E-JUSTICE

STANDARD NO(S):   NYSLEAP

DATE: August 11, 2018

REFER TO: Michael Schell

I.   OBJECTVE:

To establish policy and procedures for the members of the Seneca County Sheriff's Office when using the New York State Division of Criminal Justice Services E-Justice system.

II.   POLICY:

It is the policy of the Seneca County Sheriff's Office to utilize the e-Justice system or conduct Criminal history inquires, as needed in the performance of duties, in accordance with all applicable State and Federal Laws and in accordance with the Use and Dissemination Agreement with the New York State Division of Criminal Justice Services (DCJS).

The system is for official use, for law enforcement purposes only. Access for private, personal or social purpose is strictly prohibited. Information is to be accessed only for the reasons stated herein and in compliance with all applicable Departmental, DCJS or National Crime Information Center (NCIC) regulations.

III.   PROCEDURE:

A. E-Justice Terminal Agency Coordinator (TAC)- will oversee who has access to e-justice and will be the liaison between the department and DCJS. The TAC will update users or remove users and will request what e-justice programs the user can access. Other TAC functions are:

1. Ensure system security and proper system functioning.

2. Administer and maintain certification test records.

3. Disseminate user names and passwords to members.

4. Conduct periodic audits to ensure compliance with Departmental, DCJS and NCIC regulations and policies governing use of the system.

B. Access:

1. Any member of the office who requires access to law enforcement information may access some or all e-justice TAC modules, with the permission of supervisor and the TAC.

2. All users of the system will be required to take and pass the Limited Access NCIC Terminal Operator certification test within six months of receiving user name and password. Note: users who have full certification do not have to complete this test. Users will have to retest at intervals determined by DCJS.

3. The e-justice TAC will maintain a record of certification for each user. This includes, certification status, expire date and data related to past compliance with applicable regulations. All will be kept as a permanent record for the duration of the user's employment. It is the TAC's responsibility to notify DCJS of a user who is no longer employed by the agency.

C. Security:

1. Criminal history records that are received as a result of an arrest or an investigation made by members of the Sheriff's office shall be placed in the secured records file, CID investigation file, sent to arraignment court or placed in an approved shred container.

2. All records for criminal history will be tracked and maintained by the TAC.

3. Any workstation on which the e-justice system has been activated must be kept secure. Once the system has been accessed, the user must maintain a physical presence at the workstation at all times. If the user must leave the workstation, or has completed the session, the e-justice application must be closed.

4. Members must report to their immediate supervisor or to the TAC any attempts or suspected attempts at unauthorized access into the e-justice system.

D. Usage- Criminal Justice Repository:

1. Access into the Criminal Justice Repository is only for the purpose of administering a criminal justice function. Criminal Justice function is defined as the prevention, detection and investigation of the commission of an offense; the apprehension of a person for the alleged commission of an offense; the detention, release on recognizance or bail of a person charged with an offense prior to the disposition of the charge; the

prosecution and defense of a person charged with an offense; the detention, release on recognizance or bail of a person convicted of an offense prior to sentencing; the sentencing of offenders, probation, incarceration, parole and proceeding in a court subsequent to a judgment of conviction relation hereto.

2. No inquiry into the criminal justice repository is possible without the requestor's name, request reason code and full case number being listed. In addition, a copy of the criminal justice data will be maintained in the case file for any cases that have a case file.

3. Personnel will disclose information obtained from these systems outside the Department only as authorized by law, and only for a valid law enforcement purpose or other official Department business.

4. All information obtained via the criminal justice repository is to be used for the purpose to which the inquiry was intended. All inquiries made through the criminal justice repository are tracked via an automatic audit trail. The requestor's name, request reason, case year and case number are automatically saved for each individual request. The audit information is available to the e-justice TAC and DCJS to ensure compliance with regulations.