it is the responsibility of system administrators to ensure accounts are disabled when users are separated from the agency, or when FBI/CJIS rules otherwise require account access be disabled. (1.8.2.d)

F. If a breach of security is discovered, an immediate audit of the RMS system shall take place. All RMS user accounts will be checked to ensure proper access and rights. A short report of these findings will be submitted to the Chief and Deputy Chief by a system administrator. FBI/CJIS and State of Michigan protocols for CJIS a security breach shall also be followed as defined in Com-4. (1.8.2.e)

G. All CJIS software and databases at this agency, including RMS, shall meet FBI/CJIS password requirements. This includes requiring users to change their passwords every 90 days. As part of the annual system security audit, a system administrator will ensure RMS password security settings meet this and other FBI/CJIS rules for passwords. (1.8.2.f)

Issued Date: 09/10/2020, 09/11/2024

Issued by

Scott Merlo
Director of Public Safety