ROSENBERG POLICE DEPARTMENT

General Order 5.03 Criminal Justice Information Security

Effective Date: 12-28-2020

Approved: 

Chief of Police

Reference: CJISD-ITS-DOC-08140-5.2

I. POLICY

Law enforcement needs timely and secure access to services that provide data wherever and whenever for stopping and reducing crime.

It is the policy of this department to ensure proper handling and use of Criminal Justice Information (CJI); managing electronic computing systems by establishing authorized uses and users; establishing protocols for storage, security, and retention of CJI; and prohibiting inappropriate uses of such equipment and resident information.

II. PURPOSE

To define and provide clear direction to the use and prohibited uses of department electronic computing and recording equipment, to provide for data security and retention periods, and to establish protocols for proper handling of CJI.

III. DEFINITIONS

Access to Criminal Justice Information — The physical or logical (electronic) ability, right or privilege to view, modify or make use of Criminal Justice Information.

Agency Coordinator (AC) — A staff member of the Contracting Government Agency who manages the agreement between the Contractor and the Agency.

Authorized User/Personnel — An individual, or group of individuals, who have been appropriately vetted through a national fingerprint-based record check and have been granted access to CJI data.

Authorized Recipient — (1) A criminal justice agency or federal agency authorized to receive CHRI pursuant to federal statute or executive order; (2) A nongovernmental entity authorized by federal statute or executive order to receive CHRI for noncriminal justice purposes; or (3) A government agency authorized by federal statute or executive order, or state statute which has been approved by the United States Attorney General to receive CHRI for noncriminal justice purposes.

Case / Incident History — All relevant information gathered about an individual, organization, incident, or combination thereof, arranged so as to serve as an organized record to provide analytic value for a criminal justice organization. In regard to CJI, it is the information about the history of criminal incidents.

Contractor — A private business, agency or individual which has entered into an agreement for the administration of criminal justice or noncriminal justice functions with a Criminal Justice Agency or a Noncriminal Justice Agency. Also, a private business approved by the FBI CJIS Division to contract with Noncriminal Justice Agencies to perform noncriminal justice functions associated with civil fingerprint submission for hiring purposes.

Contracting Government Agency (CGA) — The government agency, whether a Criminal Justice Agency or a Noncriminal Justice Agency, which enters into an agreement with a private contractor.

Criminal History Record Information (CHRI) — A subset of CJI. Any notations or other written or electronic evidence of an arrest, detention, complaint, indictment, information or other formal criminal charge relating to an identifiable person that includes identifying information regarding the individual as well as the disposition of any charges.

Criminal Justice Agency (CJA) — The courts, a governmental agency, or any subunit of a governmental agency which performs the administration of criminal justice pursuant to a statute or executive order and which allocates a substantial part of its annual budget to the administration of criminal justice.

Criminal Justice Information (CJI) — Criminal Justice Information is the abstract term used to refer to all of the FBI CJIS provided data necessary for law enforcement agencies to perform their mission and enforce the laws, including but not limited to: biometric, identity history, person, organization, property (when accompanied by any personally identifiable information), and case/incident history data. In addition, CJI refers to the FBI CJIS-provided data necessary for civil agencies to perform their mission; including, but not limited to data used to make hiring decisions. The following type of data are exempt from the protection levels required for CJI: transaction control type numbers (e.g. ORI, NIC, FNU, etc.) when not accompanied by information that reveals CJI or PII.

Criminal Justice Information Services Division (FBI CJIS or CJIS) — The FBI division responsible for the collection, warehousing, and timely dissemination of relevant CJI to the FBI and to qualified law enforcement, criminal justice, civilian, academic, employment, and licensing agencies.

Information System — A system of people, data, and processes, whether manual or automated, established for the purpose of managing information.

Interstate Identification Index (III) — The CJIS service that manages automated submission and requests for CHRI that is warehoused subsequent to the submission of fingerprint information. Subsequent requests are directed to the originating State as needed.

Local Agency Security Officer (LASO) — The primary Information Security contact between a local law enforcement agency and the CSA under which this agency interfaces with the FBI

CJIS Division. The LASO actively represents their agency in all matters pertaining to Information Security, disseminates Information Security alerts and other material to their constituents, maintains Information Security documentation (including system configuration data), assists with Information Security audits of hardware and procedures, and keeps the CSA informed as to any Information Security needs and problems.

