

Medina Police Department

Subject: CJDN Security Policy	Policy Number: 4300		CJDN Security Policy
Reference: CJDN/BCA Policies	Pages: 2		
Personnel: Sworn and Non-Sworn Personnel			
Issue Date: 12-14-2016	Revised Date: 11-17-2020	Review Date: As Needed	

4300 - PURPOSE

This document shall be considered the official CJDN Security Policy for the Medina Police Department regarding the physical and personnel security of the CJDN system. All staff must follow the policies contained herein. This will assure proper usage of the system and adherence to all local, state, and federal regulations that govern the use of the MNJIS computer system. The TAC manages the operation of the CJDN terminal on a local agency level and is responsible for ensuring that all state and local policies are enforced regarding the use of the CJDN terminal.

4300.1 – ACCESS TO CJDN SYSTEM

Access to the CJDN shall be limited to employees who have been certified by the BCA to operate the terminal. Currently, at Medina Police Department, this is limited to TAC, Investigator, and other sworn and/or non-sworn personnel who have completed training and certified as CJDN operators. All other personnel of the Medina Police Department must make their Criminal Justice inquiries through their CJDN operators.

Staff having access to the CJDN system must meet the follow requirements:

- 1) Be an employee of Medina Police Department.
- 2) Successfully pass a State and National fingerprint background check.
- 3) Be trained and certified within six months of hire and biennially thereafter.
- 4) Complete Basic Security Awareness Training within six months of hire or assignment and biennially thereafter.

New employees of the Medina Police Department shall be fingerprinted within 30 days of employment or assignment and the fingerprint cards shall be sent to the BCA for a background check.

A potential new employee of the Medina Police Department shall have a background check completed before they are hired. When running the criminal history on that person, the Purpose Code of “J” shall be used.

The FBI fingerprint-based background check results letters on CJDN operators, appropriate IT personnel, and other agency personnel having unescorted access to the terminals are to be kept on file and available upon request during an audit.

The TAC will issue a unique username and password to authorized users with access to the CJDN and Portal 100. Authorized users will be given a unique password to have access to criminal histories. That Criminal History Password will be changed by the TAC at least every 2 years. A list of these assigned passwords shall be kept by the TAC in a locked cabinet.

4300.2 – TRAINING OF NON-CERTIFIED CJDN USERS

NCIC requires that all sworn personnel must receive basic, formal MNJIS/NCIC training within the first 12 months of hire, and bi-annual refreshers thereafter. All training will be documented.

The Medina Police Department will meet this requirement by having all employees, including officers, reserves, community service officers and other non-certified CJDN users view the BCA's Mobile Access Training (MDT/MDC). The training is fifteen minutes long and will be viewed bi-annually. Users will successfully pass the Mobile Access Certification.

4300.3 – SECURITY OF TERMINAL

The CJDN terminals and Criminal Justice Information for the Medina Police Department are maintained in a secure area. Only authorized personnel who have passed a State and National fingerprint background check are allowed unescorted access to the secure areas.

All personnel who have direct responsibility to configure and maintain computer systems and networks with direct access to FBI CJIS systems must successfully pass a fingerprint-based background check.

Criminal History responses, as well as all other CJDN printouts, will be destroyed when no longer needed. These documents will be placed in the secure shredder box provided by Randy's Sanitation and shredded on site at the Medina Police Department on a monthly basis.

4300.4 – OCCASION UNESCORTED ACCESS

Those who have infrequent access for job duty that requires access to a physically secure area where CJI is located will sign the Occasional Unescorted Access Security Agreement. This will include, but not limited to those who repair utilities, vehicle maintenance personnel, those contracted for shredding, etc. This agreement will be kept on file with the TAC and remain in effect for two years.