


ELIZABETH POLICE DEPARTMENT GENERAL ORDERS			
VOLUME: 5	CHAPTER: 17	# OF PAGES: 10	
SUBJECT: COMMUNICATIONS CENTER READINESS			
EFFECTIVE DATE: March 1, 2023		ACCREDITATION STANDARDS: 1.6.3 (NJCOMS)	
BY THE ORDER OF: Chief Giacomo Sacca			
BY AUTHORITY OF: Police Director Earl J. Graves			
SUPERSEDES ORDER #:			

PURPOSE: The purpose of this policy is to outline information and identify procedures required for the effective management of the Communications Center so that it remains in a state of operational readiness at all times.

POLICY: It is the policy of the Elizabeth Police Department to maintain our Communications Center in a state of operational readiness so that we may best serve the needs of our residents, businesses, and community visitors during both routine and emergency calls for service.

PROCEDURES:

I. Management of the Communications Center

- A. The Chief of Police shall assign a commander to be in charge of the communications function (Communications Commander) for the department.
- B. The Communications Commander shall be responsible for this policy.
 - 1. Annual Review: they will review the policy annually to ensure it is current and that no modifications need to be made.
 - 2. Monthly Inspection: they will be responsible for a monthly in-person inspection of the Communications Center as outlined and required by this policy. The monthly inspection shall be documented and submitted through the chain of command to the Chief of Police.
 - 3. Concurrent Responsibility: the Communications Commander's need to remedy shortcomings discovered during the monthly inspection or during the course of their duties and responsibilities of maintaining the Communications Center's operational readiness shall supersede an equally ranked officer's authority.
- C. The Communications Commander shall, without pause, bring to the Chief of Police's attention any identified shortcoming that has a strong likelihood of being a significant liability to the department.
- D. The Communications Commander may, with the input and authorization of the Chief of Police, assign a supervisor or supervisors to assist with the Communications Center's management responsibilities.

II. Operational Readiness Areas

- A. Maintaining a Communications Center's operational readiness entails managing personnel, equipment, training, collaboration, and certifications across many functions within and outside the department. Outlined below are critical elements of operational readiness that the Communications Commander must manage continually.
 - 1. Communications Personnel
 - a. **Staffing**: the Communications Center shall be appropriately staffed so that communications personnel can adequately respond to anticipated call levels, foreseeable emergencies, and planned events.
 - b. **Training**: Communications Center personnel (sworn and civilian) who operate a communications console shall be appropriately trained and certified for that function in whatever capacity they serve. Allowing an employee to become uncertified exposes the department to significant liability. Additionally, the employee is not educated or trained in essential updates required to perform their

duties. Therefore, the Communications Commander shall see to it that the following at a minimum is completed and documented correctly in department training records:

- 1). Basic Telecommunicator Course
 - a). This training requirement is set forth by the New Jersey Office of Emergency Telecommunications Services.
 - b). New personnel: all new personnel who are required to be certified due to their assignment to the Communications Center shall be trained and certified as a Basic Telecommunicator before being authorized to act as a call taker or answering a Public Safety Answering Point (PSAP).
 - c). In-service training: the Basic Telecommunicator certification requires 24 hours of continuing education for each three (3) year period from the date issued. Copies of these classes shall be retained with the original certification and made available to the New Jersey Office of Emergency Telecommunications Services upon request or inspection.
- 2). Emergency Medical Dispatch Course (EMD)
 - a). This training requirement is set forth by the New Jersey Office of Emergency Telecommunications Services.
 - b). New personnel: each employee providing Emergency Medical Dispatch services will successfully complete an Emergency Medical Dispatch Course and have a current CPR certification approved by the State of New Jersey Department of Health and the New Jersey Office of Emergency Telecommunications Services.
 - c). In-service training: once obtained, an Emergency Medical Dispatch certification requires a minimum of 24 hours of continuing education (medical in nature) every three (3) years from the date of certification.
- 3). TTY/TDD Operations (Deaf and Hard of Hearing)
 - a). American with Disabilities Act (ADA) regulation requires 9-1-1 and other telephone emergency service providers to provide TTY/TDD users with direct access and an opportunity to benefit from the emergency services that are equal to the opportunity

afforded to others. Many of the citizens protected by ADA communicate via texting and expect to do the same with a PSCC or PSAP.

