GENERAL ORDERS:	Chapter 29	**PUBLISHED DATE:**	12/7/2020
		EFFECTIVE DATE:	12/7/2020
APPROVED BY:	Chief Dana Wingert	**REVISED DATE:**	

Criminal Justice Information Security and Disposal

I. Purpose

The purpose of this policy is to provide appropriate controls to protect Criminal Justice Information (CJI) from creation through dissemination and destruction.

II. Policy

The department will follow the FBI Criminal Justice Information Services (CJIS) Security Policy. Employees shall protect and control electronic and physical CJI while at rest and in transit and take appropriate safeguards for protecting CJI to limit potential mishandling or loss while being stored, accessed, or transported. Classified and sensitive data shall be properly disposed of, when no longer usable, in accordance with this policy.

III. Definitions

Arrest Data – Information pertaining to an arrest for a public offense and includes the charge, date, time and place. Includes arrest warrants for all public offenses outstanding and not served and includes the filing of charges, by preliminary information, the date and place of alleged commission and county of jurisdiction.

Criminal History Data – Any of the following information maintained by the Iowa Department of Public Safety in a manual or automated data storage system and individually identified: arrest, conviction, disposition, correctional, adjudication, and custody data.

Criminal Investigative Data – Information collected during an investigation where there are reasonable grounds to suspect that specific criminal acts have been committed by a person.

Criminal Justice Information (CJI) – The term used to describe all FBI CJIS provided data necessary for a law enforcement agency to perform their mission including, but not limited to biometric, identity history, biographic, property and case/incident history data.

Intelligence Data – Information on identifiable individuals compiled in an effort to anticipate, prevent, or monitor possible criminal activity.

Surveillance Data – Information on individuals, pertaining to participation in organizations, groups, meetings or assemblies, where there are no reasonable grounds to suspect involvement or participation in criminal activity by any person.

IV. Roles

A. Terminal Agency Coordinator (TAC)
   1. The TAC role is assigned to the Communications Section Administrator within the Administration Division.

B. Police Technology Section (PTS)
    1. The Public Safety Systems Manager, who reports to the City Information Technology Department, along with PTS will work in partnership with the TAC to ensure compliance with state and federal CJIS policies.

V. Criminal justice information media protection

A. Scope
    1. Applies to any:
        a. Electronic or physical media containing CJI while being stored, accessed or physically moved from a secure location in the department
        b. Authorized person who accesses, stores or transports electronic or physical CJI media

B. Media protection
    1. Employees shall follow appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of CJI, such as:
        a. Restricting access to electronic and physical media to authorized individuals
        b. Escorting, by authorized personnel, of visitors who are in secure areas where CJI data is present
        c. Locking or logging off computers when not in the immediate vicinity of the work area
        d. Not using:
            (1) Public computers to access, store or transmit CJI, such as hotel business center computers or public library computers
            (2) Any mobile devices such as smartphones or tablets, or any personally owned information systems to access, store, or transmit CJI unless authorized by the department
                (a) Mobile devices do not include department issued laptop computers with appropriate secure login access.
        e. Securely storing:
            (1) Electronic and physical media within a physically secure or controlled area such as a locked drawer, cabinet or room
            (2) All hardcopy CJI printouts in an area accessible to only those employees whose job function require them to handle such documents and ensuring that only authorized users remove CJI printed or digital media
        f. Physically protecting CJI until media end of life when it is destroyed or sanitized using approved equipment, techniques and procedures.
        g. Taking appropriate action when in possession of CJI while not in a secure area:
            (1) CJI must not leave the employee's immediate control while physical controls are not in place and shall not be left in plain public view.
            (2) Precautions must be taken to obscure CJI from public view, such as by means of an opaque filter or envelope for hard copy printouts. For electronic devices like laptops, use session lock or privacy screens.
        h. When CJI is electronically transmitted or stored outside the boundary of the physically secure location, the data shall be immediately protected using encryption.
            (1) Storage devices include external hard drives from computers, printers and copiers used with CJI, thumb drives, flash drives, magnetic tape, CD's/DVD's and laptops.