National Crime Information Center (NCIC) — An information system which stores CJI which can be queried by appropriate Federal, state, and local law enforcement and other criminal justice agencies.

Noncriminal Justice Agency (NCJA) — A governmental agency, or any subunit thereof, that provides services primarily for purposes other than the administration of criminal justice. Examples of services include, but not limited to, employment suitability, licensing determinations, immigration and naturalization matters, and national security clearances.

NCJA (Government) — A Federal, state, local, or tribal governmental agency or any subunit thereof whose charter does not include the responsibility to administer criminal justice, but may have a need to process CJI. An example would be the central IT organization within a state government that administers equipment on behalf of a state law-enforcement agency.

Terminal Agency Coordinator (TAC) — Serves as the point-of-contact at the local agency for matters relating to CJIS information access. A TAC administers CJIS systems programs within the local agency and oversees the agency's compliance with CJIS systems policies.

IV. RESPONSIBILITIES

It is the responsibility of this agency to ensure the protection of CJI between the FBI CJIS Division and its user community. The entities listed are tasked with the strategic functions and roles concerning governance and operation of information systems used to access and disseminate CJI.

Terminal Agency Coordinator (TAC)

The TAC serves as the point-of-contact at the local agency for matters relating to CJIS information access. The TAC administers CJIS systems programs within the local agency and oversees the agency's compliance with CJIS systems policies.

Criminal Justice Agency (CJA)

A CJA is defined as a court, a governmental agency, or any subunit of a governmental agency which performs the administration of criminal justice pursuant to a statute or executive order and which allocates a substantial part of its annual budget to the administration of criminal justice. State and federal Inspectors General Offices are included.

Noncriminal Justice Agency (NCJA)

A NCJA is defined (for the purposes of access to CJI) as an entity or any subunit thereof that provides services primarily for purposes other than the administration of criminal justice.

Contracting Government Agency (CGA)

A CGA is a government agency, whether a CJA or a NCJA, that enters into an agreement with a private contractor subject to the CJIS Security Addendum. The CGA entering into an agreement

with a contractor shall appoint an agency coordinator.

Agency Coordinator (AC)
An AC is a staff member of the CGA who manages the agreement between the Contractor and agency. The AC shall be responsible for the supervision and integrity of the system, training and continuing education of employees and operators, scheduling of initial training and testing, and certification testing and all required reports by NCIC. The AC shall:

1. Understand the communications, records capabilities, and needs of the Contractor which is accessing federal and state records through or because of its relationship with the CGA.
2. Participate in related meetings and provide input and comments for system improvement.
3. Receive information from the CGA (e.g., system updates) and disseminate it to appropriate Contractor employees.
4. Maintain and update manuals applicable to the effectuation of the agreement, and provide them to the Contractor.
5. Maintain up-to-date records of Contractor's employees who access the system, including name, date of birth, social security number, date fingerprint card(s) submitted, date security clearance issued, and date initially trained, tested, certified or recertified (if applicable).
6. Train or ensure the training of Contractor personnel. If Contractor personnel access NCIC, schedule the operators for testing or a certification exam with the CSA staff, or AC staff with permission from the CSA staff. Schedule new operators for the certification exam within six (6) months of assignment. Schedule certified operators for biennial re-certification testing within thirty (30) days prior to the expiration of certification. Schedule operators for other mandated class.
7. The AC will not permit an untrained/untested or non-certified Contractor employee to access CJI or systems supporting CJI where access to CJI can be gained.
8. Where appropriate, ensure compliance by the Contractor with NCIC validation requirements.
9. Provide completed applicant fingerprint cards on each Contractor employee who accesses the system to the CJA (or, where appropriate, CSA) for criminal background investigation prior to such employee accessing the system.
10. Any other responsibility for the AC promulgated by the FBI.

Local Agency Security Officer (LASO)
Each LASO shall:

1. Identify who is using the CSA approved hardware, software, and firmware and ensure no unauthorized individuals or processes have access to the same.
2. Identify and document how the equipment is connected to the state system.
3. Ensure that personnel security screening procedures are being followed as stated in this Policy.
4. Ensure the approved and appropriate security measures are in place and working as expected.
5. Support policy compliance and ensure the CSA ISO is promptly informed of security incidents.

