California State University
NORTHRIDGE
Department of Police Services

POLICY/PROCEDURE NUMBER: 07-O.A.-006 Page 1 of 16

SUBJECT: RECORDS ADMINISTRATION

EFFECTIVE DATE: December 18, 2019 REVIEW DATE: December 18, 2020

AMENDS/SUPERSEDES: Training Bulletin, *RECORDS UNIT PROCEDURES – **RESTRAINING ORDERS**, July 1, 2004;* Training Bulletin, *RECORDS UNIT PROCEDURES –**SUBPOENA**, July 1, 2004;* Training Bulletin, *RECORDS UNIT PROCEDURES-**VALIDATIONS**, July 1, 200;* Procedural Directive #2004-11, *Citation, DL310 Form, Restraining Order, CLETS/JDIC Teletype Processing Update*, October 6, 2004; February 12, 2007 version; January 27, 2010 version; February 16, 2011 version; January 8, 2014 version; January 7, 2015 version.

IACLEA STANDARDS: 16.1.4, 16.1.7, 16.1.10, 16.1.11, 16.2.1, 16.2.2, 16.2.3

CSU POLICE SYSTEMWIDE POLICY – NO

APPROVED: Gregory L. Murphy, Chief of Police

I. PURPOSE

The purpose of this directive is to establish the policies and procedures of the records unit administrative function that are basic to the management, operational, and information needs of the agency and to provide the department at large with a definitive records retention schedule. The records unit of the university police is the central repository for paper copy records, unless otherwise specified within this policy, and shall function in accordance with agency policy and state and federal laws pertaining to privacy and security precautions as they relate to agency records and criminal history information.

II. POLICY

California State University, Northridge uses an online Records Information Management System (RIMS) that links the communications center dispatching, law enforcement field reporting, police records, evidence, and investigative case management. The records unit is integral to the effective delivery of law enforcement services.

III. DEFINITIONS

A. Authorized Person or Agency: Any person or agency authorized by court order, statute, or decisional law to receive CORI
B. CCHRS: Los Angeles County Consolidated Criminal History Reporting System
C. CLETS: California Law Enforcement Telecommunications System

D. CORI: Criminal Offender Record Information
E. Criminal Justice Agency: Any person or component thereof that performs a criminal justice activity as its principal function
F. Criminal Justice Information: Records and data compiled by criminal justice agencies for purposes of identifying criminal offenders; summaries of arrests; pretrial proceedings; the nature and disposition of criminal charges; sentencing; incarceration, rehabilitation and release
G. CJIS: Criminal Justice Information System
H. DVROS: Domestic Violence Restraining Order System
I. EPO: Emergency Protective Order
J. JDIC: Justice Data Interface Controller
K. Juvenile Records: Those records pertaining to an individual under the age of eighteen (18)
L. NCIC: National Crime Information Center
M. Need to Know: CORI is essential to complete official duties
N. OAH: Orders After Hearing (restraining orders)
O. Records Check: Retrieval of automated records from the California Department of Justice via the California Law Enforcement Telecommunications system (CLETS)
P. Records Clerk: A full or part time non-sworn employee who supports the records management operation of the Department relating to the maintenance, control, release, destruction, and security of hard copy and digital records.
Q. Records Supervisor: As defined by the California Code of Regulations (11CA ADC section 1001) A full-time, non-peace officer employee of a participating California law enforcement agency who performs law enforcement records supervising duties which include records maintenance, control, release, destruction, and security 50% or more of the time within a pay period.
R. RIMS: Records Information Management System
S. Right to Know: Individual, group, or entity entitled and authorized to obtain CORI
T. SDT: Subpoena Duces Tecum - A writ issued by a court at the request of one of the parties to a suit; it requires a witness to bring to court or to a deposition, any relevant documents under the witness' control
U. Subpoena: A writ issued by a court at the request of one of the parties to a suit; it requires a witness to bring to court or to a deposition any relevant documents under the witness's control
V. TRO: Temporary Restraining Order

IV. PROCEDURES

A. Privacy and Security Precautions for Agency Records

1. Separation of juvenile records from adult records

a. Juvenile criminal records shall be separated from adult criminal records.
b. Each juvenile record shall be stored in the locked file drawers in a sealed envelope clearly labeled “JUVENILE,” with a cover sheet that includes the juvenile’s name, report number, and charge. The records unit is a secured facility with proxy card entry access only and an after-hours motion sensor alarm.
c. Juvenile files will be stored in chronological order.
d. Access to hard-copy juvenile files is restricted to authorized personnel.
e. Crime reports containing juvenile information that is entered into the Records Information Management System (RIMS) initially by police officers can only be viewed by those authorized to view juvenile records

(as per WIC 826). Access levels of RIMS are established and controlled by the Special Services Captain.

