LITTLE ROCK POLICE DEPARTMENT
GENERAL ORDER

G. O. 112 COMPUTER INFORMATION SECURITY

DATE:	DISTRIBUTION:	REPLACES:	NUMBER:
12/13/2023	DEPARTMENTAL	09/26/2023	G. O. 112

I. General

A. All police computer systems, (including but not limited to the Records Management System (RMS), Computer Aided Dispatch system, Mobile Data Computers, Workstations, Laptops, Notebooks and the City-wide network, hardware and software, are for the official use of Police Department employees and are intended to improve the efficiency and effectiveness of departmental operations.

B. Operation of the above systems must be in accordance with established security measures as described in City of Little Rock Administrative Personnel Policy and Procedures Manual, and as outlined below. Access shall be limited by security settings as determined by the employee's Division Commander and training level. Records and information maintained by the Little Rock Police Department are for the exclusive use of departmental employees only and shall not be disseminated to persons who are not affiliated with a bona fide law enforcement agency or as directed by command supervisors.

II. Security for Computer Systems

A. Each employee must complete the Network Users Agreement in order to gain access to the systems they will need to accomplish their assigned tasks. The completed forms shall be forwarded to the LRPD Information Systems Coordinator (ISC).

B. The Information Systems Coordinator (ISC) serves as the Arkansas Crime Information Center (ACIC) Terminal Agency Coordinator (TAC) for the Little Rock Police Department and any other City of Little Rock departments that access ACIC. The ISC shall immediately be notified of any newly hired employees of the Little Rock Police Department, Little Rock District Courts, City Attorney's Office, and the 911 Communications Center. Additionally, the ISC shall be notified when any City employee transfers into one of the above-listed departments or is a newly appointed Little Rock Fire Department Investigator. Upon notification of a newly hired or transferred employee, the ISC will determine if the employee will be directly accessing the Arkansas Crime Information Center (ACIC) or if the employee will only have access to criminal justice information (CJI). If the employee will need direct access to ACIC, the ISC will configure the employee in the ACIC system and email a link to the employee to take the required Security Awareness training and test that are prerequisites to being enrolled in the ACIC Basic class. Once the employee completes the required prerequisites, the ISC will enroll them in an ACIC Basic class. If the employee will not need direct access to ACIC and they will only have access to criminal justice information, the ISC will configure the employee in the CJIS Online system and email a link to the employee to take the required CJIS Security Awareness training and test. All employees (full and part-time), interns, and volunteers working in any of the above-listed agencies must complete CJIS security awareness training within their first thirty (30) days of employment.

Prior to configuring any employee in ACIC or CJIS Online, the ISC will confirm the employee has a current fingerprint-based background check on file, ~~and~~ perform a criminal history check on the employee via ACIC/NCIC, *and ensure the completion of required CJIS identity proofing procedures. Identity proofing shall be completed during the new employee's first five (5) days of employment as part of the on-boarding process and shall conform to FBI CJIS Division standards.*

C. The ISC or designated Technology and Equipment Section personnel shall be the only departmental employees authorized to determine, based upon the employee's duties and level of training, the level of access to the Police R.M.S., LRPD Incident Report Direct Entry system, Arkansas Crime Information System, National Crime Information System, CJIS Online, Computer Aided Dispatch System, Mobile Data Computers (M.D.C.), Court Connect, and MOVEAR/CAPSLOCK.

D. Each employee who seeks access to any police system shall do so with their own unique User ID number and password and shall access only those files and records as specified by their security level and job description. When not in use, systems shall be locked using the Windows software application or logged off to prevent unauthorized entry.

1. No employee shall attempt to modify any record or file which would be illegal or which tends to impair the operation of this department in its administration of justice. No employee shall attempt to make changes to or delete any file or record contained in the R.M.S., the Arkansas Crime Information System, the National Crime Information System, or the Computer Aided Dispatch System without proper authorization.

2. All entries, inquiries, modifications and attempted deletions are recorded in electronic logs which are maintained by the Office of Information Technology and reviewed on a semiannual basis by an employee designated by the Chief of Police.

3. Any discovered attempt to modify or delete any file or record, or the removal or disabling of any security software installed, which tends to impair the operation of this department, will be documented and forwarded through the Chain of Command to the Technology and Equipment Section.

E. No employee shall use another employee's Network User ID and password nor shall any employee attempt to secure the User ID and password of another employee. Only the employee or their supervisors, after verification of identity, shall receive User ID and password information. Unauthorized attempts to obtain such information shall be reported to the offender's Division Commander for investigation.

1. Passwords, access code assignments, file permissions and access violations shall be audited on an annual basis.

F. Those employees who have State and National computer system security shall access those files and records in accordance with specific training provided for the use of the State and National computer systems.

1. Information retrieved from State and National computer files and the National Law Enforcement Telecommunications System (N.L.E.T.S.) is intended for official police-use only and the dissemination of this information to noncriminal justice individuals is strictly prohibited and could subject the offender to criminal and civil penalties [A.C.A. § 12-12-212].

2. Each employee who has State and National computer access must be recertified every ~~two years~~ *year* to maintain security authorization. Failure will result in immediate suspension of access and the employee will be required to attend the *ACIC* Basic Terminal Operator course to obtain *re*certification.