V. CRIMINAL JUSTICE INFORMATION AND PERSONALLY IDENTIFIABLE INFORMATION

Criminal Justice Information (CJI)
Criminal Justice Information is the term used to refer to all of the FBI CJIS provided data necessary for law enforcement and civil agencies to perform their missions including, but not limited to biometric, identity history, biographic, property, and case/incident history data. The following categories of CJI describe the various data sets housed by the FBI CJIS architecture:

1. Biometric Data—data derived from one or more intrinsic physical or behavioral traits of humans typically for the purpose of uniquely identifying individuals from within a population. Used to identify individuals, to include: fingerprints, palm prints, iris scans, and facial recognition data.
2. Identity History Data—textual data that corresponds with an individual's biometric data, providing a history of criminal and/or civil events for the identified individual.
3. Biographic Data—information about individuals associated with a unique case, and not necessarily connected to identity data. Biographic data does not provide a history of an individual, only information related to a unique case.
4. Property Data—information about vehicles and property associated with crime when accompanied by any personally identifiable information (PII).
5. Case/Incident History—information about the history of criminal incidents.

The following type of data are exempt from the protection levels required for CJI: transaction control type numbers (e.g., ORI, NIC, FNU, etc.) when not accompanied by information that reveals CJI or PII.

The intent of the CJIS Security Policy is to ensure the protection of the aforementioned CJI until the information is: released to the public via authorized dissemination (e.g. within a court system; presented in crime reports data; released in the interest of public safety); purged or destroyed in accordance with applicable record retention rules.

Criminal History Record Information (CHRI)
Criminal History Record Information (CHRI), sometimes informally referred to as "restricted data", is a subset of CJI. Due to its comparatively sensitive nature, additional controls are required for the access, use and dissemination of CHRI. In addition to the dissemination restrictions outlined below, Title 28, Part 20, Code of Federal Regulations (CFR), defines CHRI and provides the regulatory guidance for dissemination of CHRI. While the CJIS Security Policy attempts to be architecturally independent, the III and the NCIC are specifically identified in Title 28, Part 20, CFR, and the NCIC Operating Manual, as associated with CHRI.

- **Access, Use and Dissemination of Criminal History Record Information (CHRI), NCIC Restricted Files Information, and NCIC Non-Restricted Files Information**
  This section describes the requirements for the access, use and dissemination of CHRI, NCIC restricted files information, and NCIC non-restricted files information.

- **Proper Access, Use, and Dissemination of CHRI**
  Information obtained from the III is considered CHRI. Rules governing the access, use, and dissemination of CHRI are found in Title 28, Part 20, CFR. The III shall be accessed only for an authorized purpose. Further, CHRI shall only be used for an authorized

purpose consistent with the purpose for which III was accessed. Dissemination to another agency is authorized if (a) the other agency is an Authorized Recipient of such information and is being serviced by the accessing agency, or (b) the other agency is performing personnel and appointment functions for criminal justice employment applicants.

- **Proper Access, Use, and Dissemination of NCIC Restricted Files Information**
  The NCIC hosts restricted files and non-restricted files. NCIC restricted files are distinguished from NCIC non-restricted files by the policies governing their access and use. Proper access to, use, and dissemination of data from restricted files shall be consistent with the access, use, and dissemination policies concerning the III described in Title 28, Part 20, CFR, and the NCIC Operating Manual. The restricted files, which shall be protected as CHRI, are as follows:

  1. Gang Files.
  2. Known or Appropriately Suspected Terrorist Files.
  3. Supervised Release Files.
  4. Immigration Violator File (formerly the Deported Felon Files).
  5. National Sex Offender Registry Files.
  6. Historical Protection Order Files of the NCIC.
  7. Identity Theft Files.
  8. Protective Interest Files.
  9. Person With Information (PWI) data in the Missing Person Files.

  The remaining NCIC files are considered non-restricted files.

- **Proper Access, Use, and Dissemination of NCIC Non-Restricted Files Information**

  - **For Official Purposes**
    NCIC non-restricted files are those not listed as restricted files in the previous section. NCIC non-restricted files information may be accessed and used for any authorized purpose consistent with the inquiring agency's responsibility. Information obtained may be disseminated to (a) other government agencies or (b) private entities authorized by law to receive such information for any purpose consistent with their responsibilities.

  - **For Other Authorized Purposes**
    NCIC non-restricted files may be accessed for other purposes consistent with the resources of the inquiring agency; however, requests for bulk data are discouraged. Information derived from NCIC non-restricted files for other than law enforcement purposes can be used by authorized criminal justice personnel only to confirm the status of a person or property (i.e., wanted or stolen). An inquiring agency is authorized to charge a nominal administrative fee for such service. Non-restricted files information shall not be disseminated commercially.