2. Procedures for the collection, dissemination, and retention of fingerprints, photographs, and other forms of identification pertaining to juveniles.

   a. The records supervisor is responsible and accountable for the maintenance, dissemination, retention, and destruction of juvenile records.
   b. Juvenile records are not to be released under the same state and federal laws that pertain to adult records unless the juvenile committed what is deemed a serious offense.
   c. All juvenile arrest and identification records will be collected, retained, disseminated, and destroyed in strict compliance with existing statutes, decisional law, and policies or orders by the juvenile court.
   d. Juveniles will not be fingerprinted and photographed on a routine basis. If the officer determines that fingerprinting and photographing of a juvenile offender is necessary (e.g., serious offenses and felonies), he/she will obtain prior approval from the shift supervisor.
   e. All juvenile arrest and/or identification records (fingerprints, photographs or physical descriptions) will be affixed to the original report and clearly marked ***JUVENILE*** prior to copying or filing.
   f. The collection, dissemination, and retention of fingerprints, photographs, and any other form of identification pertaining to juveniles shall be strictly limited and controlled.

      1) Access to juvenile records will be limited to those with both "a right- and a need-to-know" in strict compliance with all existing state and federal laws.
      2) The Special Services Captain, his/her designee, and/or designated records staff will control dissemination of any juvenile records.
      3) Juvenile records that are disseminated will be documented in written form within the case file indicating information disseminated, receiving authority, date, and agency representative authorizing release.

   g. A juvenile, upon reaching adult age, may petition to have his/her record sealed. The request should be sent directly to the Department for consideration, to be reviewed by the Chief of Police. If the request is denied, the individual may pursue a court order to seal the record.

   h. Upon receipt of a court order to seal the juvenile's record, the Special Services Captain shall comply with the court order ensuring a copy of such order is forwarded to all agencies that participated in the arrest.

      1) The records supervisor or designee shall immediately provide a copy of the court order to the California Department of Justice (DOJ).
      2) The court order and case materials shall be sealed in an envelope and the date of destruction shall be clearly indicated.
      3) Upon the destruction date the record shall be destroyed.

i. Juvenile Detention Documentation

1) Non-secure and secure detention logs shall be maintained in a folder located in the report writing room.
2) The first day of every month, the records supervisor or designee shall collect the prior months juvenile detention log sheets from the report writing room.
3) If juveniles were detained, the records supervisor or designee takes the log to a Lieutenant of Patrol Operations for approval and signature. In their absence, the log will be taken to the Deputy Chief or Special Services Captain in his/her absence for approval and signature.
4) Pursuant to Section 2071(d)(6) W&I, log entries recorded on the secured and non-secured detention logs shall be tallied monthly and entered on the Monthly report on the Detention of Minors, CYA form 10.402.
5) The records supervisor or designee shall prepare the report and send the form to the California Corrections Standards Authority email address listed at the bottom section of the form. The form is emailed to the California Corrections Standards Authority by the 10th day of the month.
6) A file of the Monthly Report on the Detention of Minors in Jails/Lockups shall be maintained by the records supervisor and is kept in a binder by year in a secured juvenile drawer.

3. Physical security and access control for agency files

a. The records unit is a secured facility with proximity card entry access only and an after-hours motion sensor alarm. If the motion sensor alarm is activated, dispatch is to immediately notify the on-duty shift supervisor, who will investigate to ensure that the security of the records unit has not been compromised.

b. Original files shall not be removed from the records files without the approval of the records supervisor, Special Services Captain, Deputy Chief, or the Chief of Police.

1) If an officer requires a report/record, he/she may request it directly from the records supervisor. Should a report/record be required by an officer during non-business hours, the shift supervisor shall call the Special Services Captain or his/her designee for approval to access the records unit to obtain the requested record. Records maintained within the Investigations Unit are not accessible to officers after hours.
2) No copies of reports shall be disseminated outside of this department without approval of the Chief of Police or a member of the Command Staff.

