	MEDFIELD POLICE DEPARTMENT	**POLICY NO. 4.21**

INFORMATION SYSTEMS SECURITY

MASSACHUSETTS POLICE ACCREDITATION STANDARDS REFERENCED: **82.1.6, 82.1.7, 41.3.7**	DATE OF ISSUE: 07/02/2023 EFFECTIVE DATE: 07/02/2023 REVISION DATE: 11/03/2025
ISSUING AUTHORITY: Michelle Guerette Chief of Police	

BACKGROUND:

The Medfield Police Department utilizes computer equipment to aid in accomplishing its primary mission of responding to calls for service, preventing crime, apprehending criminals, and documenting incidents. Computers and access to databases supplied by this Department make employees' work more efficient and more accurate.

This policy will serve as a guide to help all employees preserve the integrity of our data, manage the use of computer systems, decrease liability exposure, and prevent unlawful or wrongful actions involving computers and data. This policy supplements the policies and users agreements of state and federal data providers such as LEAPS/NCIC/CJIS and contracted databases.

POLICY:

The Department's information systems are comprised of both mobile data and stationary computer systems that are linked in a closed system. It is the policy of this Department to utilize these information systems to enhance our ability to perform our mission and to improve officer safety through the availability of information while maximizing security protocols and system integrity.

PROCEDURES:

Data Security

All users of the Department's information systems share the job of protecting hardware, software, and data from abuse. The potential for someone (citizen or employee) suffering a loss or inconvenience due to the improper or inappropriate use of the Department's information systems is real, whether malicious or accidental.

The use of Department's information systems and equipment are solely for purposes authorized by the Department. Unauthorized use is a violation of these policies and procedures. The following rules shall be adhered to with regard to the use of the Department's information systems:

1. Software used in the Department's information systems are property of the Department and will not be used, copied, or distributed without permission from the Chief of Police, or his designee, and in compliance with pertinent license agreements and state and federal law.

2. The Department will maintain proprietary rights over any work generated by its members in the course of their duties, and software or files will not be sold, distributed, or maliciously deleted without permission from the Chief of Police, or his designee. The use and distribution of such files will be at the discretion of the Chief or his designee. Employees shall not encrypt data or change permissions of files or folders without the formal approval of the Chief or his designee.

3. Only software that has been approved by the Department, in accordance with operational needs, will be installed on any Information Systems computer. Employees may not download personal software and/or data into an Information Systems computer without review and authorization of the data and/or software by the Chief or his designee. ***[41.3.7(a)]***

4. Employees may not intentionally develop, introduce, or install viruses on any Department equipment or computer.

5. Regular backup of data shall be accomplished at intervals determined by the Chief or his designee.

6. Off-site storage of otherwise irreplaceable data and programs will be conducted as determined by the Chief or his designee. The Department Systems Administrator shall also be assigned to conduct or coordinate an in-house back-up daily, and a weekly backup that is stored inside locally in the secure Department Server Room located in the records office of the police station. The Department also has an offsite backup every hour and every day that is stored with the Town of Medfield' third party vendor. ***[82.1.6(b)]***

7. Data files (word processing, e-mail, and spread sheets) will be backed up if they are stored on the Department server. Backup of data not stored on the server is the responsibility of each user. The Department cannot be held responsible for lost data due to system failure caused by power outages or other problems with the system that may cause an unexpected shut down. ***[82.1.6(a)]***

8. Data maintained or obtained by this Department shall not be distributed in violation of investigative confidentiality or C.O.R.I. Data may be distributed for legitimate law enforcement purposes only. ***[82.1.7]***

Network Security

Access to the Department's Information Systems network will be limited to those with a legitimate need to use the system to access or input data as determined by the Chief of Police or his designee. Each authorized user of the systems will be issued a login name and password and receive basic training in the use of the system. Users are responsible for maintaining the security of their passwords, and should never share them with anyone, including other employees. Passwords may be changed whenever a security infraction has been discovered or periodically to ensure security. Passwords shall be changed at least annually and passwords shall be audited annually. The appearance of passwords on terminal screens and printouts are suppressed. ***[82.1.6(c)(d)] [82.1.7]***

The Department shall provide various layers of protection to safeguard data and software from unauthorized access. These security measures include:

1. Servers and routers shall be located in a locked or secure area to avoid physical illegal, unauthorized access to this hardware.

2. Detection of illegal penetration and prevention of unauthorized access to the data processing systems.

3. Prevention of unauthorized access to stored data.

Supervised access to the network by vendors, maintenance technicians, and contractors may be allowed on an as needed basis, and only with permission of the Chief or his designee.