    A response to NCIC person inquiry may include NCIC restricted files information as well as NCIC non-restricted files information. Employees shall not disseminate restricted files information for purposes other than law enforcement.

  - **Storage**

When CHRI is stored, agencies shall establish appropriate administrative, technical and physical safeguards to ensure the security and confidentiality of the information. These records shall be stored for extended periods only when they are key elements for the integrity and/or utility of case files and/or criminal record files.

- **Justification and Penalties**

    - **Justification**
      In addition to the use of purpose codes and logging information, all users shall provide a reason for all III inquiries whenever requested by NCIC System Managers, CSAs, local agency administrators, or their representatives.
        - Justification shall be made in the following manner:
            - Use of appropriate Purpose Code (PUR) when performing inquiries which can interface with the NCIC III.
            - Use of Reason for Inquiry (RFI) fields when performing inquiries which interface with the NCIC III.
    - **Penalties**
      Improper access, use or dissemination of CHRI and NCIC Non-Restricted Files information is serious and may result in administrative sanctions including, but not limited to, termination of services and state and federal criminal penalties.

- **Personally Identifiable Information (PII)**
  For the purposes of this document, PII is information which can be used to distinguish or trace an individual's identity, such as name, social security number, or biometric records, alone or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, or mother's maiden name. Any FBI CJIS provided data maintained by an agency, including but not limited to, education, financial transactions, medical history, and criminal or employment history may include PII. A criminal history record for example inherently contains PII as would a Law Enforcement National Data Exchange (N-DEx) case file.

  PII shall be extracted from CJI for the purpose of official business only. All PII, including that extracted from CJI, shall be handled in accordance with the policies of the City of Rosenberg.

VI. POLICY AND IMPLEMENTATION

The Policy areas focus upon the data and services the FBI CJIS Division exchanges and provides to the criminal justice community.

While the major theme of the policy areas is concerned with electronic exchange directly with the FBI, it is understood that further dissemination of CJI to Authorized Recipients by various means (hard copy, e-mail, web posting, etc.) constitutes a significant portion of CJI exchanges. Regardless of its form, use, or method of dissemination, CJI requires protection throughout its life.

The policy areas are:

- Policy Area 1—Information Exchange Agreements
- Policy Area 2—Security Awareness Training
- Policy Area 3—Incident Response
- Policy Area 4—Auditing and Accountability
- Policy Area 5—Access Control
- Policy Area 6—Identification and Authentication
- Policy Area 7—Configuration Management
- Policy Area 8—Media Protection
- Policy Area 9—Physical Protection
- Policy Area 10—System and Communications Protection and Information Integrity

- **Policy Area 1: Information Exchange Agreements**
  The information shared through communication mediums shall be protected with appropriate security safeguards. The agreements established by entities sharing information across systems and communications mediums are vital to ensuring all parties fully understand and agree to a set of security standards.

  Information exchange agreements outline the roles, responsibilities, and data ownership between agencies and any external parties. Information exchange agreements for agencies sharing CJI data that is sent to and/or received from the FBI CJIS shall specify the security controls and conditions described in this document. Information exchange agreements shall be supported by documentation committing both parties to the terms of information exchange.

  - **Management Control Agreements with the City of Rosenberg Information Services Department**
    The City of Rosenberg Information Services Department shall sign and execute a management control agreement (MCA) with the Rosenberg Police Department, which stipulates management control of the criminal justice function remains solely with the CJA, i.e. the Rosenberg Police Department.

  - **Private Contractor User Agreements and CJIS Security Addendum**
    A CJIS Security Addendum shall be signed by all private contractors who perform criminal justice functions for the CJA. Private contractors who perform criminal justice functions shall meet the same training and certification criteria required by governmental agencies performing a similar function, and shall be subject to the same extent of audit review as are local user agencies. All private contractors who perform criminal justice functions shall acknowledge, via signing of the CJIS Security Addendum Certification page, and abide by all aspects of the CJIS Security Addendum. Personnel shall verify the latest version of the form is being employed before the execution of any addenda.