4. Procedures and criteria for the release of department records

a. Requests for department records by the public are to be made during

regular business hours.

b. Release of adult criminal records shall be in accordance with department policy and state and federal laws.

c. The privacy and security of criminal history record information shall be in accordance with U.S. Department of Justice Regulations, 2B Code of Federal Regulations Part 20, and "Criminal Justice Information Systems" regarding access, review, dissemination, accuracy, integrity, security, and audit requirements.

d. As defined in the California Public Records Act, "Public records include any writing containing information relating to the conduct of the public's business prepared, owned, used, or retained by any state or local agency regardless of physical form or characteristics." Based upon this definition, reports of crimes and incidents generated in the daily course of business of a law enforcement agency are public records and subject to release under the Act, with certain exemptions.

e. This agency maintains the security information of its records according to the California Public Records Act, Government Code 6250-6265, requiring that specific information be released unless the release would endanger the safety of a person or endanger the successful completion of an investigation.

f. Records personnel shall refer to the Commission on Peace Officer Standards and Training (POST) Law Enforcement Records Management Guide and/or consult the POST Management Counseling Services Bureau for issues related to records management that may require additional research.

g. Request for Release of Information

1) Police Reports and Records requested by other departments within the institution, outside law enforcement agencies, insurance companies, public (including CSUN parents and students), and agencies/companies conducting background investigations on current or former students/staff/faculty, shall conform to the following procedures.

a. The requesting party must complete a CSUN Department of Police Services Release of Information Request form, copies of which are located in the forms file shelf in the records unit; in the master forms book in records; in the police shift supervisor's office, at the front reception counter and electronically on the police server under Data/Forms. For external law enforcement, public safety, and judicial partners, the DPS records release form may be completed by a member of the command staff, detectives, or records units

b. Per Government Code Section 6254, a fee is assessed ($10.00 for private parties and insurance company

requests). No fee is charged to outside law enforcement agencies.

c. The records supervisor or designee provides an available detective with the redacted reports that are being requested for copies or that require forwarding.

d. The detective will cross out those areas they deem should be redacted for legal reasons (as per CORI/HIPPA/FERPA) or information that may hinder the case investigation.

e. At no time shall an arrest report be copied and/or provided to someone requesting a copy of said report until such time as it has been criminally filed with the District or City Attorney's office.

f. Once the record is returned to the records supervisor or designee from the detective, theywill forward the report to the Special Services Captain (or a Patrol Operations Commander in his/her absence) who will review the redacted report and decide if it is ready for release or if further/less redaction is required.

g. The reviewing Commander will decide which reports need to be forwarded to the Chief for final approval.

h. The records supervisor will keep track of all reports that are in the process of review, etc. and of who in Command Staff has authorized release of the report. The completed release forms are scanned and attached to the report in RIMS and hard copies are held in the file.

i. ***No copies of reports (hardcopy or electronic) shall be disseminated outside of this department without approval of the Chief of Police or a member of the Command Staff.***

j. Fees for hardcopies of reports are paid at the Parking & Transportation Services lobby window. k. For hardcopies, the records supervisor or designee stamps the approved report for release, makes a copy of the requesting person's identification, verifies payment of the report copy, and makes a copy of the payment receipt to be scanned and attached in RIMS. A hard copy will also be placed in the file.

l. The Information Request Form is attached to the report.

m. Various reports forwarded to departments within the institution (e.g., Student Health Center-medical related reports; Counseling Services – mental illness; Equity and Diversity – Title IX matters and harassment; Residential Life – student living environment issues; Student Judicial Affairs – student misconduct; Human Resources – employee misconduct and other HR related matters; University Auditor – cases involving state property/monies; Environmental Health and Safety – cases involving risk and liability management issues for the university) have been granted automatic approval for forwarding by the Chief of Police (i.e., no requirement for completion of an Information Request Form)

pending conclusion of the above process. Redacted copies provided to CSUN departments will be done so via “myCSUNbox” whereby reports provided are posted in a viewable pdf format only. Reports posted in “myCSUNbox” are viewable for 6 months, at which time they’ll be deleted. Printing a hardcopy is prohibited by the Department and removed as an option from the software program.