3. Any employee who disseminates criminal history information *outside the LRPD organization* from any State or National computer system must log that dissemination into a Criminal History log that shall be maintained within areas where State and National Criminal History information may be gained.

   a) Dissemination of criminal history information as described above must be to criminal justice officials, outside the LRPD organization, authorized to receive criminal history information.

   b) The criminal justice official receiving the information must be identified by organization, name, employee number or social security number, address and phone number along with the date and time the information was disseminated.

   c) Completed criminal history log sheets shall be maintained in the criminal history logbook until such time as the designated members of the ACIC Terminal Agency Coordinator, (T.A.C.) collects them.

   d) Criminal history logs must be available for inspection during normal business hours.

4. All requests for new R.M.S. programs or applications, the modification of current programs or applications or the addition of information to code tables effecting any R.M.S. application shall be forwarded through the employee's chain of command to the Technology and Equipment Lieutenant.

   a) Only employees designated by the Chief of Police are authorized to contact the Office of Information Technology Programmers and request changes or modifications to any system.

   b) Unauthorized attempts to change or modify any program or application shall be documented by O.I.T. and forwarded to the Office of the Chief of Police.

5. The Information Systems Coordinator, in conjunction with the Records Compliance Specialist, will ensure compliance with all requirements set forth by ACIC and NCIC Policies and Procedures, Departmental General Orders, CALEA Standards, and will review all requests.

6. All requests for assistance, investigation of file activity or mistakes on the part of any employee or specific user information, from the Office of Information Technology, shall be routed through the Technology and Equipment Lieutenant.

G. Any supervisor who needs additional training for their employees or any employee who desires additional training on the R.M.S., Arkansas Crime Information System, the National Crime Information System, the Computer Aided Dispatch System, or the Mobile Data Computer, should contact the Technology and Equipment Lieutenant to schedule the requested training.

H. To be in compliance with Criminal Justice Information Services (CJIS) best practices, all employees of the Little Rock Police Department shall be fingerprinted every five (5) years, and the LRPD encourages all other City Departments whose employees have access to criminal justice information to implement a similar policy.

III. Special Investigations Computer Systems

A. A Systems Administrator, designated by the Special Investigations Division Commander, will be assigned the responsibility for all computer security, access and the operation of computer systems unique to the Special Investigation Division. Each employee will use a unique password and system login as designated by the Systems Administrator.

B. The Systems Administrator shall be the only division employee authorized to issue user login and passwords and shall determine, based upon the user's duties, the level of access to computer systems unique to the Special Investigations Division.

1. The Systems Administrator will maintain and audit on a quarterly basis the login files for unauthorized access and the completeness of the password list.

C. The Systems Administrator shall be responsible for backing up computer systems located in the Special Investigations Division on a weekly basis. Other backup routines may be performed as needed. Backup tapes will be stored off premise in a lockbox maintained by the Special Investigations Division.

IV. Mobile Data Computers

A. General

1. Mobile Data Computers have been installed in police vehicles to assist officers in the execution of efficient police functions and to reduce the amount of radio traffic necessary to conduct police operations.

2. Officers have been trained in the use and care of the Mobile Data Computer and are expected to use this equipment in accordance with instructions provided. Mobile Data Computers were designed and have been programmed to provide information from local, State and National computer files on persons, vehicles, and other property.

a) Officers shall use the Mobile Data Computer to check information on persons, vehicles, and other property and shall not request Central Communications conduct these types of transactions.

b) The only exceptions to this Order will be when an officer needs a printout of the information for inclusion with other reports or does not have a Mobile Data Computer or the Mobile Data Computer is not functioning properly.

c) If the unit is not functioning properly, officers are expected to request repairs as soon as possible during the normal working hours of the Office of Information Technology or the next business day the Office of Information Technology is open.

d) Employees will not change any settings on the computer which disable or interfere with its normal functions.

3. Officers shall log on with their designated User ID and password. Officers shall not use another employee's User ID and password to obtain access to the system. At the end of shift, officers shall log off the Mobile Data Computer system.

V. Departmental Workstations and Laptops

A. The use of all departmental computer systems shall be for official police business only.

B. Employees shall ensure all computer equipment is kept clean and shall request necessary repairs or replacement through the Information Systems Coordinator, or any person authorized to submit a Help Desk ticket, who shall submit a Help Desk ticket to the Office of Information Technology.

1. Employees who experience difficulties logging into the City-wide network may call 918-5288 and ask the Help Desk person to assist the employee gaining access to the Network.

a) Requests for repairs, changes to software applications, folder permissions and any other computer request*s* will be directed to the Information Systems Coordinator or any other police department employee who is on the IT Approval List with authority to add network profiles, new computer hardware and software, etc. The IT Approval List can be accessed via the Little Rock Intranet.

C. Many departmental workstations and laptops have been designated to be used by specific individuals. The unauthorized use of departmental workstations or laptops or the unauthorized deletion of files or applications is not permitted without authorization from a supervisor.

D. The introduction of non-City approved computers into the City-wide network or the introduction of unauthorized programs, applications or viruses into any City computer system is strictly prohibited.

E. All departmental workstation computers and laptops are subject to be inventoried by authorized employees and all programs on any departmental workstation computer or laptop must be authorized and have appropriate documentation to verify license authenticity.

F. Personnel of the Office of Information Technology must conduct an evaluation of outside software and data disks before such software is added to any workstation, laptop or Mobile Data Computer.

1. To request assistance for additions of software and modification of current operating systems, contact the Information Systems Coordinator.

Additions and revisions are *italicized and underlined*.

Deletion are denoted with a strike through.