    1. Private contractors designated to perform criminal justice functions for a CJA shall be eligible for access to CJI. Access shall be permitted pursuant to an agreement which specifically identifies the agency's purpose and scope of providing services for the administration of criminal justice. The agreement

between the CJA and the private contractor shall incorporate the CJIS Security Addendum approved by the Director of the FBI, acting for the U.S. Attorney General, as referenced in Title 28 CFR 20.33 (a)(7).

- **Secondary Dissemination**
  If CHRI is released to another authorized agency (e.g. the Office of the District Attorney), the releasing agency shall log such dissemination.
  - A cover sheet shall be completed for all hard copy data containing CHRI CJI (e.g. DA packet, CCH and CR) that leaves the office that generated it.
  - Personnel taking possession of the CHRI data shall sign the cover sheet and thereby acknowledgment that he/she understands that the data is restricted and commitment to proper disposition, destruction or disposal of the documents.

- **Secondary Dissemination of Non-CHRI CJI**
  If CJI does not contain CHRI and is not part of an information exchange agreement then it does not need to be logged.

  Dissemination shall conform to the following in order to validate the requestor of the CJI as an employee and/or contractor of a law enforcement agency or civil agency requiring the CJI to perform their mission or a member of the public receiving CJI via authorized dissemination:

  - Agencies requesting non-CHRI CJI shall complete such requests in writing on official agency letterhead. Requests may be submitted via standard mail, e-mail or fax. All such requests shall clearly indicate the following information:

    - Date of request
    - Name of requesting agency
    - Name of individual requesting information
    - Contact information (at a minimum, telephone number) for individual requesting information

  - Upon receipt of a request, TCOs shall confirm that the agency is authorized to receive CJI. This shall be accomplished by conducting an NLETS Orion File inquiry via Omnixx to confirm that the requesting agency has an Orion file (ORI). If the agency has an ORI, this constitutes authorization to receive CJI.
  - The TCO shall notify the Communications supervisor on duty, or, in their absence, the Sergeant on duty of the request and of the validity of the requesting agency's ORI before releasing information.

- **Policy Area 2: Security Awareness Training**
  Basic security awareness training shall be provided within six months of initial assignment, and biennially thereafter, for all personnel who have access to CJI. Training will be documented and maintained for all personnel. Incident response training shall be included as part of required security awareness training.

- **Policy Area 3: Incident Response**
  The Rosenberg Police Department will follow the procedures outlined by the City of Rosenberg policy as well as those of this document to safeguard against breaches. Security breaches shall include, but not be limited to, one of the following:

  - Security policy violation
  - Misuse of password (e.g. use of password by another employee)
  - Identification of malware or computer virus on an information system connected to TLETS/NLETS

  Incidents shall be promptly reported as outlined in the Incident Handling Response Plan (Appendix A) upon recognition of suspected or actual security breaches.
  Incidents will be further investigated and handled in accordance with the policies of the Information Services Department of the City of Rosenberg.

- **Policy Area 4: Auditing and Accountability**
  The information systems of the Rosenberg Police Department shall generate audit records for defined events as laid out by CJIS policy. The list of auditable events shall be reviewed periodically and updated as necessary.

  - **Events**
    The following events shall be logged:
    1. Successful and unsuccessful system log-on attempts.
    2. Successful and unsuccessful attempts to:
       a. access permission on a user account, file, directory or other system resource;
       b. create permission on a user account, file, directory or other system resource;
       c. write permission on a user account, file, directory or other system resource;
       d. delete permission on a user account, file, directory or other system resource;
       e. change permission on a user account, file, directory or other system resource.
    3. Successful and unsuccessful attempts to change account passwords.
    4. Successful and unsuccessful actions by privileged accounts.
    5. Successful and unsuccessful attempts for users to:
       a. access the audit log file;
       b. modify the audit log file;
       c. destroy the audit log file.

  - **Content**
    The following content shall be included with every audited event:
    1. Date and time of the event.
    2. The component of the information system (e.g., software component, hardware component) where the event occurred.
    3. Type of event.
    4. User/subject identity.
    5. Outcome (success or failure) of the event.

- **Response to Audit Processing Failures**
  The agency's information system shall provide alerts to the appropriate agency officials in the event of an audit processing failure (i.e. the Administrative Lieutenant and the IS Department of the City of Rosenberg). Audit processing failures include, for example: software/hardware errors, failures in the audit capturing mechanisms, and audit storage capacity being reached or exceeded.

