	Bridgeport Police Department POLICY AND PROCEDURE GENERAL ORDER	Distribution ALL PERSONNEL	General Order Number **10.12**
		Original Issue Date 7/16/19	Reissue/Effective Date 7/16/19
Order Title: **NCIC, CJIS and COLLECT PROCEDURES**		Accreditation Standard: POSTC: 1.10.5	Section 10
		Section Title SUPPORT AND TECHNICAL SERVICES	
Rescinds:		**Armando J. Perez, Chief of Police**	

This General Order is for departmental use only and does not apply in any criminal or civil proceeding. This General Order should not be construed as creation of a higher legal standard of safety or care in an evidentiary sense with respect to third party claims. Violations of this General Order will only form the basis for departmental administrative sanctions. Violations of law will form the basis for civil and criminal sanctions in a recognized judicial setting

I. PURPOSE:

The purpose of this general order is to establish a written directive that outlines the policies, procedures, and guidelines required by state and federal authorities to ensure the Bridgeport Police Department is in compliance concerning access and maintenance of CJIS, COLLECT and NCIC information systems.

II. POLICY:

The Bridgeport Police Department ("Department") will assure that all Department personnel access and maintain CJIS, COLLECT and NCIC information systems in a manner that meets all Bridgeport Police Department, state and federal guidelines. The Deputy Chief of Patrol is responsible for overseeing Department activities related to these criminal justice systems, and will designate Department personnel to act as the Department's Terminal Agency Control Officer (TAC) and the Local Agency Security Officer (LASO). The person(s) designated as the TAC and LASO shall report directly to the Deputy Chief of Patrol in carrying out their duties and responsibilities of those positions as outlined below.

This Department directive is meant to compliment the COLLECT and FBI-CJIS Security Policy and is not meant to provide less-stringent requirements than the FBI-CJIS Security Policy which is incorporated within this directive as Appendix. Violations of this directive may result in disciplinary action up to, and including, dismissal.

III. DEFINITIONS

CJI (Criminal Justice Information): Refers to all information disseminated by the State and Federal Criminal Justice Information Systems and COLLECT.

COLLECT (CONNECTICUT ON LINE LAW ENFORCEMENT TELECOMMUNICATIONS SYSTEM): The State of Connecticut's version of NCIC.

CSA ISO (CJIS System Agency Information Security Officer): Serves as the security point of contact (POC) to the FBI CJIS Division ISO.

Digital Media: Any form of electronic media designed to store data in a digital format. This includes, but is not limited to: memory device in laptops, computers, and mobile devices; and any removable, transportable electronic media, such as magnetic tape or disk, optical disk, flash drives, external hard drives, or digital memory card.

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.

Local Agency Security Officer (LASO): A security point of contact for local agencies that have access to criminal justice information.

NCIC (NATIONAL CRIME INFORMATION CENTER): A computer system controlled and operated by the Federal Bureau of Investigation in Washington DC, that gives law enforcement agencies access to information on warrants, criminal histories, stolen property, and missing persons statewide and nationwide.

Physical media: Physical Media refers to media in printed form. This definition includes, but is not limited to, printed documents, printed imagery, printed facsimile.

Terminal Agency Coordinator (TAC): The Point of Contact at an agency for matters relating to access to CT CJIS information. The TAC administers CJIS systems programs within the agency and oversees the agency's compliance with CJIS systems policies.

IV. PROCEDURE

A. Terminal Agency Coordinator (TAC) Duties and Responsibilities

1. The TAC is responsible for overseeing all Department activities related to the access and maintenance of CJIS, COLLECT and NCIC information in accordance with the CT-CJIS and FBI- CJIS manuals and the COLLECT manual.

2. The TAC will maintain contact with CJIS and COLLECT personnel to remain aware of changes to state and federal requirements, and will make recommendations for amendments to this directive in accordance with those changes.

3. Additional duties and responsibilities include, but are not limited to, the following:

    a. Complete the CJIS Security Compliance Certification Form in compliance with CJIS requirements;
    b. Complete all forms and reports required by COLLECT;
    c. Assure that agency employees receive training in compliance with this directive;
    d. Maintain a roster of authorized employees and make appropriate notifications when employees are terminated or transferred to a position that does not require access;
    e. Conduct background checks and provide security clearance for non-employees who are contracted to service equipment and assure they complete a non-disclosure agreement;
    f. Coordinate agency practices with the LASO to assure security of the system and system information; and
    g. Maintain validation procedures in accordance with these guidelines.
    h. Responsible for issuing all department radios to authorized employees (only) and maintaining an accurate updated list of each individual(s) with uniquely identified radio(s)
    i. Responsible for verifing annuel that each authorized employee issued a department radio has his or her assigned radio.
    j. Responsible for disconnecting any and all Bridgeport Police Department radios that are lost and or not accounted for after completing an inventory.
    k. Responsible for maintaining an accurate updated list of all department issued electronic devices, to include user, model, make and serial numbers

B. Duties and Responsibilities of the Local Agency Security Officer (LASO)

1. The LASO will coordinate his/her activities with the TAC to assure that all required security requirements are maintained and the TAC is made aware of any discovered security issues.

