	ARGYLE POLICE DEPARTMENT
	CRIMINAL JUSTICE INFORMATION SERVICES (CJIS) SECURITY
	Effective Date: 21DEC20
	Approved: _____ **Chief of Police**
	Reference: FBI Criminal Justice Information Services (CJIS) Security Policy, Version 5.8, 06/01/2019

I. PURPOSE

The intent of the following policies is to ensure the protection of the Criminal Justice Information (CJI) and its subset of Criminal History Record Information (CHRI) until such time as the information is purged or destroyed in accordance with applicable record retention rules.

The following policies were developed using the FBI's Criminal Justice Information Services (CJIS) Security Policy. The Argyle Police Department may complement this policy with a local policy; however, the CJIS Security Policy shall always be the minimum standard.

A. The purpose of this directive is to provide Police Department members specific guidelines and procedures relating to who can access criminal justice information (CJI) and how to maintain proper security of CJI data.

B. The directive also identifies the roles and responsibilities of certain people when the security of CJI data or a PC that accesses CJI has been breached.

Persons in violation of this general order are subject to disciplinary action, up to an including loss of access privileges, civil and criminal prosecution and/or termination of employment.

II. SCOPE

The scope of this policy applies to any electronic or physical media containing FBI CJI while being stored, accessed or physically moved from a secure location from the Argyle Police Department. In addition, this policy applies to any authorized person who accesses, stores, and/or transports electronic or physical media.

III. DEFINITIONS

A. **Access to Criminal Justice Information (CJI)** - is the physical or logical (electronic) ability, right or privilege to view, modify or make use of criminal justice information (CJI).

B. **Administration of Criminal Justice** – The detection, apprehension, detention, pre-trial release, post-trial release, prosecution, adjudication, correctional supervision, or rehabilitation of accused persons or criminal offenders. It also includes criminal identification activities; the collection, storage, and dissemination of criminal history record information; and criminal justice employment. In addition, *administration of criminal Justice* includes "crime prevention programs" to the extent access to criminal history record information is limited to law enforcement agencies for law enforcement programs (e.g. record checks of individuals who participate in Neighborhood Watch or "safe house" programs) and the result of such checks will not be disseminated outside the law enforcement agency.

C. **Authorized Person** – is a person who has completed security awareness training as prescribed in section VI, has been fingerprinted, and has been subjected to a background check. An authorized person may include Town and Police Department employees, peace officers from other agencies, service technicians, and contractors.

D. **Contractor** – is a private business, agency, or individual which has entered into an agreement for the administration of criminal justice or non-criminal justice functions with a Criminal Justice Agency or a Non-Criminal Justice Agency. Also, a private business approved by the FBI CJIS Division to contract with Non-Criminal Justice Agencies to perform non-criminal justice functions associated with civil fingerprint submission for hiring purposes.

E. **Criminal History Record Information (CHRI)** - is a subset of CJI and for the purposes of this document is considered interchangeable. 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 in this policy, Title 28, Part 20, Code of Federal Regulations (CFR), defines CHRI and provides the regulatory guidance for dissemination of CHRI.

F. **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, 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 tomake hiring decisions.

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.

5. **Case/Incident History** - information about the history of criminal incidents.

G. **Criminal Justice Information Services Division (CJIS)** – is 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.

H. **CJIS Systems Agency (CSA)** - is a duly authorized state, federal, international, tribal, or territorial criminal justice agency on the CJIS network providing statewide (or equivalent) service to its criminal justice users with respect to the CJIS data from various systems managed by the FBI CJIS Division. The Texas Department of Public Safety is the CSA for the State of Texas.

I. **DPS Background Check** – for the purpose of this directive, a *DPS background check* is a state run, national fingerprint-based background records check.

J. **Local Agency Security Officer (LASO)** – The primary information security contact between a local law enforcement agency and the Texas Department of Public Safety under which this agency interfaces with the FBI CJIS Division. The LASO actively represents the local 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 Texas Department of Public Safety informed as to any Information Security needs and problems. For the purposes of this directive, *LASO* is Sergeant Daniel Rounsavall.

K. **Security Awareness Training** – is the training provided or approved by the Texas Department of Public Safety that satisfies CJIS security training requirements prescribed in section VI.

L. **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. For the purposes of this directive, the TAC is Sergeant Daniel Rounsavall.

IV. Proper Access, Use, and Dissemination of CHRI

Information obtained from the Interstate Identification Index (III) is considered CHRI. Rules governing the access, use, and dissemination of CHRI are found in Title 28, Part 20, CFR.

A. The III shall be accessed only for an authorized purpose.

B. CHRI shall only be used for an authorized purpose consistent with the purpose for which III was

accessed.