C. Media transport
    1. During transport, employees shall protect electronic and physical media containing CJI to prevent inappropriate use and disclosure through the following means:
        a. Securing hand carried confidential electronic and paper documents by:

(1) Storing CJI in a locked briefcase or lockbox
(2) Only viewing or accessing the CJI electronically or in a physically secure location with authorized personnel
(3) Packaging hardcopy printouts in such a way as to not have any CJI viewable
(4) Having complete shipment tracking and history when mailing, along with signature confirmation of delivery, to ensure the release to authorized individuals

b. Restrict the pickup, transfer and delivery of CJI to authorized personnel
c. Not taking CJI home or when travelling unless authorized

2. Dissemination to another agency is authorized if the other agency is:
   a. An authorized recipient of such information or,
   b. Performing personnel and appointment functions for criminal justice employment applicants

D. Breach notification and incident reporting
1. The department will promptly report incident information to the appropriate authorities.
2. If CJI is improperly used, disclosed, lost, or reported as not received, the following procedures will be followed:
   a. The employee shall notify their supervisor and a memo submitted within 24 hours of discovery containing a detailed account of the incident, events leading to the incident, and steps taken or to be taken in response to the incident.
   b. The supervisor will communicate the situation to the TAC (Communications Section Administrator).
      (1) In the case of CJI misuse, the TAC will be responsible for reporting the misuse to the Iowa Department of Public Safety.
   c. The TAC will ensure the Public Safety Systems Manager or designee is promptly informed of IT security incidents.
      (1) The Police Technology Section (PTS) will establish a security incident response and reporting procedure to discover, investigate, document, and report to the Iowa Department of Public Safety Technology Services Bureau and the FBI CJIS Division ISO major incidents that significantly endanger the security or integrity of CJI.
      (2) PTS will collect and disseminate all security incident related information received from the DOJ, FBI CJIS Division, and other entities to the department.

VI. Disposal of media (physical or electronic) and procedures

A. Scope
1. Applies to all employees, contractors, temporary staff and other individuals with access to FBI CJIS systems or data, sensitive and classified data, and media and to all equipment that processes, stores, or transmits such data.
2. When no longer usable, any electronic storage media, hard copies, print-outs and other similar items used to process, store or transmit FBI CJI and classified and sensitive data shall be properly disposed of in accordance with this policy.
   a. Physical media (print-outs and other physical media) shall be disposed of by one of the following methods:
      (1) Using department shredders
      (2) Placed in locking shredding bins for a contractor to come on-site and shred as witnessed by a department employee
   b. Electronic media (hard-drives, CD's, flash drives, etc.) shall be disposed by one of the following:
      (1) Overwriting (at least 3 times) – using a program to write 1s and 0s onto the location of media where the file is to be sanitized

(2) Degaussing – magnetically erase data from magnetic media using strong magnets or electronic degausses
(3) Destruction – physically destroying magnetic media by crushing or disassembling so that no data can be pulled

c. IT systems that have been used to process, store, or transmit CJI shall not be released from department control until the equipment has been sanitized and all stored information has been cleared using the above methods.

VII. Use and release of criminal justice information

A. General
1. Employees shall not inappropriately disclose any information connected with their employment that might discredit or imperil the efficiency of the department unless authorized or ordered.
2. Iowa Code Chapter 692 regulates "Criminal History Data", "Intelligence Data", "Investigative Data", and "Surveillance Data", and prescribes the conditions under which such data may be released. It also prescribes criminal and civil penalties for improperly handling and releasing such data.
3. Employees shall adhere to Iowa Code Chapter 232 and any other related Iowa Code Chapter which strictly controls the release of information pertaining to a juvenile.
   a. Juvenile records and files in all cases, including those alleging delinquency shall be confidential and are not public records except:
      (1) Information pertaining to a child who is at least ten years of age and who is taken into custody for a delinquent act which would be a forcible felony offense if committed by an adult unless sealed or restricted by court order or,
      (2) When specifically allowed by Iowa Code
   b. Any release of juvenile records and files should be approved by an authority on the subject.

B. Criminal history data
1. State and federal criminal history data may not be disseminated outside the department unless it is for official purposes.
   a. An electronic record, identifying the employee and purpose of inquiry, will be created each time a criminal history is requested via the IOWA or NCIC system.

C. Arrest data
1. Arrest data originating with the department, subject to juvenile restrictions, may be disseminated without legal restraint.

D. Intelligence data
1. Intelligence data may be disseminated:
   a. Within the department without restriction
   b. Outside of the department if:
      (1) It is for official purposes and,
      (2) A record of the person or organization, date, and purpose of dissemination is available and,
      (3) The need to know and intended use are reasonable
2. Examples of intelligence data include:
   a. Field Intelligence Reports (FIR)
   b. Intelligence bulletins and reports
   c. Supplemental reports written primarily to anticipate, prevent, or monitor possible criminal activity

E. Criminal investigative data

1. Criminal investigative data, subject to juvenile restrictions, may be disseminated without legal restraint.
    a. The department may restrict the dissemination as allowed by Iowa Code.
2. Police reports pertaining to a criminal case are an example of criminal investigative data.

F. Surveillance data
1. Employees are prohibited from placing surveillance data in files or data storage systems.
2. Information on a political or protest group that is peaceful in nature and where there are no reasonable grounds to suspect violation of the law is an example of surveillance data.