- **Audit Monitoring, Analysis, and Reporting**
  The Administrative Lieutenant, or other responsible management official, shall designate an individual or position to review/analyze information system audit records for indications of inappropriate or unusual activity, investigate suspicious activity or suspected violations, to report findings to appropriate officials, and to take necessary actions. Audit review/analysis shall be conducted at a minimum once a week. The frequency of review/analysis should be increased when the volume of an agency's processing indicates an elevated need for audit review. The agency shall increase the level of audit monitoring and analysis activity within the information system whenever there is an indication of increased risk to agency operations, agency assets, or individuals based on law enforcement information, intelligence information, or other credible sources of information.

- **Time Stamps**
  The information systems performing auditing functionalities shall provide time stamps for use in audit record generation. The time stamps shall include the date and time values generated by the internal system clocks in the audit records. The agency shall synchronize internal information system clocks on an annual basis.

- **Protection of Audit Information**
  The agency's information system shall protect audit information and audit tools from modification, deletion and unauthorized access.

- **Audit Record Retention**
  The agency shall retain audit records for at least one (1) year. Once the minimum retention time period has passed, the agency shall continue to retain audit records until it is determined they are no longer needed for administrative, legal, audit, or other operational purposes. This includes, for example, retention and availability of audit records relative to Freedom of Information Act (FOIA) requests, subpoena, and law enforcement actions.

- **Logging NCIC and III Transactions**
  A log shall be maintained for a minimum of one (1) year on all NCIC and III transactions. The III portion of the log shall clearly identify both the operator and the authorized receiving agency. III logs shall also clearly identify the requester and the secondary recipient. The identification on the log shall take the form of a unique identifier that shall remain unique to the individual requester and to the secondary recipient throughout the minimum one year retention period.

- **Policy Area 5: Access Control**

- **Account Management**

  - **Account Creation and Activation**
    Account creation and activation shall be managed according to the policy of the City of Rosenberg Information Services Department. Users will be assigned group membership and appropriate authorization upon creation and as needed.

  - **Account Validation**
    Users shall be validated annually by the TAC or his/her alternate and documentation shall be retained. Validation shall confirm, at a minimum, a verification of active users.

  - **Account Disabling**
    Upon termination or transfer, all associated accounts will be disabled in Spillman and Omnixx by the LASO and TAC. All other permissions and access shall be removed or disabled by the Information Services Department of the City of Rosenberg.

- **System Use Notification**
  All information systems from which CJI may be accessed shall display an approved system use notification message, before granting access, informing potential users of various usages and monitoring rules. The system use notification message shall, at a minimum, provide the following information:

  1. The user is accessing a restricted information system.
  2. System usage may be monitored, recorded, and subject to audit.
  3. Unauthorized use of the system is prohibited and may be subject to criminal and/or civil penalties.
  4. Use of the system indicates consent to monitoring and recording.

  The system use notification message shall provide appropriate privacy and security notices (based on associated privacy and security policies or summaries) and remain on the screen until the user acknowledges the notification and takes explicit actions to log on to the information system.

- **Session Lock**
  The information system shall prevent further access to the system by initiating a session lock after a maximum of 30 minutes of inactivity, and the session lock remains in effect until the user reestablishes access using appropriate identification and authentication procedures. The session lock shall take the form of a screen saver with password.

  Users shall directly initiate session lock mechanisms to prevent inadvertent viewing when a device is unattended. A session lock is not a substitute for logging out of the information system.

In the interest of officer safety, devices that are: (1) part of a police vehicle; or (2) used to perform dispatch functions and located within a physically secure location, are exempt from this requirement.

- **Personally Owned Information Systems**
  A personally owned information system shall not be authorized to access, process, store or transmit CJI or be connected to the internal TLETS network.

- **Wireless Access Restrictions**
  All personnel shall conform to the policy of the Information Services Department of the City of Rosenberg concerning the use of wireless devices and access.

- **Cellular Risk Mitigations**
  Organizations shall, at a minimum, ensure that cellular devices:

  1. Apply available critical patches and upgrades to the operating system as soon as they become available for the device and after necessary testing.
  2. Are configured for local device authentication.
  3. Use advanced authentication.
  4. Erase cached information when session is terminated.
  5. Employ personal firewalls or run a Mobile Device Management (MDM) system that facilitates the ability to provide firewall services from the agency level.
  6. Employ antivirus software or run a MDM system that facilitates the ability to provide antivirus services from the agency level.

