	Bridgeport Police Department POLICY AND PROCEDURE GENERAL ORDER	Distribution ALL PERSONNEL	General Order Number **10.13**
		Original Issue Date 7/16/19	Reissue/Effective Date 7/16/19
Order Title: **Security of the Communications Center**		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. POLICY & PURPOSE

The purpose of this policy is to establish rules and procedures for security measures and authorized access to the entire Bridgeport Police Department Communications Center area.

II. DEFINITIONS

Communications Center: The area of the Emergency Operations Center (EOC) building that encompasses the public safety telecommunications function, to include E9-1-1 intake, police and fire dispatch and data teletype operations of the Bridgeport Police Department.

Controlled Area: An area, a room, or a storage container, for the purpose of day-to-day CJI access and storage, that with limited access during CJI processing times to only those personnel authorized to access or view CJI, or that is locked when attended.

Criminal Justice Information: Includes all FBI CJIS provided data necessary for law enforcement to perform its mission including, but not limited to biometric, identity history, biographic, property and case/incident history data.

1. Biometric data is 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 is textual data that corresponds with an individual's biometric data, providing history of criminal and/or civil events for the identified individual.

3. Biographic data is 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 is information about vehicles and property associated with crime.
5. Case/incident history information about the history of criminal incidents.

Physically Secure Location: A facility or an area, a room, or a group of rooms, within a facility with both physical and personnel security controls sufficient to protect CJI and associated information systems.

III. PROCEDURES

A. Access to the Department Communications Center / Security Measures – Generally

[redacted]

4. For the purpose of this policy, communications equipment shall mean: radio transmit/receive components, antennae, telephone switching and recording equipment, computer mainframe systems, and any other equipment that may be added or changed for the improvement and operation of the communications system. Furthermore, for the purposes of this policy, the phrase communications equipment encompasses both the primary and back-up communications resources.

B. Designation of Physically Secure Locations

1. The Department Communications Center and Computer Information Services are designated as a "Physically Secure Location "in compliance with Bridgeport Police Department policy and the Federal Bureau of Investigation's Criminal Justice Information Services (CJIS) Security Policy (CSP).

2. Designation as a "Physically Secure Location" with restricted access is due to the sensitive nature of access to CJI and the critical infrastructure of telecommunications equipment and systems, to include services and routers in the CIS area.

3. The administrative area outside of the actual Department's Communications Center is designated as a controlled area.

[redacted]

[redacted]

[redacted]

C. Access to Department Communications Center Limited to Authorized Personnel

[redacted]

[redacted]

D. Background Checks

1. All employees who will have unescorted or unrestricted access (either physically or logical access) to the Department Communications Center are, and specifically CJIS systems, must be fingerprinted and a background check completed prior to employment or assignment. The results of all background investigations will be maintained by the Chief of Police or designee.

2. All other personnel, including maintenance workers and repair personnel, must be fingerprinted and a background check completed prior to being authorized for unescorted or unrestricted access to the Department Communications Center area.

E. Annual Review of Individuals Authorized for Unescorted Access

1. On an annual basis, the Communications Supervisor shall review the list of all persons with access to the Department Communications Center to ensure each has proper background checks and an appropriate level of security awareness training for their level of access.

2. Appropriate action per Department or Department Communications Center directive will be taken immediately for any authorized person found with unescorted access in the Department Communications Center.

F. Visitor Control to the Department Communications Center

1. All visitors to the Department Communications Center, defined as any person who is not properly authorized to have unescorted access to the physically secure location, shall be authenticated by the Department Communications Center employee permitting access to the location.

2. All visitors shall be escorted by a Department Communications Center employee at all times and have the visitor's activity monitored.

G. Access Control for Display Medium

1. All physical access to information system devices that display CJI(e.g. computer monitors) shall be arranged and positions such that visitors within or viewing into the physically secure location within the Department Communications Center cannot access or view CJI.

[redacted]

[redacted]