



Fitchburg State University Police Department

Subject: COMMUNICATION CENTER SECURITY	
Reference: MPAC: 81.3.1 IACLEA: N/A	
Effective Date: June 30, 2019	Review Date:
By Order of: Michael J Cloutier, Chief of Police	

General Order

11.3.3

PURPOSE:

To comply with the Massachusetts Department of Criminal Justice Information Services requirement of safe and secure communication center and control of criminal justice information (CJI) and information system hardware, software, and media.

POLICY:

Fitchburg State University Police Department will ensure that criminal justice information (CJI) and information system hardware, software, and media are physically protected through access control measures within its communication center.

PROCEDURE:

A. Physical Space

1. No unauthorized personnel are allowed in the Communication Center. All doors leading to the Dispatch Center shall be kept locked or closed at all times. Only those personnel working in the Communication Center, and the OIC, a Sergeant or Lieutenant, or those authorized by the Chief or designee are allowed entry. Employees should use the telephone or radio to obtain needed information from the Dispatcher.
 - a. All authorized members of the department will be given access through use of their employee ID (OneCard) to enter the communication center.
 - b. Authorized members will be designated by the Chief or designee.
2. Off-duty Dispatch personnel and other department personnel shall not congregate in the Communication Center.

Chapter 11-Communciations and Dispatch Services

3. The Chief or designee may authorize tours of the Communication Center at appropriate times, and with advance notice to the OIC.
4. Any member of the Fitchburg State University's Technology, Capital Planning and Maintenance, or contractor having legitimate business will be accompanied by a dispatcher or member of the police department while in an area where CJI terminals are present. These terminals are located in the communication center, cruisers, and command staff work stations.
5. All hardware and Transmission lines will be kept secure in the lower level of the station in the communication closet, where only authorized members will have access. An officer shall escort any individual needing access to the communication closet. When not being serviced, the communication closet shall be locked at all times.

B. CJI Terminals

1. Fitchburg State University Police are authorized to have CJI Terminals in the following areas:
 - a. Communication Center
 - b. Cruisers
 - c. Administrative Offices
 - i. Sergeants' Office
 - ii. Lieutenants' Office
2. All Access and usage of CJI Terminals will comply with Fitchburg State University Police's General Order 11.3.1 and 11.3.2.
3. When station terminals are not in use screens should automatically enter screen saver mode, or be logged off.
4. Cruiser's mobile data terminals that have access through CAD shall be placed in the close position with the laptop screen down when not in use or when an officer is not in the cruiser.
5. At no time will the screen of a CJI terminal be photographed, screen shot, or captured outside the applicable use of the department.
6. CJI terminals within the communication center will not be visible or made visible to any non-CJI certified individual.

C. CJIS Strong Password Policy

1. In keeping with the FBI CJIS Security Policy and industry best practices, access to any CJIS application requires the use of a strong password.
2. Strong passwords must meet the following requirements:
 - a. Contain a minimum of eight (8) characters
 - b. Contain at least one number AND at least one of the following symbols: ~!@#\$\$%^&*()-_
 - c. Be different from the last 10 passwords used

Chapter 11-Communciations and Dispatch Services

- d. Cannot contain your user name, a proper name, or a dictionary word.
 3. Each CJIS user is required to change his/her password every 90 days, and each new password must meet the strong password requirements listed above.
 4. The following security-related requirements have also been implemented in the CJIS environment:
 5. Five (5) invalid logon attempts will result in the lockout of the user's account. The user will need to contact the Public Safety Data Center at 617-660-4620 to get his/her account unlocked and, if necessary, to get his/her password reset.
 6. A user will be automatically logged out of all CJIS applications after 30 minutes of inactivity. The thirty minute log out does not apply to permanently mounted devices in police vehicles or to CJIS workstations used specifically for dispatch functions. However, it does apply to all other devices, such as terminals in detective units and mobile devices not permanently attached to police vehicles.
 7. These requirements will ensure the security and integrity of all CJIS and FBI systems and the information they contain.
 8. Access to LAN via IMC's CAD system will adhere to the same strong password requirements.
 9. Employees locked out of IMC due to invalid logon attempts should contact the Administrative Lieutenant for password reset.
- D. Fingerprinting Requirements for CJIS Agencies**
1. The CJIS User Agreement and the FBI CJIS Security Policy require each CJIS agency to conduct fingerprint-based criminal record checks on **all personnel** prior to hire and **at least once every two years thereafter**.
 2. In addition, agencies must conduct fingerprint-based criminal record checks on all other individuals who have unescorted access to secure (non-public) areas of the agency prior to allowing access. These individuals include University IT personnel, contractors, vendors, custodians, and volunteers.
 3. These background check requests are submitted either as criminal justice employment checks (for all employees of the department) or as criminal justice checks (all non-employees).
 - a. Important: with regard to fingerprint-based background checks conducted on non-department personnel, no information received in response to a fingerprint-based check may be disseminated to the individual's actual employer.
 4. If a felony conviction of any kind exists, an employee is not to be allowed access to the CJIS or to any information derived from the CJIS, and the Department is required to notify the DCJIS, in writing, as soon as practical. In the case of a non-employee, the agency must deny unescorted access to the individual.


Chapter 11-Communciations and Dispatch Services

5. If a misdemeanor conviction exists, the Department must notify the DCJIS and must request a waiver before the employee is allowed to access the CJIS or CJI, or before the non-employee is provided unescorted access to secure areas.
 6. A part of their respective auditing programs, both the DCJIS and the FBI will check to ensure that the appropriate fingerprint-based background checks have been completed by the agency being audited. An agency which has not conducted these fingerprint-based checks as required will be found out-of-compliance in this area.
- E. **Supervision and Monitoring**
1. It is incumbent all department members to comply with all CJI related policies, and report any infraction up the chain of command.
 2. Any non-Fitchburg State University Police Department members needing access to the Communication Center or the Communication Closet shall provide their name and date of birth and information shall be entered into CAD as a call for service providing reason for access the area.
 3. No CJI information shall leave the communication center unless it is to be used for lawful purposes or immediately shredded.
 4. All CJI information that is disseminated within the department shall be kept with the related case folder and secure at all time.

Approvals:



Chief of Police



Date