C. Dissemination to another agency is authorized if:

1. The other agency is an Authorized Recipient of such information and is being serviced by the accessing agency, or
2. The other agency is performing noncriminal justice administrative functions on behalf of the authorized recipient and the outsourcing of said functions has been approved by appropriate CJIS Systems Agency (CSA) or State Identification Bureau (SIB) officials with applicable agreements in place.

V. Personnel Security Screening

A. Access to CJI and/or CHRI is restricted to authorized personnel.

B. Personnel with access to CHRI for the purposes of licensing or employment shall submit to a civil fingerprint-based record check within 30 days of employment or assignment if they:
1. have direct access to CJI,
2. have direct responsibility to configure and maintain computer systems and networks with direct access to CJI, or
3. have access to physically secure locations or controlled areas containing CJI.

VI. Security Awareness Training (CJIS 5.2.1)

A. Basic security awareness training shall be required within six months of initial assignment, and biennially thereafter, for all personnel who have access to CJI.

B. The TAC and/or his/her designee shall be responsible for making sure that all authorized personnel receive the required security awareness training.

VII. Physical Security

A. A physically secure location is a facility or an area, a room, or a group of rooms within a facility with both the physical and personnel security controls sufficient to protect the FBI CJI and associated information systems (CJIS 5.9.1).

B. The perimeter of the physically secure location shall be prominently posted and separated from non-secure locations by physical controls. Security perimeters shall be defined, controlled and secured in a manner acceptable to the CSA or SIB (CJIS 5.9.1.1).

C. Only authorized personnel will have access to physically secure non-public locations. The Argyle Police Department will maintain and keep current a list of authorized personnel (CJIS 5.9.1.2).

D. All physical access points into the agency's secure areas will be authorized before granting access.

1. Access to physically secure areas including police vehicles, is controlled by key or electronic lock released by key fob and/or key card.
2. Visitors shall be authorized persons or shall be escorted by an authorized person in accordance with this policy.

E. The agency will implement access controls and monitoring of physically secure areas for protecting all transmission and display mediums of CJI.

1. Police department employees shall control physical access to information system devices (computers) that display CJI and shall position Information system devices in such a way as to prevent unauthorized individuals from accessing and viewing CJI.

2. Preventing unauthorized access or viewing can be accomplished by:

   a. Blanking the display;
   b. Closing the display (on notebook computers)'
   c. Placing a privacy screen on the display;
   d. Enabling a password protected screensaver function that starts within five (5) minutes of inactivity.

F. Authorized personnel will take necessary steps to prevent and protect the agency from physical, logical and electronic breaches.

VIII. Media Protection

A. Controls shall be in place to protect electronic and physical media containing CJI while at rest, stored, or actively being accessed. "Electronic media" includes memory devices in laptops and computers (hard drives) and any removable, transportable digital memory media, such as magnetic tape or disk, backup medium, optical disk, flash drives, external hard drives, or digital memory card. "Physical media" includes printed documents and imagery that contain CJI.

B. The agency shall securely store electronic and physical media within physically secure locations or controlled areas. The agency shall restrict access to electronic and physical media to authorized individuals. If physical and personnel restrictions are not feasible then the data shall be encrypted (CJIS 5.10.1.2).

C. No media that will store CJI data or any PC that will access CJI data will be used by the Police Department until the Information Technology Department has verified that the media is free of any virus, Trojan horse, worm, and other harmful matter.

IX. Media Transport

A. Any time a PC that has media that contains CJI data must leave the Police Department facility for repairs, the media containing the data must first be sanitized or removed from the PC.

B. No electronic and/or physical media shall be transported outside of controlled areas unless:

1. the media remains in the custody and control of an authorized person; or
2. the media has been sanitized prior to transport.

X. Media Sanitization and Disposal

A. When no longer usable, hard drives, diskettes, tape cartridges, CDs, ribbons, hard copies, print-outs, and other similar items used to process, store and/or transmit FBI CJI shall be properly disposed of in accordance with measures established by Argyle Police Department.

B. Physical media (printouts and other physical media) shall be disposed of by one of the following methods:

1. shredding using Argyle Police Department issued shredders.
2. incineration using Argyle Police Department incinerators or witnessed by Argyle Police Department personnel onsite at agency or at contractor incineration site, if conducted by non-authorized personnel.

C. Electronic media (hard-drives, tape cartridge, CDs, printer ribbons, flash drives, printer and copier hard drives, etc.) shall be disposed of by one of the Argyle Police Department methods:

1. **Overwriting (at least 3 times)** - an effective method of clearing data from magnetic media. As the name implies, overwriting uses a program to write (1s, 0s, or a combination of both) onto the location of the media where the file to be sanitized is located.
2. **Degaussing** - a method to magnetically erase data from magnetic media. Two types of degaussing exist: strong magnets and electric degausses. Note that common magnets (e.g., those used to hang a picture on a wall) are fairly weak and cannot effectively degauss magnetic media.
3. **Destruction** – a method of destroying magnetic media. As the name implies, destruction of magnetic media is to physically dismantle by methods of crushing, disassembling, etc., ensuring that the platters have been physically destroyed so that no data can be pulled.