- b). This training requirement is set forth by the [Association of Public Safety Communications Officials](#) (APCO) and the [National Emergency Number Association](#) (NENA) through APCO/NENA ANS 1.108.1 ([Minimum Training Standard for TDD/TTY Use in the Public Safety Communications Center](#) - 2018).
- c). New Personnel: each new telecommunications employee shall receive training compliant with 3.105 (Required Training 2.1.1 through 2.1.2).
- d). In-Service and Ongoing Training:
 - 1). As technologies continue to evolve in the emergency communications arena, emergency communications professionals must take steps to ensure that their organizations keep up with those advancements. Below you will find recommendations as they relate to the continuing education component of this topic.
 - 2). The department shall make TTY/TDD refresher training available to any personnel who have contact with individuals from the public who are deaf, deaf-blind, hard of hearing, or people who have a speech disability. This training shall occur as often as training for voice calls but at a minimum, every six months (Required Ongoing Training 2.1.3 through 2.1.4)
- 4). CJIS Training Security Awareness Training
 - a). This training requirement is set forth by the FBI CJIS Division through the [CJIS Security Policy](#) (5.2.1).
 - b). Security Awareness Training **shall be** required within six months of initial assignment and biennially after that.
 - c). New personnel: the Terminal Agency Coordinator (TAC) shall appropriately train all new Communications Center personnel so that they can legally access the Criminal Justice Information System.

- d). In-service training: the Terminal Agency Coordinator (TAC) shall appropriately refresh all Communications Center personnel to maintain their legal access rights to the Criminal Justice Information System.
 - 5). Handling the Mentally Ill Training
 - a). This training requirement is set forth by the New Jersey State Association of Chiefs of Police Law Enforcement Accreditation Program.
 - b). New personnel: communications personnel (sworn and civilian) shall receive training in the department's policy pertaining to Handling the Mentally Ill.
 - c). In-service training: at least triennially (every three years), communications personnel (sworn and civilian) shall receive refresher training in the department's policy pertaining to Handling the Mentally Ill.
 - c. **Critical Incident Stress Debriefing**: the health and welfare of Communications Center personnel (sworn and civilian) are a vital component of how they will respond in times of stress and extreme pressure. It is critical that personnel receive Critical Incident Stress Debriefing following any seriously traumatic incident.
 - 1). Debriefing is a specific technique designed to assist others in dealing with the physical or psychological symptoms that are generally associated with trauma exposure.
 - 2). Critical Incident Stress Debriefing should take place as soon as possible but typically no longer than the first 24 to 72 hours after the initial impact of the incident.
 - 3). Depending upon the seriousness, duration, and impact a critical incident had on an employee, the Chief of Police should consider the use of administrative time, the employee assistance program, and the municipality's workers' compensation insurance to assist any employee experiencing difficulty in returning to work following a traumatic event that they participated.
2. Fire Detection and Suppression Systems
- a. All employees are tasked with the safety of the Communications Center.
 - 1). **Fire Detection Instruments**: fire detection equipment (e.g., ionization/photoelectric, photoelectric, ionization, and heat) is essential for the quick detection of fire emergencies within the Communications Center. Communications personnel

should report any instrument malfunction to the Communications Commander and the Shift Supervisor as soon as possible. If the instrument's light does not flash as taught in training, it shall be deemed malfunctioning.

- 2). **Fire Suppression Equipment:** fire suppression equipment (e.g., fire extinguishers, overhead water sprinklers, clean agent fire suppression systems, etc.) are critical tools to extinguish a fire emergency when detected before it grows. Communications personnel should report any outdated certificate they find affixed to any fire suppression equipment to the Communications Commander via email.

- b. Annually, the municipal fire official shall conduct an inspection of the entire facility, including the Communications Center, and issue a certificate of inspection. The certificate shall be displayed in an area observable to all employees of the department.

3. Environmental Systems

- a. Equipment located in the Communications Center produces large amounts of thermal heat. It is critical that the center's environmental HVAC system is operating correctly in order to cool the room and the equipment.
- b. If at any time the Communications Center's HVAC system fails, it shall be considered an emergency. The Communications Commander and the Shift Supervisor shall be contacted immediately. If they are not available, the commander's supervisor shall be contacted.

4. Standby Generator and Uninterruptible Power Source Devices (UPS)

- a. Standby Generator: the Communications Center is equipped with a commercial standby generator that produces enough power to energize all the equipment in the Communications Center in the event of power failure from the commercial electrical grid.

- 1). The Communications Commander shall make sure the standby generator is tested in conformance with the Communications policy.
 - 2). The standby generator shall be tested at full load at least annually.

If the Communications Center loses power, it shall be documented in an email to the Communications Commander. The power failure may count as a full load test as long as it is documented that the Communications Center was adequately supplied with power during the outage.

