CJDN Security Policy and Discipline for Misuse of the CJDN

808.1 PURPOSE AND SCOPE

This policy shall be considered the official CJDN (Criminal Justice Data Network) Security Policy for the Columbia Heights Police Department regarding the physical and personnel security of the CJDN system. It also addresses discipline for misuse 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 Terminal Agency Coordinator (TAC) for the Columbia Heights Police Department is the Police Office Supervisor or his/her designee. 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.

808.2 ACCESS TO CJDN SYSTEM

808.2.1 DEFINITION OF CJDN

CJDN – The Criminal Justice Data Communications Network is the overall system which provides criminal justice agencies computer access to data stored on state and national systems.

808.2.2 ACCESS TO CJDN

Access to the CJDN shall be limited to employees who have been certified by the BCA to operate the terminal. Currently, at the Columbia Heights Police Department, this is limited to Support Services personnel.All other personnel of the Columbia Heights Police Department must make their Criminal Justice inquiries through their CJDN operators.

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

(a) a.Be an employee of Columbia Heights Police Department.

(b) b. Successfully pass a State and National fingerprint background check.

(c) c. Be trained and certified within six months of hire and biennially thereafter.

(d) d.Complete Basic Security Awareness Training within six months of hire or assignment and biennially thereafter.

808.2.3 NEW EMPLOYEES

Per the FBI CJIS Security Policy (5.7) any employee or contractor needs to complete the BCA screening requirements prior to having any CJI access, to include access to physically secured areas.

A potential new employee of the Columbia Heights 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.

808.2.4 FINGERPRINT CARDS
Fingerprint cards on CJDN operators are to be kept in a locked drawer by the Office Supervisor.

808.2.5 PASSWORDS
The TAC will issue a unique username and password to authorized users with access to the CJDN and PS Portal. 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.

808.2.6 MULTIPLE LOG-INS
Employees shall only be logged into one terminal at a time. Once the employee has completed their work on a computer they must log off of their current work station before attempting to access another.

Employees must have a valid business need for multiple computer logins at any given time.

808.3 TRAINING OF SWORN OFFICERS

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

808.3.2 ONGOING TRAINING
The Columbia Heights Police Department will meet this requirement by having all officers complete the BCA's recorded training for MDT/MDC officers. The training will be viewed annually by sworn personnel. The department's TAC will facilitate this annual training.

808.4 SECURITY TERMINAL
The CJDN terminals and Criminal Justice Information for Columbia Heights 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 area.

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 secure bins for shredding.

808.5 CJDN MISUSE SUBJECT TO DISCIPLINE

808.5.1 INQUIRIES

Inquiries into the motor vehicle registration, driver license, criminal history or any other file in the MNJIS/NCIC systems will be performed for criminal justice purposes only.

808.5.2 MISUSE SUBJECT TO DISCIPLINARY ACTION

Any employee misusing information or obtaining information for other than official criminal justice purposes from the Criminal Justice Data Network may be subject to disciplinary action.

When performing any file inquiries or making any entries into NCIC or MNJIS, it is important to remember that the data stored in MNJIS/NCIC is documented criminal justice information and this information must be protected to ensure correct, legal and efficient dissemination and use. The individual receiving a request for criminal justice information must ensure that the person requesting the information is authorized to receive the data. The stored data in NCIC and MNJIS is sensitive and should be treated accordingly, and unauthorized request or receipt of NCIC or MNJIS material could result in criminal proceedings.

808.6 POTENTIAL VIOLATIONS

808.6.1 ADDRESSING A POTENTIAL VIOLATION

When the Chief of Police, Captain or the TAC becomes aware that an employee of the Columbia Heights Police Department is using a CJDN terminal, CJDN terminal generated information, CJDN equipment, or CJDN access not in accordance with agency policies, state policies, or NCIC policies and said problem is not deemed merely operator error, the Chief of Police or his designee, or the TAC shall promptly address the violation.

808.6.2 PROCEDURE FOR POTENTIAL VIOLATIONS

The Chief of Police or his designee shall meet with the person who is alleged to have violated the policy and determine appropriate sanctions, which may include any or all of the standard discipline policies currently in place at the Columbia Heights Police Department, including verbal reprimand, written reprimand, suspension, or termination. Intentional misuse of the CJDN system is a serious violation and the BCA will be notified within 24 hours of a security incident. If criminal behavior is believed to have occurred, appropriate agencies will be notified for further investigation.

The specific situation in each case of misuse of the CJIS system will be looked at, with all circumstances considered when determining disciplinary actions. Consideration will be given to the extent of loss or injury to the system, agency, or other person upon release or disclosure of sensitive or classified information to an unauthorized individual. This also includes activities which result in unauthorized modification or destruction of system data, loss of computer system processing capability, or loss by theft of any computer system media including: optical or magnetic storage medium, hardcopy printout, etc.

808.7 TERMINATING OF CJDN ACCESS

The TAC, with the approval of the Chief of Police, may at any time terminate a staff person's access to the CJDN system for any rule violation.

808.8 STATE LAW RELATED TO DVS ACCESS

Effective October 1st, 2018, Minn. Stat. § 171.12 Subd. 1a. requires the Minnesota Department of Public Safety Driver and Vehicle Services to immediately and permanently revoke the authorization of any individual who entered, updated, accessed, shared, or disseminated data in violation of state of federal law.

- As the ability to access MN DPS data is a critical component of a police employee job function, loss of access may result in termination of employment.