2. The LASO will conduct unannounced audits of inquiries and make written reports concerning the audit findings. In addition, triennial security audits, as required by state and federal guidelines will be conducted and reports filed with the TAC utilizing the forms provided by CJIS and COLLECT.

3. Other duties and responsibilities of the LASO include, but are not limited to, the following:

a. Identify individuals authorized to use the CJIS-approved hardware, software, and firmware, and ensure no unauthorized individuals or processes have access to the same.
b. Identify and document how the equipment is connected to CJIS systems;
c. Ensure that personnel security screening procedures are being followed as stated in this Policy;
d. Ensure the approved and appropriate security measures are in place and working as expected; and
e. Support policy compliance and ensure the TAC and CJIS ISO is promptly informed of security incidents.

C. Accessing CJIS/COLLECT Information on Personal or Public Devices

1. Department personnel may only access CJIS/COLLECT information on authorized Department computer terminals Department personnel are prohibited from accessing CJIS/COLLECT information on Personal cellular phones, tablets, computers, iPads and any other personally owned electonic devices. Doing so may result in disciplinary action.
2. Department E-Mails that contain any information as it relates to CJIS/COLLECT can ONLY be accessed from a Departmentissued/approved electronic device.

3. Department personnel will not utilize publicly accessible computers to access, process, store, or transmit CJI. Publicly accessible computers include, but are not limited to: hotel business center computers, convention center computers, public library computers, public kiosk computers, etc.

4. This section does not apply to employees accessing information on personally-owned or public devices that is available to the general public.

D. Protection of CJIS/COLLECT Media

[redacted]

3. Dissemination of CJI to another agency is authorized if the other agency is an Authorized Recipient of such information and is being serviced by the accessing agency, or the other agency is performing personnel and appointment functions for criminal justice employment applicants.

4. Department personnel shall protect and control electronic and physical media during transport outside of controlled areas and restrict the pickup, receipt, transfer and delivery of such media to only authorized personnel.

5. If CJI is mailed or shipped, the agency must document procedures and only release to authorized individuals. The sending agency will not mark the package confidential. Packages containing CJI material are to be sent by method(s) that provide for complete shipment tracking and history, and signature confirmation of delivery.

6. Department personnel will not take CJI home, or when traveling, unless authorized by the LASO. When disposing of CJI documents, such documents will be shredded.

E. Physical Protection of CJI and Hardware

[redacted]

[redacted]

[redacted]

4. The LASO or TAC will maintain a list of authorized Department personnel who have have access to physically secure non-public locations. The agency will implement access controls and monitor physically secure areas for the protection of all CJI transmissions and display mediums. Authorized personnel will take necessary steps to prevent and protect the agency from physical, logical and electronic breaches.

5. All personnel with CJI physical and logical access must meet the minimum personnel screening requirements prior to CJI access. These requirements include the following:

[redacted]

6. Personnel shall properly protect and not share any individually issued keys, proximity cards, computer account passwords, etc., and shall report loss of issued keys, proximity cards, etc. to authorized agency personnel. If the loss occurs after normal business hours, or on weekends or holidays, personnel are to call the LASO or TAC to have authorized credentials, like a proximity card, de-activated and/or door locks possibly rekeyed.

7. Personnel will safeguard and not share passwords, Personal Identification Numbers (PIN), Security Tokens (i.e. Smartcard), and all other facility and computer systems security access procedures. Personnel will protect from viruses, worms, Trojan horses, and other malicious code and not access Internet sites on computers that access CJI.

8. Personnel will report any physical security incidents to the LASO to include facility access violations, loss of CJI, loss of laptops, cell phones, thumb drives, CDs/DVDs and printouts containing CJI.

9. All properly vetted IT staff assigned to support CJI-associated systems will protect CJI from compromise by performing the following:

[redacted]

11. The LASO will assure that the following actions are completed:

    a. Conduct appropriate data backups and take appropriate measures to protect all stored CJI.
    b. Ensure only authorized vetted personnel transport off-site tape backups or any other media that store CJI that is removed from physically secured location.
    c. Perform timely application of system patches (part of configuration management);
    d. Identify applications, services, and information systems containing software or components affected by recently announced software flaws and potential vulnerabilities resulting from those flaws.

12. The LASO shall establish Access Control measures that include the following:

    a. Address least privilege and separation of duties;
    b. Enable event logging of:
        1) Successful and unsuccessful system log-on attempts;
        2) Successful and unsuccessful attempts to access, create, write, delete or 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 access, modify, or destroy the audit log file.
    c. Prevent authorized users from utilizing publicly accessible computers to access, process, store, or transmit CJI. Publicly accessible computers include, but are not limited to: hotel business center computers,

convention center computers, public library computers, public kiosk computers, etc.