- b. Uninterruptible Power Source Devices: certain Communications Center equipment is connected to UPS devices to maintain their operational ability between the time of power cut until the standby generator kicks in and takes over the load.
 - 1). Backup UPS devices are maintained by this department in case of failure of a primary device.
 - 2). Communications Center personnel shall check the status of any UPS devices connected to their equipment at the start of their shift based on their training. If any UPS device is found to be malfunctioning, a backup UPS device shall be installed by them, or someone else, as soon as possible.
 - c. Emergency Lighting: the Communications Center is equipped with emergency lighting in the event of power failure. If emergency lighting does not activate during a power failure, communications personnel shall notify the Communications Commander and the Shift Supervisor as soon as possible.
5. Communications Center Security
- a. Surveillance Systems: the Communications Center and police building are equipped with a surveillance system. Suppose at any time Communications Center personnel discover a failure in the system (i.e., camera not working, display screen not working, etc.). In that case, they shall notify the Communications Commander via email and the Shift Supervisor right away.
 - b. Physical Security: the Communications Center and police building are equipped with physical security devices (e.g., locks, access control devices, intercoms, fences, etc.) Suppose at any time Communications Center personnel discover a failure of a physical security device (i.e., access control device not working). In that case, they shall notify the Communications Commander via email and the Shift Supervisor right away.
6. Computers, Networks, and Network Access
- a. The employee responsible for performing the functions of a Network Administrator shall at least quarterly conduct an inventory of all servers, endpoints (computers), devices, and all other electronic equipment necessary for the communication center's normal and backup operations. The purpose of this inventory is to identify inoperable equipment and equipment that is reaching the end of its life span so that it can be replaced before failure.
 - b. The Communications Center network (inter/intranet) shall be protected by a Layered Defense System (LDS) at all times to protect it from unauthorized access, which could lead to data theft, data manipulation, or operational systems failure.

- 1). A Layered Defense System is a form of cybersecurity for securing military and government computer systems against malicious cyber-attacks. A layered defense system has seven (7) components:
 - a). Physical: the department's data shall be stored in a secure IT room. When the room is unoccupied, it will be locked. No unauthorized personnel shall be allowed to enter the IT room.
 - b). Network: the department shall use only enterprise-grade hardware, advanced firewall configuration, SSL VPN security, and intrusion detection and prevention. The department shall maintain a vendor capable of threat management response.
 - c). Applications: the department shall employ data encryption (at rest and in transit), antivirus protection, timely patching and updating of software and firmware, two-factor authentication, malware protection, and log management.
 - d). Servers: the department shall employ file integrity monitoring, updating software and firmware, and role-based access controls.
 - e). Data: the department shall employ data backup, at-rest and in-transit encryption, retention/destruction/archiving management, and lifecycle management.
 - f). Devices: all devices connected to the network shall be protected in the same manner as traditional endpoints. Additionally, devices shall have the capability of being managed remotely by the network administrator or their designee. This management shall include the requirement that the device contains routine access control and wipe capabilities if lost.
 - g). User: the department shall use two-factor authentication for access to the Communications Center servers. Employees shall receive training at least annually that addresses safety and security protocols relative to cybersecurity.

7. Communication with Deaf or Hearing Impaired People (TTY/TDD)

- a. Communications personnel shall test the equipment used to communicate with deaf or hearing impaired people at the beginning of their shift to ensure it is operational.

8. Methods of Communication

- a. Communications personnel shall monitor all communication methods on a continual basis so that a disruption can be identified as soon as possible.
 - b. Methods of communication include but are not limited to the following:
 - 1). Base station radios
 - 2). Inbound Communications Center telephone lines
 - 3). The Internet
 - 4). Fax machine
 - 5). Public Safety Answering Point (PSAP)
 - 6). Intercom system
 - 7). Interagency computer networks
 - c. Communications personnel shall notify the Shift Supervisor of any failure in a communication method as soon as a hazard is identified. If the Shift Supervisor cannot remedy the failure, they shall contact the Communications Commander right away.
9. Records Stored in Communications
- a. Any records stored within the Communications Center that contain either Criminal Justice Information (CJI) or Personally Identifiable Information (PII) shall be secured so that no one without Security Awareness Training can view them.

III. Operational Readiness Exercise and Debriefings

- A. Tabletop Exercise: at least once every three (3) years, the Communications Center with select personnel shall participate in a tabletop exercise that involves a mass casualty incident. The tabletop exercise shall be documented in a report by the Communications Commander in writing. The report shall contain the following at a minimum:
 - 1. The date and duration of the tabletop exercise,
 - 2. Who participated in the tabletop exercise,
 - 3. The type of mass casualty incident (appropriate to our jurisdiction),
 - 4. Any strengths or weaknesses identified during the tabletop exercise,
 - 5. Any need for training modification identified,

6. Any need for policy modification identified, and
 7. Any other information the Communications Commander deems essential or appropriate.
- B. Critical Incident Debriefing: any time the Communications Center experiences a critical incident of a significant nature (as defined by the Communications Commander), there shall be a communications personnel's debriefing by the Communications Commander. The purpose of this debriefing is to identify weaknesses in any system, need for additional training or modification of existing training, policy modification, etc.

IV. Monthly Readiness Inspection

- A. On a monthly basis, the Communications Commander or their designee shall conduct an unannounced readiness inspection of the Communications Center.
- B. The inspection shall focus on the areas identified in Section II of this policy.
- C. The Communications Commander is not required to check every area in its entirety during each monthly inspection. For example, the Communications Commander may opt to audit the records of a certain number of communications personnel for adherence to training requirements.
- D. The Communications Commander shall document their findings in a report to the Chief of Police for visibility (transparency) and action, if necessary.
- E. The Communications Commander is authorized to create and modify a form, in place of a report, as the monthly reporting mechanism.