- **Policy Area 6: Identification and Authentication**

  - **Identification Policy and Procedures**
    Each person who is authorized to store, process, and/or transmit CJI shall be uniquely identified by the assignment of a Spillman user name, an Omnixx login, and an access badge allowing access to secure areas. Yearly validations shall ensure that all user IDs belong to currently authorized users. Identification data shall be kept current by adding new users and disabling and/or deleting former users.

  - **Password**
    The Rosenberg Police Department shall follow the secure password attributes, below, to authenticate an individual's unique ID. Passwords shall:

    - Be a minimum length of eight (8) characters on all systems.
    - Not be a dictionary word or proper name.
    - Not be the same as the Userid.
    - Expire within a maximum of 90 calendar days.
    - Not be identical to the previous ten (10) passwords.
    - Not be transmitted in the clear outside the secure location.
    - Not be displayed when entered.

- **Policy Area 7: Configuration Management**

    - **Network Diagram**
      The Information Services Department of the City of Rosenberg shall ensure that a complete topological drawing depicting the interconnectivity of the agency network, to criminal justice information systems and services is maintained in a current status.
      The network topological drawing shall include the following:

        1. All communications paths, circuits, and other components used for the interconnection, beginning with the agency-owned system(s) and traversing through all interconnected systems to the agency end-point.
        2. The logical location of all components (e.g., firewalls, routers, switches, hubs, servers, encryption devices, and computer workstations). Individual workstations (clients) do not have to be shown; the number of clients is sufficient.
        3. "For Official Use Only" (FOUO) markings.
        4. The agency name and date (day, month, and year) drawing was created or updated.

- **Policy Area 8: Media Protection**

    - **Media Storage and Access**
      All electronic and physical media shall be stored within physically secure locations or controlled areas. Access to electronic and physical media is limited to authorized individuals.

    - **Physical Media in Transit**
      The controls and security measures in this document also apply to CJI in physical (printed documents, printed imagery, etc.) form. A CJI coversheet tracking chain-of-custody shall be used for all physical media to be transported outside of the secure location. (See **Policy Area 1 – Secondary Dissemination**)

    - **Electronic Media Sanitization and Disposal**
      The Rosenberg Police Department shall follow the policies for electronic media sanitization and disposal as set forth by the Information Services Department of the City of Rosenberg.

    - **Disposal of Physical Media**
      Physical media shall be disposed of according to the policies of the City of Rosenberg and as set forth by local, state and federal regulations. Physical media containing CJI or PII shall be shredded on site. Destruction shall be witnessed and documented by authorized personnel.

- **Policy Area 9: Physical Protection**

- **Physical Access Authorizations**
  The City of Rosenberg shall issue credentials to authorized personnel who are allowed access to the physically secure areas.

- **Access Control for Display Medium**
  Physical access to information system devices that display CJI shall be controlled. Additionally, such information system shall be positioned in such a way as to prevent unauthorized individuals from accessing and viewing CJI. Employees are responsible to secure the screen on their mobile terminal prior to exiting their patrol vehicle and while conducting prisoner transports. The employee is responsible to ensure law enforcement sensitive information and CJIS information being displayed on their computer screen is not visible to the public or individuals being transported in the vehicle.

- **Monitoring Physical Access**
  Physical access to secure areas and information systems shall be monitored to detect and respond to physical security incidents.

- **Visitor Control**
  Physical access shall be controlled by authenticating visitors before authorizing escorted access to the physically secure location (except for those areas designated as publicly accessible). Visitors shall be escorted and monitored at all times.

- **Delivery and Removal**
  The LASO shall authorize and control information system-related items entering and exiting the physically secure location.

- **Policy Area 10: System and Communications Protection and Information Integrity**

  - **Information Flow Enforcement**
    Any and all CJI data that leaves the secure location shall be encrypted in accordance with the most current CJIS standards, as prescribed.

  - **Boundary Protection**
    The Rosenberg Police Department shall work in the established network framework as established by the Information Services Department of the City of Rosenberg. This framework shall, as a minimum:

    1. Control access to networks processing CJI.
    2. Monitor and control communications at the external boundary of the information system and at key internal boundaries within the system.
    3. Ensure any connections to the Internet, other external networks, or information systems occur through controlled interfaces (e.g. proxies, gateways, routers, firewalls, encrypted tunnels.
    4. Employ tools and techniques to monitor network events, detect attacks, and provide identification of unauthorized use.