2) Juvenile Records: Welfare and Institutions Code 827 gives the juvenile court control over the release of all juvenile information to be disclosed to third parties by any law enforcement official.

3) All student records at California State University, Northridge are maintained in accordance with the provision of the Family Educational Rights and Privacy Act (FERPA). The university defines as "directory information" and normally makes public, the following information from a student's record: student name, e-mail, major field of study, dates of attendance, class level, enrollment status (e.g., undergraduate or graduate, full-time or part-time), degrees earned, honors and awards received. The university does not release to the general public any other information, including courses, grades, address, or telephone number unless a student submits a written request.

Two special provisions are available to students:

a. A request may be made that any or all of the above listed "directory information" not be made public under the provisions of FERPA.
b. A request may be made that non-directory information, including address, be released to agencies of the state of California when requested for employment recruitment purposes under the provisions of Assembly Bill 771 (Chacon).

To affect either of these provisions, a written request must be submitted by the student to the Registrar's Office counter at the Student Services Center.

B. Record Retention Schedule

1. The department’s record retention schedule is consistent with legal requirements as outlined in the POST Records Management Guide. The record retention schedule, which applies to all departmental records regardless of unit (i.e. law enforcement records, personnel records, parking records, etc.) is accessible on the DPS “Police$” server “P:\Data\Forms\Records’ Forms” and is entitled “*DPS Records Retention Schedule.*”

2. The record retention schedule includes:

    a. Records to be retained;
    b. Retention period reference suggested by government agencies such as the DOJ, CHP, courts, Government Code and Penal Code; and
    c. Campus-suggested retention periods.

3. Those personnel responsible for records contained in the Records Retention Schedule are required to purge records annually per the schedule within 60 days of the end of each calendar year. When this task is complete, this fact shall be conveyed in writing to the Special Services Captain.

C. Collection and Submittal of Crime Data

1. The Department participates in the Uniform Crime Reporting (UCR) process by reporting crime statistics to the California Department of Justice on a monthly basis. This information is subsequently merged into national reporting systems such as the Federal Bureau of Investigation database.

2. Statistics are captured through the RIMS database and statistical reports are generated at the end of each month for submission to DOJ in accordance with UCR standards. As a backup, the records supervisor maintains a written copy of crime statistics.

3. The following reports are compiled and printed from the RIMS Reports program:

    a. UCR Return 'A'
    b. Property report
    c. Property Stolen and Recovered report
    d. Arson report
    e. Domestic Violence report
    f. Violent Crimes Committed Against Seniors report
    g. Anti-Reproductive Rights Crime report
    h. Monthly Arrest and Citation report
    i. Hate Crimes report
    j. Officers Assaulted/Killed (LEOKA)

4. All reports, except the Hate Crimes report, are entered into the E-CARS Plus program which imports the data directly into the Department of Justice database.

5. The Hate Crimes report is entered directly into the Hate Crime Report System which imports the data directly into the Department of Justice database.

6. The department participates in the Department of Education's Higher Education Opportunity Act and reports statistics on an annual basis in the Annual Crime Awareness and Campus Security Act report. The statistics are complied as defined by the Jeanne Clery Disclosure of Campus Security Policy and Campus Crime Statistics Act (Clery Law).

Reference Policy/Procedure Number 03-O.A.-002 for details and procedures.

7. The department participates in the California Annual Campus Safety Plan reporting which must be posted/released by January 1st of each year.

   a. The records supervisor or designee assists the Campus Clery Director in populating the document with the statistics captured by the RIMS database.
   b. Upon approval of the report by the Special Services Captain and Chief of Police, confirmation of the approval is forwarded to the Campus Clery Director who will forward the report to the Chancellor's Office.
   c. Hate Crime and Noncriminal acts of hate violence statistics from all CSU campuses are compiled by the Chancellor's Office to be included in the report prior to distribution.

8. The Department participates in the Bi-Annual Drug-Free Campus Act which mandates, per federal guidelines, the reporting of alcohol-related crime statistics. This information is gathered by the records supervisor and Special Services Captain, reviewed and approved by the Chief of Police, and then forwarded to the CSUN Klotz Student Health Center for dissemination. Information regarding alcohol and drug educational programs is also provided by the department to the local community through training and presentations by the Crime Prevention function as coordinated by the Captain.

