A. Policy

It is the policy of the police department to adhere to City administrative regulations and copyright protection laws concerning software licensing and use. Compliance is necessary to protect critical computer systems within the department from damage and to protect system users from liability.

B. Procedure

1. All software purchases are to be made through established purchasing procedures, utilizing purchase orders.

2. City controlled acquisition of shareware is permitted provided that the author is paid the requested fee and that registration is handled in the same way as for commercial software products.

3. All software will be first delivered to the City Information Management Services Section before installation so that unsuitable software can be avoided, registration can be accomplished, and appropriate records kept.

C. Rule

1. Only software that has been acquired and registered by the City may be installed on any City computer.

2. No personal software, whether or not such use complies with the licensing agreement, may be installed on a City owned computer.

3. A back-up copy of original diskettes is to be made by the person installing the software.

4. Employees may use City owned software at home only if it is permitted by the licensing agreement and prior approval has been obtained from the employee's supervisor.

5. Except for back-up purposes, City employees may not duplicate any licensed software or related documentation for use either on or off City premises, unless the employee is expressly authorized to do so by agreement with the licensor.

6. Software may be used on local area networks or on multiple computers only in accordance with applicable license agreements.

7. No employee may give or lend software to any other organization, vendors, other employees, volunteers or members of the public.

8. No addition to or modification shall be made to any installed software by anyone not identified as a system administrator for the police department.
A. Policy

Mobile data terminals are provided as a resource to aid authorized personnel in the course of their police investigations. Various types of data can be accessed using MDTs. Information requested via MDTs shall be limited to official police inquiries only.

B. Procedure

1. Authorized MDT information consists of CCIC and NCIC files, Department of Revenue files, CAD screens, the Lakewood Automated Reporting System, electronic mail, car-to-car messaging, and car-to/from-dispatch messaging. Access to CCIC, NCIC and DOR files may be limited depending on the individual user’s OSN privileges.

2. Passwords and password security are the sole responsibility of the authorized user.
   a. To enhance security, passwords shall not be badge or employee numbers.
   b. Individual passwords shall not be provided to any other person.

3. Operator security numbers (OSN) and associated use are the sole responsibility of the authorized user.
   a. OSNs shall not be provided to any other person.

4. Sworn supervisory personnel and agents assigned to the Personnel Investigation Unit shall have, or be provided, access to any MDT record for investigative or other authorized purposes.

5. The Internal Affairs Unit shall be responsible for conducting random audits of car-to-car messaging, car to dispatch messaging and dispatch to car messaging on a quarterly basis to ensure compliance with departmental guidelines for MDT messaging.

C. Rule

1. MDTs shall be used for official purposes only.

2. Information obtained through the use of MDTs shall not be shared with any individual not having authorization or a need to know or receive that information.

3. No floppy disks, PCMCIA cards, CD-ROM, tapes, etc., shall be utilized on or with the MDTs unless provided by the department for a specific purpose.

4. No software, firmware, or code shall be utilized, installed, modified, activated, or deactivated by any MDT user. Only the previously mentioned applications may be activated and utilized by the user. No modifications are permitted, including screen displays, fonts, colors, sound, data files, and related effects. Software shall be installed only by authorized system administrators.

5. Language used on the MDT system shall be professional in nature.
6. When leaving a vehicle equipped with an MDT unattended, user personnel shall ensure that the vehicle is locked.

7. Caution should be used when accessing information from CCIC, NCIC, or DOR files when a prisoner is in the patrol car or a civilian ride-along is present. This information is privileged and for authorized users to view only.

3740 Newcom CCIC/NCIC/DOR INTERNET ACCESS

A. Policy

Unless authorized by a supervisor, Internet access to Newcom from a location outside of a City of Lakewood facility is prohibited. If access is necessary and approved by a supervisor a public or shared computer shall not be used for such access.

B. Procedure

1. Authorized Newcom information consists of CCIC, NCIC and Department of Revenue files. Access to these files may be limited depending on the individual user’s OSN privileges.

2. Passwords and password security are the sole responsibility of the authorized user.
   a. To enhance security, passwords shall not be badge or employee numbers.
   b. Individual passwords shall not be provided to any other person.

3. Operator security numbers (OSN) and associated use are the sole responsibility of the authorized user.
   a. OSNs shall not be provided to any other person.

4. Sworn supervisory personnel and agents assigned to the Personnel Investigation Unit shall have, or be provided, access to any CCIC record for investigative or other authorized purposes.

C. Rule

1. Newcom shall be used for official purposes only.

2. Information obtained through Newcom shall not be shared with any individual not having authorization or a need to know or receive that information.

3. When leaving a Newcom workstation personnel shall ensure they log off Newcom or lock the computer.