13. The LASO shall maintain an Account Management program in coordination with the TAC, to include the following:

    a. Ensure that all user IDs belong to currently authorized users;
    b. Keep login access current, updated and monitored. Remove or disable terminated or transferred or associated accounts;
    c. Authenticate verified users as uniquely identified;
    d. Prevent multiple concurrent active sessions for one user identification, for those applications accessing CJI, unless the agency grants authority based upon operational business needs;
    e. Not use shared generic or default administrative user accounts or passwords for any device used with CJI.

14. The LASO shall maintain a list of Passwords for all authorized users. Passwords will include the following standards:

    [redacted]

15. The LASO will maintain Network Infrastructure protection measures that include the following:

    a. Take action to protect CJI-related data from unauthorized public access;
    b. Control access, monitor, enabling and updating configurations of boundary protection firewalls;
    c. Enable and update personal firewall on mobile devices, as needed;
    d. Ensure confidential electronic data is only transmitted on secure network channels using encryption and advanced authentication when leaving a physically secure location. No confidential data should be transmitted in clear text;
    e. Ensure any media that is removed from a physically secured location is encrypted in transit by a person or network;
    f. Not use default accounts on network equipment that passes CJI like switches, routers, firewalls;
    g. Make sure law enforcement networks with CJI shall be on their own network, accessible by authorized personnel who have been properly vetted;
    h. Utilize Virtual Local Area Network (VLAN) technology to segment CJI traffic from other noncriminal justice agency traffic to include other city and/or county agencies using same wide area network; and
    h. Communicate and keep agency personnel informed of all scheduled and unscheduled network and computer downtimes, all security incidents and misuse. The ultimate information technology management control belongs to the Bridgeport Police Department.

F. Electronic Media Sanitization and Disposal

[redacted]

G. Breach Notification and Incident Reporting:

[redacted]

H. Misuse and Unauthorized Use of CJI Systems

1. Misuse of computing, networking or information resources may result in temporary or permanent restriction of computing privileges up to employment termination. In some misuse situations, account privileges will be suspended to prevent ongoing misuse while under investigation. Additionally, misuse can be prosecuted under applicable statutes. All files are subject to search. Where follow-up actions against a person or agency after an information security incident involves legal action (either civil or criminal), the evidence shall be collected, retained, and presented to conform to the rules of evidence laid down in the relevant jurisdiction(s). Complaints alleging misuse of Department computing and network resources and CJI systems and/or data will be directed to the TAC or Deputy Chief of Patrol for appropriate disciplinary action.

2. The following are examples of misuse or unauthorized conduct:

    a. Using someone else's login that you are not the owner;
    b. Leaving computer logged in with your login credentials unlocked in a physically unsecure location, allowing anyone to access agency systems and/or CJI systems and data in your name;
    c. Allowing an unauthorized person to access CJI at any time for any reason;
    d. Allowing remote access of issued computer equipment to CJI systems and/or data without prior authorization by the LASO;
    e. Obtaining a computer account that you are not authorized to use;
    f. Obtaining a password for a computer account of another account owner;
    g. Using the agency network to gain unauthorized access to CJI.
    h. Knowingly performing an act that interferes with the normal operation of CJI systems.

i. Knowingly propagating a computer virus, Trojan horse, worm and malware to circumvent data protection, or compromising existing security holes to CJI systems;
j. Violating terms of software and/or operating system licensing agreements or copyright laws;
k. Duplicating licensed software, except for backup and archival purposes, that circumvent copyright laws for use in agency systems, for home use or for any customer or contractor;
l. Deliberately wasting computing resources to include streaming audio, videos for personal use that interferes with network performance;
m. Using electronic mail or instant messaging to harass others;
n. Masking the identity of an account or machine;
o. Posting materials publicly that violate existing laws or the agency's codes of conduct;
p. Attempting to monitor or tamper with another user's electronic mail or files by reading, copying, changing, or deleting without explicit agreement of the owner;
q. Using Department technology resources to advance unwelcome solicitation of a personal or sexual relationship while on duty or through the use of official capacity;
r. Unauthorized possession of, loss of, or damage to the agency's technology equipment with access to CJI through unreasonable carelessness or maliciousness;
s. Maintaining CJI or duplicate copies of official files in either manual or electronic formats at his or her place of residence or in other physically non-secure locations without express permission.
t. Using agency technology resources and/or CJI systems for personal or financial gain.
u. Deliberately failing to report promptly any known technology-related misuse by another employee that may result in criminal prosecution or discipline under this policy;
v. Using personally owned devices on the Department network to include personally-owned thumb drives, CDs, mobile devices, tablets on wifi, etc. Personally owned devices should not store Department or CJI data.

3. The above listing is not all-inclusive, and any suspected technology resource or CJI system or CJI misuse will be handled by the TAC or Deputy Chief of Patrol on a case by case basis. Activities will not be considered misuse when authorized by the LASO or TAC for security or performance testing.

I. CJIS Media Protection

[redacted]