D. Records Validation Procedures

1. The records supervisor or designee is responsible for validating and certifying the NCIC files.

2. Upon receipt of the validation package, the records coordinator will immediately remove the validation acknowledgement letter, sign, date and fax or email it to the Department of Justice (DOJ).

3. The records supervisor will review the entries on the enclosed list for completeness, accuracy and current status.

4. In accordance with NCIC policy, validation of vehicle, boat, wanted person, missing person, supervised release and restraining order requires CSUN to have recent consultation with an appropriate complainant, victim, prosecutor, court, motor vehicle registry file or another appropriate source or individual.

5. In the event attempts to contact the victim, complainant, etc., are unsuccessful, the entering authority must make a determination based upon the best information and knowledge available whether or not to retain the original entry in the file.

6. The records supervsior or designee will make any necessary changes in the record or status through the CLETS terminal.

7. The records supervsior or designee will certify that all records in the automated systems program validation list (printouts) have been reviewed for accuracy and completeness.

8. Upon completion of the package, the records supervisor or designee will immediately remove the validation certification letter, sign, date, and fax or email to DOJ.

9. The NCIC Advisory Policy Board has established sanctions to enforce compliance with the validation program. If this agency's certification letter is not received by DOJ by the due date, the invalidated records will be purged from the NCIC files.

E. Central Records Information

1. The Records Information Management System (RIMS) is accessible to police operations personnel twenty-four hours a day, on a read-only basis, with the exception of the report writing module.

2. Dispatchers have access to RIMS twenty-four hours a day, with full access, not including administrator access.

3. The Deputy Chief, Captain, two patrol operations Lieutenants, records supervisor, and IT systems analyst have both full access and administrator access to RIMS. The Captain of Special Services Division however is the primary administrator of the department's RIMS central records computer system.

4. To account for the status of reports, the records supervisor or designee shall audit the RIMS system on a daily basis to ensure that the correct case numbers are being assigned and accounted for.

5. Sergeants shall:

   a. Ensure that follow-up reports are prepared on a specified schedule not to exceed the officer's work week, or a designated date assigned by a patrol operations Commander, investigations supervisor, Captain, or Deputy Chief in their absence;
   b. Ensure that report corrections are completed by their designated date.

6. The records supervisor or designee, upon receipt of all reports, shall review the reports for accuracy and ensure that crime report numbers are correctly cross-referenced.

F. Record-Keeping Responsibilities

1. The original of all case reports will be maintained in numerical order in the master case report files retained in the Records Information Management System (RIMS).

2. Under no circumstances will an original report be removed from the records unit; only copies will be routed to appropriate personnel for follow-up as required.

3. Arrest, crime, traffic, complaint, and incident reports are kept in the records unit, a secured facility with proxy card entry access only and an after-hours motion sensor alarm.

4. Personnel files, background investigation files, and personnel complaint files on current employees are secured in the Chief's administrative area and are under the direct custodial care of the special assistant to the Chief.

5. The investigators retain copies of all cases actively under investigation. The investigations unit is a secured facility with proximity card entry access only.

6. It is the responsibility of all designated custodians to ensure that access to confidential files is handled on a need-to-know basis. The Chief of Police will resolve conflicts relating to the legitimate need to access confidential files.

7. Prior to submission to the records unit for further data entry and storage, each report will be reviewed by the shift supervisor for completeness. When appropriate, the shift supervisor will approve the report via RIMS and it will automatically route for records review.

8. The investigations supervisor will screen the case reports, determine what type of follow-up is required, and assign the case to the appropriate individual as described in the Case Screening and Case Management Systems Policy (Policy/Procedure Number 05-C.I.-001).

9. As follow-up reports, supplements and status reports are received by the records supervisor or designee, the case number is cross-checked, verified and filed with the original report.

10. The Special Services Captain and Investigations Unit Supervisor are the primary persons responsible for tracking the status of all reports recorded within the RIMS central records system that fall within their area(s) of responsibility. The Records supervisor or designee will monitor the status of all reports being entered and managed within the RIMS central records system, consulting with the Investigations Unit Supervisor when discrepancies are found.

