23.00.170 MOBILE DATA COMPUTERS (CALEA 41.3.7)

Principle: Designated Bellevue Police Department staff have been issued or may occasionally use Mobile Data Computers (MDC's) that allow for transmission of electronic messages both computer to computer, multi-computer, between computer and City of Bellevue network, and between computer and NORCOM's Computer Aided Dispatch System (CAD).

The MDC's have been issued to staff to enhance the efficiency of the officers on duty. They are intended for police operations and not as a personal communication tool. Users of the MDC shall be ACCESS certified and follow the rules and guidelines as set forth in this Standard.

Policy

User Agency Access Policy: City of Bellevue is the owner of the MDC and operating software, and connectivity and thereby have primary responsibly for maintaining the integrity of those systems.

NORCOM is the owner of the New World/Tyler systems and thereby has primary responsibility for maintaining the integrity of those systems.

While NORCOM does not have the authority or the desire to dictate user agency policy or suggest disciplinary action, NORCOM does reserve the right to restrict or deny system access should professional standards not be met by a user agency.

No employee shall knowingly make use of or access any computer equipment to which he/she is not authorized.

Should the individual actions of a User necessitate potential limitations or denial of usage of the system, the severity of the violation(s) will determine whether a warning is issued to the User Agency or whether it is brought before the Joint Operations Board for a decision to deny access.

An agency may petition the Joint Operations Board for a User's reinstatement to the system at such time they determine no further violations will occur.

User Agency System Access: Any time a determination is made that an employee is not to have access to the system whether temporary or permanent, a supervisor shall notify NORCOM techs to ensure that the CAD Security File is updated.

Electronic Messaging: NORCOM is equipped with a CAD/Mobile software system that allows for the transmission of electronic quick messages and computer to computer or multi-computer message sending. The system is intended for the enhancement of NORCOM operations. NORCOM owns the MDC software system, New World that interfaces with the CAD System. The Washington State ACCESS System for Police Departments is also in place at Bellevue Police Records and NORCOM. Strict rules and guidelines apply. Refer to ACCESS Manual.

Practices:
Use of the MDC equipment in a moving vehicle is inherently dangerous. Officers using this equipment while operating a motor vehicle must exercise caution and avoid potential distractions created by the use of the MDC. Should a collision occur related to the use of the MDC, the policy/procedure related to City vehicles involved in a collision will apply.

Members of the Bellevue Police Department may use the MDC's only for official business. Message sending capabilities shall not be used for transmission of information that promotes discrimination on the basis of age, gender, marital status, race, creed, color, religion, national origin, sensory, mental or physical disability, or sexual orientation. It shall not be used for the following activities, including but not limited to:

- Sexual harassment.
- Personal political or religious views.
- Any unlawful activity.
- Union business.
- Personal opinions or comments regarding a call.

No one but trained, authorized members of the Bellevue Police Department shall access or otherwise make use of the MDC's.

No member shall attempt, in any manner, to circumvent the security system of the MDC.

No member shall tamper with, or attempt to repair, any hardware component for which he/she has not been specifically trained and assigned to maintain and/or repair.

No member shall modify, reconfigure, add to, or delete from any software application, operating system or peripheral device unless specifically trained and assigned to do so.

No member shall knowingly make a fictitious, unauthorized, anonymous, or inaccurate entry into the MDC data base and/or message handling system.

No member shall knowingly make use of, turn off, or log off any computer terminal to which he/she is not logged on without permission from a supervisor or commander.

No member shall make use of any other individual's security password as a means of security access to any computer.

No member shall record, disseminate, or cause to be recorded and/or disseminated, any record or records of system security passwords or devices of other persons without the expressed written permission of the Assistant Chief or his/her designee.

Any member who has cause to believe that the computer system security, security file and/or integrity has been violated, compromised, or jeopardized, shall immediately report the same to his/her supervisor or commander.

Responsibility:

Employees have no expectation of privacy when utilizing the MDC.

Electronic messages cannot be protected against unauthorized access caused by:

- User's failure to maintain password security.
- Devices logged onto the system, but left unattended by users.
- Messages forwarded to others by recipient.
- Messages printed at locations where individuals other than the intended recipient may view.
- Messages directed to the wrong recipient.
- Messages saved/stored by the member prior to logging off the system and/or leaving their computer.

