POLICY 205

EFFECTIVE DATE 12-01-14

Eugene Police Department

Criminal Justice Information System (CJIS)

205.1 PURPOSE AND SCOPE

We have a duty to safeguard personal information from unlawful or unauthorized usage. The following guidelines are established for the use and security of the following: LEDS terminal, Mobile Data Terminal (MDT), and other related CJIS information. Failure to comply with this policy can result in disciplinary action. This policy governs any Department employee or volunteer with access to a LEDS terminal, MDT, or any other piece of equipment that relays CJIS information.

205.2 CJIS SECURITY POLICY

It shall be the policy of Eugene Police Department to protect the integrity of the LEDS database and all data and information obtained through use of Mobile Data Terminals and/or hard-wired LEDS terminals by strictly following the procedures outlined in this policy. Data accessed through the system will only be used for assigned law enforcement duties. No unauthorized personnel will have access to the data and the data will never be used for personal gain, nor will it be reviewed or disseminated except for legitimate criminal justice or training purposes.

205.3 DEFINITIONS

LEDS Terminal – This term includes all computers (desktop or laptop) that have access, via wireless or hardwired networks, to LEDS, NCIC, or any other law enforcement database.

MDT - Mobile Data Terminal; this includes all vehicle-mounted computers that have access, via wireless or hardwired networks, to LEDS, NCIC, or any other law enforcement database.

Secure Location - This term includes the areas of Eugene Police Department that are not open to the public and that are accessible by authorized personnel. This term also includes official police vehicles that are locked and/or attended by authorized sworn police personnel.

Non-secure Location - This term includes all other locations not specified by “Secure Location.”

205.4 CJIS SECURITY PROCEDURES

a. When accessing CJIS, LEDS, and NCIC data from internal non-secure, secure locations, encryption shall be employed.

b. Each person authorized with physical or logical access to Terminal/MDT data shall receive security awareness training within six months of appointment or employment and thereafter at least every two years, in accordance with CJIS policy; this training will be documented.

c. Maintain a roster and/or agency-issued credentials (officer badge, access card, etc.) of authorized personnel with unescorted access into physically-secure areas.

d. Only authorized ISD or EPD technical support personnel, or authorized CJIS-approved vendors are allowed to install, remove, or change component devices, network connections, and remove or alter software and other programs.

e. When transporting non-law enforcement personnel in police vehicles, officers will close the screen of the MDT or position it in a manner that will prevent unauthorized viewing of MDT data. LEDS terminal screens shall be positioned to prevent unauthorized viewing.

f. When utilizing remote support, users shall log out of all public safety systems. Remote support for public safety systems must be documented.

g. User/Operator List shall be reviewed annually and as needed. Documented changes will be retained for a minimum of one year. Changes in authorized personnel will be immediately reported to LEDS Training section.

h. All printouts of CJIS data shall be promptly filed with the corresponding incident records. Otherwise, such printouts should be promptly shredded. Disposal or destruction is witnessed or carried out by authorized personnel.

i. The Department shall keep a list of all MDT IDs and contact(s) so that devices can be promptly disabled, should the need arise.

j. The local CJIS network equipment shall be located in a physically secure location.

k. All law enforcement vehicles containing MDTs shall be securely locked when not in use.

l. All computers used for processing CJIS data shall have anti-virus software installed; all will have latest available updates for the operating system & anti-virus. MDT(s) shall have a personal firewall enabled.

m. It shall be the responsibility of each authorized user to report any violations of this security policy up the chain-of-command and/or proper authorities with an immediate email to the **Eugene Police Security Administration* email group, which will initiate the steps of the formal incident response plan.

n. No personal electronic devices (PC, personal laptop, personal iPad) or software shall be allowed on the agency's LEDS network.

o. No personal software or applications (games, etc.) shall be allowed on the department's LEDS network.

p. No publicly-accessible computers shall be allowed on the agency's LEDS network.

q. EPD shall authorize and control information system-related items entering and exiting the physically-secure location.

r. EPD shall abide by the City of Eugene Information Services Security Alert and Advisories process. For further details, see the ISD Incident Response policy.

s. During regular business hours, users will not access concurrent LEDS sessions. Approved exceptions must be approved and documented by the TAC.