G. Subpoena Processing Procedures

1. When a subpoena is received for a police officer by mail, the records supervisor or designee will:

   a. Notify the Special Services Captain and make the entry for the officer in RIMS.
   b. Issue a paper subpoena to the officer with a return envelope for signature and returning to the court.
   c. Bond payment of $275.00 must accompany civil subpoenas.

2. When a subpoena is received for a police officer by telephone request and a faxed copy of the subpoena, the records administrator will:

   a. Notify the Special Services Captain and make the entry for the officer in RIMS.

b. Notify the shift supervisor to give the officer telephonic service.
c. Notify the court witness coordinator of results of service.

3. When a subpoena is received by mail from another agency or a civilian witness, the records supervisor or designee will:

a. Notify the Special Services Captain and make the entry for the officer in RIMS
b. Forward to the investigations unit supervisor for personal service.
c. Once result of service is received, note on the log and return the subpoena to the court witness coordinator.

4. A CSUN police officer shall appear as ordered by any lawful court summons/subpoena. The records supervisor or designee will work with the shift supervisor to ensure that the officer is notified in a timely manner. Subpoenas received with less than 48 hours notice will be rejected, unless the subpoena date is a regularly scheduled work day for the officer.

For emergency situations or scheduling conflicts (e.g., approved vacations, training, etc.), the records supervisor or designee will be responsible for coordinating such with the court. Officers are responsible for ensuring the records supervisor or designee is notified of said emergencies or conflicts within 72 hours of the subpoena appearance date/time, or as soon as possible.

5. As the custodian of records, the records supervisor may accept; refuse, based on errors, or consult with command staff to respond to a subpoena dues tecum (SDT). The records supervisor shall declare the response is true and complete under penalty of perjury.

H. Restraining Order Processing Procedures

1. All restraining orders presented to the CSUN Police Department for intake into our restraining order system shall be provided to the records supervisor or designee.

2. The records supervisor or designee will date stamp the form upon receipt and then enter the information into RIMS.

3. All restraining orders shall be issued a report number upon intake if one is not already present.

4. If the restraining order is a result of a CSUN case or the protected party is a university resident and/or is the university itself, then the records supervisor or designee,or the on duty dispatcher in their absence shall enter the information into the CLETS/JDIC system.

5. If the order is provided as a “for-your-information” (i.e. non-resident student who filed it with the agency where he resides but feels he could be contacted by the restrained party on university grounds), the records supervisor for designee will:

a. Make a copy of the restraining order;
b. Issue the copy a report number;

c. Place a date stamp;
d. Enter the information into RIMS.

6. The records supervisor or designee will oversee the accuracy, maintenance and retention of all restraining orders placed within the original records file and "active" file maintained within communications unit and the records unit, in addition to that information that is entered into CLETS/JDIC and RIMS.

7. The records supervisor or designee is responsible for the verification of the existence of a restraining order and notification via CJIS/CLETS, as necessary, of the issuance of a restraining order by the court.

8. To verify that the restraining order exists, the records supervisor or designee will:

a. Check the department's records and restraining order files for a copy provided by the protected person and inquire into DVROS;
b. Check the type of restraining order;
c. Check the terms of the order;
d. Issue a crime report number if not found in department records.

9. When the university has jurisdiction over the residence of the plaintiff (protected person), the records supervisor or designee will immediately notify DOJ via CJIS/CLETS, of the following information:

a. In accordance with NCIC policy, the restrained person's (respondent's) name, race, date of birth and, if available, other personal descriptive information;
b. The names of the protected person(s);
c. The issuance and the expiration date of the order;
d. The terms and conditions of the order, including stay-away, no contact and residency exclusion orders;
e. Whether the order was served upon the respondent or whether the respondent was present in court;
f. Provide the crime report number when appropriate.

I. Traffic Citation Processing Procedures

1. The officer issuing the citation enters the cite information into RIMS.

2. Completed traffic citations will be placed in the shift supervisor's mail box prior to the end of shift for review.

3. The shift supervisor shall review the citation for accuracy and either approve the citation by placing his/her initials in the lower right corner of the citation or return the citation to the issuing officer for corrections(s).

4. The citation is then routed to records, at which time the records supervisor or designee will review the citation information entered into RIMS.