Mobile Data Computer Access & Restrictions

Mobile Data Computer (MDC) access is available for use while in a cruiser. The MDC provides access to the Department's Information Systems, LEAPS, CJIS, and CORI. See the Department policy on **CORI – Criminal Offender Record Information.** In addition to the data security and network security procedures listed above the following procedures shall be used with regard to MDC's:

1. Mobile communications and transactions, as well as chat functions, will be recorded and logged. All such functions shall conform to FCC guidelines regarding radio transmissions and shall not contain improper language or subject matter. MDC to MDC communications shall be limited to communication which is relevant to Department activity.

2. All MDC transactions shall be in accordance with NCIC and CJIS guidelines and all users must be certified in such use. Federal law, title 28 regulates access and

dissemination of NCIC/LEAPS records. All inquiries made using a MDC are subject to these guidelines. No information received through any state, national or record management system (RMS) database will be released to any unauthorized individual.

3. Tampering with computer settings is prohibited. This includes, and is not limited to, RMS settings, and any settings that relate to any hardware previously installed in or on the MDC, or any component thereof. ***[41.3.7(b)]***

4. The MDC shall not be used to access or attempt to access internet sites not previously approved by the Chief or his designee.

Any user who finds a potential lapse in security on any system shall be obligated to report the potential lapse to the System Administrator forthwith. The system(s) shall then be taken out of service until the System Administrator can investigate the problem.

Knowledge of passwords in computer security systems shall not be used to damage computer resources, obtain additional access, take access away from another user, gain unauthorized access, or otherwise make use of computing resources for which proper authorization has not been given. Violations of this policy may be criminal and punishable under Massachusetts General Law Ch. 266 Sec. 120F.

Mobile Data Computer Use

Officers may obtain information through the MDC via CJIS, however, the MDC is not a substitute for radio communication with the Dispatch. Officers will notify Dispatch via radio of all stops or interactions with the public and must verify any “hit” (warrant or revoked license/registration) through Dispatch to confirm accuracy. The following rules and procedures apply to the use of a Department MDC:

1. At the start of the shift, patrol officers shall check the MDC while completing their routine vehicle check. Officers shall log onto the assigned MDC and shall remain active on the system for their entire tour. Any problems or damage shall be reported to the Shift Commander immediately. The Shift Commander is responsible for notifying the System Administrator of any problems.

2. No food, beverage or any other substance that may inflict damage will be placed on or near the MDC.

3. Officers shall be responsible for any damage to the MDC during their tour of duty. This includes damage caused by neglect, misuse, mistreatment or malicious treatment of the MDC.

4. Only a stylus pen or a clean finger may be used to operate the touch screen. Use of any other object to activate the touch screen is prohibited as it may damage the screen display.

5. Use of cleaning solvents and liquid based products on the computer is prohibited. Fingerprints may be wiped from the screen with a soft cloth. If further cleaning is required, advice should be sought from the System Administrator.

6. The MDC will operate in cold and hot conditions due to its rugged design, however, the MDC should be removed from the vehicle when it is anticipated that the vehicle will be out of service for an extended length of time (i.e. out of service, disabled). The MDC should also be removed when the temperatures are predicted to be below 10 degrees Fahrenheit. During the colder months, the MDC should be allowed to warm in a heated vehicle for 20 minutes prior to use.

7. If the MDC is not working:

a. Check to see if other officers' MDC's are having similar trouble.
b. Check to see that the power light is on.
c. Check with Dispatch to verify server status or CJIS status.
d. If trouble persists, notify the System Administrator.

8. Officers must log off of the MDC at the end of their tour and turn off the computer.

Mobile Data Storage

All communications and queries shall be recorded and archived at Police Headquarters. The Department may conduct system audits as necessary. This includes all queries, messages, chats, and other communications via the MDC. This information is subject to administrative review and subpoena in both civil and criminal matters. All records of NCIC query information will be maintained for 2 years. After this time all records shall be destroyed. All other logs shall be maintained for 1 year.

MDC Audible Alarm

Each MDC is equipped with an audible alarm device so that officers can be notified of pertinent messages or announcements. The audible alarm setting on all terminals shall be left on. No officer shall mute, turn off or disable the alarm(s).

***In the event that a query results in a NCIC/LEAPS "hit" response, all on-line users will receive an alarm. Only dispatchers may conduct a verification of the "hit" and print out a hard copy via the CJIS system in Dispatch.