MUSKEGON LAW ENFORCEMENT RECORDS MANAGEMENT SYSTEM
AGENCY USE AGREEMENT

I. PURPOSE

To outline the acceptable use of the Muskegon Law Enforcement Records Management System (MLERMS) by user agencies.

II. OVERVIEW

A. The Muskegon Law Enforcement Records Management System (MLERMS) is the property of Muskegon Central Dispatch 9-1-1 and its member agencies.

B. Access to MLERMS is restricted to member agencies and other criminal justice agencies with an assigned ORI number assigned by the Michigan State Police, Law Enforcement Information Network (LEIN) Field Services Unit approved by the Muskegon Central Operations for Police Services Board, Committee for Records Access/Sharing.

C. The system may only be used for legitimate criminal justice business purposes in serving the interests of member agencies in the course of normal operations.

D. Effective security is a team effort involving the participation and support of each user who deals with information and/or information systems. It is the responsibility of every computer user to understand these guidelines and to conduct their activities accordingly.

III. POLICY

A. Ownership

1. Muskegon Central Dispatch 9-1-1 and the Muskegon Central Operations for Police Services Board desires to provide a reasonable level of access to law enforcement records in an effort to improve information sharing between criminal justice agencies; however, it is understood that:

   a. The Muskegon Law Enforcement Records Management System (MLERMS) is the property of Muskegon Central Dispatch 9-1-1 and its member agencies.
   b. The records created and stored on MLERMS remain the property of the agency creating the record and are considered confidential.

2. Muskegon Central Dispatch 9-1-1 and the Muskegon Central Operations for Police Services Board reserves the right to monitor or audit the network and systems on a periodic basis to ensure compliance with this policy.

B. Access

1. Only agencies and users approved by the Muskegon Central Operations for Police Services Board, Committee for Records Access/Sharing, will be allowed access to MLERMS.

2. Agencies requesting access to MLERMS must:

   a. Submit a completed Acceptable Use agreement.
   b. Assign an Agency Security Officer.
   c. Create and enforce written directives concerning the use of MLERMS which corresponds with this agreement for their respective employees.
   d. Vet and appropriately train its authorized users, including training to the standards established by LEIN.

3. Each person requesting access to MLERMS must:

   a. Complete a MLERMS User Agreement.
   b. Submit a completed Muskegon Central Dispatch 9-1-1 Police Personnel User Form

C. General Use

1. Each agency covered by this agreement shall strictly control the access and release of information residing on the Muskegon Law Enforcement Records Management System.

   a. Each member shall establish procedures for accessing and releasing information in accordance with the Freedom of Information Act (FOIA).
   b. FOIA requests for records not created by the receiving agency shall be denied, as the receiving agency does not own / possess the record.
   c. The receiving agency should advise the requestor to contact the appropriate agency for consideration.

2. It is recommended that any information considered sensitive or vulnerable be “locked” to prevent unauthorized access.

D. System Security

1. The information created and stored on MLERMS is considered as confidential. Users should take all necessary steps to prevent unauthorized access to this information.

2. Authorized users are responsible for the security of their passwords and accounts. Passwords and accounts may not be shared. At a minimum, passwords must be changed every 90 days.

3. All personal computers, laptops, and workstations should be secured with password protected screen savers with an automatic activation feature, set at ten minutes or less, or by logging off (control-alt-delete) when the computer is unattended.

4. All devices connected to the Muskegon Central Dispatch 9-1-1 network shall continually execute approved virus-scanning software with a current database.

5. Users must use extreme caution when opening e-mail attachments received from unknown senders, which may contain viruses, e-mail bombs, or Trojan horse code.

E. Unacceptable Use

1. Under no circumstances is a user of MLERMS authorized to engage in any activity that is illegal under local, State, Federal, or International law utilizing Muskegon Central Dispatch 9-1-1 owned resources.

2. Unauthorized access, copying, removal or dissemination of classified, restricted, or sensitive information including MLERMS, NCIC, or LEIN information.

3. Installation of any copyrighted software for which agency or end user does not have an active license is strictly prohibited.

4. Installation of any software without preapproval and virus scan is strictly prohibited.

5. Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, logic bombs, etc.).

6. Revealing account passwords to others or allowing use of an account by another person.

7. Effecting security breaches or disruptions of network communication.

    a. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties.
    b. For the purpose of this policy, “disruption” includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.

8. Port scanning or security scanning is expressly prohibited unless prior notification has been given to Muskegon Central Dispatch 9-1-1 Computer Services personnel.

9. Executing any form of network monitoring which will intercept data not intended for the employee’s host, unless this activity is a part of the employee’s normal job/duty.

10. Circumventing user authentication or security of any host, network, or account.

11. Interfering with or denying service to any user other than the employee’s host.

12. Using any program/script/command or sending messages of any kind, with the intent to interfere with or disable a user’s terminal session, via any means, locally or via the Internet/Intranet.

13. Providing information or a list of law enforcement personnel or their families, addresses, or other personal information to non-criminal justice agencies or personnel.

F. Enforcement

Any violation of this policy by an agency or user may result in network removal, access revocation, corrective or disciplinary action, civil or criminal prosecution.

I have read, acknowledge, and will abide by the information obtained in this document.

Agency Name		Agency ORI	
Address	City	State	ZIP
Phone Number	Fax Number		
Agency Head Name (print or type)			
Address	City	State	ZIP
Phone Number	Fax Number		
Cellular Phone Number	Email Address		

Please attach a letter on agency letterhead explaining in detail the reason(s) access to MLERMS is needed.

Agency Head Signature	Date
Agency Head Printed	Date

Return completed form to:
Muskegon Central Dispatch 9-1-1
770 Terrace Street
Muskegon, MI 49440