5. The records supervisor or designee completes a citation transmittal form and it is sent with all processed citations to the appropriate filing entity within the traffic court system.

6. In the event a citation is returned from the court for correction(s), the records supervisor or designee will return the citation to the officer's mailbox with the court approved correction slip.

7. Upon completion of the correction, the officers will return the citation and completed correction slip to the records coordinator's mailbox for processing.

8. The records supervisor will complete affidavit of mailing on the correction form and complete a correction notification letter to the cited party. After making hard copies and scanning the information into the citation and/or case record in RIMS, the original correction slip will be stapled to the citation and submitted to the court. A copy of the correction and the original correction notification letter will be sent to the cited party.

9. A DMV form number DL310 advising a driver that his/her driver license is suspended or revoked will be:

    a. Attached to the confiscated driver license (if one is obtained) via a paperclip;
    b. Placed in the shift supervisor's mail box for approval;
    c. Upon approval, the shift supervisor will initial the lower right corner of the form;
    d. The DL310 is then routed to the records supervisor or designee who will finalize any processing required and mail the items to the appropriate DMV administrator.

J. Annual Audit of Central Records

1. On an annual basis, the Special Services Captain shall conduct an audit of the RIMS and JDIC/CLETS system for verification of all passwords and access violations.

2. The audit shall include a review of user list information and access levels.

3. A written report shall be provided to the Chief of Police in reference to the audit findings.

K. Introduction of Outside Computer Software

1. All computers maintained by the Department of Police Services shall have anti-virus software installed, which scans all disks or devices each time they are loaded on a computer.

    a. This software is updated by the systems analyst regularly;
    b. No user will have access to download or install software without the approval of the systems analyst;
    c. The systems analyst will maintain proper licensing of all software owned by the department.

2. Absolutely no software program (including shareware and screensavers) shall be used, installed, or otherwise loaded onto any department computer, the network,

or the hard drive of any department computer without authorization of the Chief of Police.

3. No software will be authorized or installed unless properly licensed for use at the California State University, Northridge Department of Police Services.

4. The systems analyst shall maintain a record of software installed on the network and on each computer. This information shall include the program name, software manufacturer, and the software license or registration number.

L. Network Server and Central Records Systems

1. The RIMS database file server is housed and secured via proximity card access, intrusion alarm, and CCTV security systems at Information Technology (IT) in Sequoia Hall; and is backed up on a daily basis to an external hard disk attached directly to the file/database server.

2. The network file/database server is housed at IT all and the network files are backed up nightly to an external tape attached directly to the file/database server.

3. Vital Records – Tape backups of RIMS files and network files are stored in a secured location at IT.

4. On a weekly basis, a tape of the RIMS database is sent by IT via courier to an off-site secure storage location.

5. Recovery of system data can be obtained through a request made by the Chief of Police or her/his designee to the University IT department.

6. The system administrator for the department's central records system (i.e., RIMS) is the Special Services Captain.

7. User access-only passwords to RIMS are issued by the Special Services Captain to department employees deemed by the Chief of Police as having a need to access information contained therein. System administrator passwords to the department network server and RIMS central records system are issued to department IT administrators by the Special Services Captain (RIMS) or the University IT (network server) as approved by the Chief of Police. Password access is rescinded and removed by the Special Services Captain upon immediate termination of employment with the department or a change in the need for access.

M. Criminal History Records

1. Computerized criminal history records can be accessed via CLETS and CCHRS web application.

2. Upon the arrest of a suspect, officers may request that a criminal history transcript or a Report of Arrests and Prosecutions (RAP) sheet be included with their report.

3. Police officers, dispatchers, investigators, the records supervisor, and records clerk have access to the CLETS terminal located in the dispatch center and in the detective division for purposes of running a RAP sheet.

4. An entry in the Criminal History Log Book will be made by the dispatcher indicating the date, name, and reason for the inquiry for audit purposes. Detectives and dispatchers are to ensure that they routinely enter correct information in the appropriate JDIC/CLETS boxes justifying their need-to-know criminal history information.

5. Printouts of criminal history information are to remain secured with the requesting police officer or investigator and subsequently attached to the police report.

6. Criminal history printouts become part of the case jacket for the investigation unit and shall be secured in investigations for active cases and in records for inactive cases.

7. Criminal history printouts are not released to the public.