D. IT systems that have been used to process, store, or transmit FBI CJI and/or sensitive and classified information shall not be released from Argyle Police Department's control until the equipment has been sanitized and all stored information has been cleared using one of the above methods.

XI. Account Management

A. The Argyle Police Department shall manage information system accounts, including establishing, activating, modifying, reviewing, disabling, and removing accounts. The TAC shall validate information system accounts at least annually and shall document the validation process.

B. All accounts shall be reviewed at least annually by the designated CJIS point of contact (POC) or his/her designee to ensure that access and account privileges commensurate with job functions, need-to-know, and employment status on systems that contain Criminal Justice Information. The POC may also conduct periodic reviews.

XII. Remote Access

A. The Argyle Police Department shall authorize, monitor, and control all methods of remote access to the information systems that can access, process, transmit, and/or store FBI CJI. Remote access is any temporary access to an agency's information system by a user (or an information system) communicating temporarily through an external, non-agency-controlled network (e.g., the Internet).

B. The Argyle Police Department shall employ automated mechanisms to facilitate the monitoring and control of remote access methods. The Argyle Police Department shall control all remote accesses through managed access control points. The Argyle Police Department may permit remote access for privileged functions only for compelling operational needs but shall document the rationale for such access in the security plan for the information system.

C. Utilizing publicly accessible computers to access, process, store or transmit CJI is strictly prohibited. Publicly accessible computers include, but are not limited to,: hotel business center computers, convention center computers, public library computers, public kiosk computers, etc.

XIII. Personally Owned Information Systems

A personally owned information system shall not be authorized to access, process, store or transmit CJI. A personal device includes any portable technology like camera, USB flash drives, USB thumb drives, DVDs, CDs, air cards and mobile wireless devices such as Androids, Blackberry OS, Apple iOS, Windows Mobile, Symbian, tablets, laptops or any personal desktop computer. When bring your own devices (BYOD) are authorized, they shall be controlled using the requirements in Section 5.13 of the CJIS Security Policy.

XIV. Reporting Information Security Events

A. Incident Definition. For the purposes of this section, *incident* means: an accidental or malicious computer attack (i.e., virus, Trojan horse, worm, etc.) against the agency's computers that access CJI; or someone obtaining another user's secure login and password to an application that can access CJI.

B. The Argyle Police Department shall promptly report incident information to appropriate authorities to include the state CSA or SIB's Information Security Officer (ISO). The LASO and

TAC serve as the Police Department's point of contact. The LASO and TAC for the Argyle Police Department is Sergeant Daniel Rounsavall, who can be contacted via email at drounsavall@argyletx.com or via telephone at (903)348-2788. The Town's Information Technology Contractor is The Fulcrum Group, who can be contacted via email at helpdesk@fulcrumgroup.net or via telephone at (817)898-1277.

C. 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. All employees, contractors and third party users shall be made aware of the procedures for reporting the different types of event and weakness 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 designated point of contact (CJIS 5.3.1).

D. Attack on Computer

1. An employee who encounters an incident involving an attack on a computer that contains an application that has access to CJI data shall immediately:

    a. Power off the computer or unplug its power cord if the computer will not power down. Under no circumstances should any individual continue to use an infected computer;
    b. If the computer is connected to the network by an ethernet cable, disconnect the cable from the computer;
    c. If the computer is a Mobile Data Terminal in a police vehicle, power it down and discontinue use of this vehicle;
    d. If the computer is a PC, place a note on the PC that the PC is not to be used;
    e. Notify the LASO without unnecessary delay via phone or e-mail;
    f. Complete the TLETS Security Incident Response Form, which is included in Appendix A at the end of this General Order;
    g. Prepare and submit to the LASO a work order for the affected computer.

2. The Town's Information Technology contractor shall inspect the computer to determine whether it has been compromised.

3. If the computer has been compromised:

    a. the LASO shall notify Texas DPS;
    b. the computer must be removed from the network;
    c. its hard drive must be cleaned or completely wiped by the Town's Information Technology Department before it can be placed back in service.

E. If an employee's secure login and/or password to an application that can access CJI data has been compromised, the employee shall immediately change his/her password, if possible, and notify the agency TAC.

XV. Policy Violation/Misuse Notification

A. Violation of any of the requirements contained in the CJIS Security Policy or Title 28, Part 20, CFR, by any authorized personnel will result in suitable disciplinary action, up to and including loss of access privileges, civil and criminal prosecution and/or termination.

B. Any violation of the requirements contained in the CJIS Security Policy or Title 28, Part 20, CFR, by any visitor can result in similar disciplinary action against the sponsoring employee, and can also result in termination of services with any associated consulting organization or prosecution in the case of criminal activity.