5. Ensure the operational failure of the boundary protection mechanisms do not result in any unauthorized release of information outside of the information system boundary (i.e. the device shall "fail closed" vs. "fail open").

- **Encryption**
  Any and all CJI data that leaves the secure location shall be encrypted in accordance with the most current CJIS standards, as prescribed. At a minimum:

  1. Encryption shall be a minimum of 128 bit.
  2. When CJI is transmitted outside the boundary of the physically secure location, the data shall be immediately protected via cryptographic mechanisms (encryption).
  3. When CJI is at rest (i.e. stored electronically) outside the boundary of the physically secure location, the data shall be protected via cryptographic mechanisms (encryption).
  4. When encryption is employed, the cryptographic module used shall be certified to meet FIPS 140-2 standards.

- **Voice over Internet Protocol**
  The Rosenberg Police Department shall follow all guidance and instructions regarding the use of Voice over Internet Protocol (VoIP) as set forth by the Information Services Department of the City of Rosenberg and in accordance with contractual agreements with the VoIP service provider.

- **Malicious Code, Spam and Spyware Protection**
  All IT systems with CJIS connectivity shall be protected with anti-virus, anti-spam and spyware protection. This shall be performed and maintained in accordance with the policies of the Information Services Department of the City of Rosenberg.

- **Personal Firewall**
  A personal firewall shall be employed on all devices that are mobile by design (i.e. laptops, handhelds, personal digital assistants, etc.). For the purpose of this Policy, a personal firewall is an application that controls network traffic to and from a user device, permitting or denying communications based on policy. At a minimum, the personal firewall shall perform the following activities:

  1. Manage program access to the Internet.
  2. Block unsolicited requests to connect to the user device.
  3. Filter incoming traffic by IP address or protocol.
  4. Filter incoming traffic by destination ports.
  5. Maintain an IP traffic log.

- **Security Alerts and Advisories**
  The Rosenberg Police Department shall follow the policies and guidance of the Information Services Department of the City of Rosenberg in reference to receiving and disseminating information system security alerts and advisories. Additional monitoring shall be conducted in accordance with the most current industry standards and departmental needs.

Appendix A

TLETS Security Incident Response Plan

There has been an increase in the number of accidental or malicious computer attacks against both government and private agencies, regardless of whether the systems are high or low profile. The following establishes an operational incident handling procedure for the Rosenberg Police Department's CJIS, TCIC/NCIC, and TLETS information systems that includes adequate preparation, detection, analysis, containment, recovery, and user response activities; track, document, and report incidents to appropriate personnel, TCIC agency officials and/or authorities. The Administrative Lieutenant is the department's point-of-contact for security-related issues and will ensure the incident response reporting procedures are initiated at the local level.

Reporting Information Security Events

The department will promptly report incident information to appropriate authorities. Information security events and weaknesses associated with information systems shall be communicated in a manner allowing timely corrective action to be taken. Formal event reporting and escalation procedures shall be in place. Wherever feasible, the department will use email to expedite the reporting of security incidents. All Communications Specialists will be made aware of the procedures for reporting the different types of events and weaknesses that might have an impact on the security of agency assets and are required to report any information security events and weaknesses as quickly as possible to the Administrative Lieutenant or the on-call IT Specialist.

Reporting Procedures for Suspected and Actual Security Breaches:

If you become aware of any policy violation or suspect that your password may have been used by someone else, first, change your password, and then report the violation immediately to the Administrative Lieutenant or the on-call IT Specialist.

Virus Reporting Procedures and Collection of Security Incident Information:

Upon identifying a problem

1. Disconnect the Ethernet cord connected to the infected information system and power down the system.

2. Notify the Administrative Lieutenant, the Terminal Agency Coordinator (TAC), and the Communications Chain-of-Command.

3. Notify the Information Technology Security Administrator.

Communications Personnel

1. Notify Ft. Bend County Sheriff's Office that TLETS will be re-routed.

2. Re-route TLETS to Ft. Bend County while the problem is addressed.

3. The TLETS system will remain disconnected from TLETS until Information Services can guarantee systems are free from virus infection.

Once free from infection and given clearance by IS personnel

1. Reconnect the system to TLETS and NLETS by reconnecting the Ethernet cord to the system and power up the system.
2. Route TLETS back to the Rosenberg Police Department.
3. Notify Ft. Bend County Sheriff's Office that TLETS has been routed back to our agency and operations are normal.