It shall be the responsibility of the supervisors and commanders to enforce this policy and to monitor messages being sent by employees.

- The Watch Commander will be responsible for routinely monitoring MDC messaging to ensure compliance with professional standards and policy.
- As part of an Administrative Investigation, a supervisor or commander shall take action to gather facts and may review and/or monitor messages being sent.
- Unless the member has a designated take home vehicle, no member shall take MDC from the station when not on shift without prior permission of their supervisor.
- MDC shall be stored in designated carts in the patrol area, machines are to be “shut down” (power off) and placed in cart with blue network cable connected.

<u>Procedure</u>

Dispatching Incidents:

Under normal circumstances, the basic information on all incidents will be dispatched verbally. Incidents should not be sent from NORCOM to an MDC without a verbal advisement to the assigned unit(s).

Under special circumstances where verbal communication would jeopardize the effectiveness or safety of an incident, total MDC communication may be utilized.

All verbal transmissions from responding units that change status or location will be recorded by NORCOM, regardless of the MDC capability of the responding unit. NORCOM should not assume nor expect responding units to record critical information in the CAD System.

Priority one (1) through three (3) incidents will be dispatched verbally and via MDC in their entirety. Priority four (4) and five (5) incidents may be dispatched via MDC with minimal information verbalized to the officer (i.e., "1B2, a Theft Report MDC").
NORCOM will ensure the officer(s) acknowledge the advisement.

NORCOM should pay special attention to transactions to remain aware of officer location and status. As with non-MDC equipped units, status checks will be performed accordingly.

Should an MDC unit not respond to a transmission requiring a response, NORCOM will attempt to gain the attention of the unit by verbalizing the unit number, followed by the phrase "Acknowledge MDC". In the event the officer does not respond, NORCOM will attempt to ascertain the unit's status. Should this attempt fail, immediate back-up shall be dispatched to the unit's last known location.

<u>MDC User Procedures:</u>

- **Routine Transmissions**
  Responding units may initiate all routine status changes, such as en-route, on-scene and clear.
- **Critical Transmissions**
  Critical requests should not be made via MDC, such as a law enforcement request for a fire/EMS response or a request for backup or assistance. Units should also avoid "silent" transmissions on important tasks to allow units without an MDC to monitor activity.
- **On-View Incidents (Traffic Stops)**
  Officers utilizing the on-view function of the MDC shall verbalize the incident to NORCOM and identify their intent to initiate the CAD incident themselves by immediately following the advisement

with the term MDC (i.e. "1B2, Traffic MDC"). The fact that an incident was on-viewed through an MDC does not change NORCOM staff responsibility to check officer status and respond accordingly.

Recommended practice: Continue to call out traffic stops on the air.

ACCESS

Please refer to 27.00.020 MISUSE OF RECORDS OR INFORMATION

Terminal Security

All users are responsible to ensure the security of the terminal sites and information received. Terminal locations must be secured with two factor authentication from unauthorized access, and all employees authorized to use the system shall be instructed on the proper use of equipment and the dissemination of information received.

Technical Agency Coordinator

The Major of the Administrative Services Section shall designate a Technical Agency Coordinator (TAC) to act as the point of contact for the WSP and the Federal Bureau of Investigation (FBI). The individual designated to function as a TAC must meet all WSP requirements for TAC's. TAC responsibilities include but are not limited to:

- The Department contact for audits conducted by the ACCESS audit staff;
- Responsibility for proper operator performance and strict adherence to regulations;
- Prompt notification of violations to the ACCESS Section;
- Ensuring proper training and certification

Reporting of Equipment or Connection Problems

Each user is responsible for the reporting of any problems with individual MDC unit or connection to City of Bellevue Support. If the AVL (Automatic Vehicle Locator) system is down, NORCOM Center Dispatchers/Supervisors will notify the Information Technology Department, and the on-duty patrol supervisor.

If you are unable to broadcast using your radio because of a poor coverage area, you can move to an area with better coverage or use an alternate form of communication such as your cell phone, MDC or a land line. If you locate an area of poor coverage, report this area immediately to Dispatch so they can document and schedule a radio technician to resolve the issue.