Sheridan Police Department
Policies and Procedures
13.2 Replaces 301.4.9
Chapter 13 – Communications
Section 2 – Security Policy

Date: January 3, 2013
Revised: 05/03/2017, 10/11/2017, 06/26/2019
03/11/2022
Reviewed: 01/13/2022

Signature:

The Sheridan Police Department adopts the CJIS Security Policy as its minimum security policy. Any Sheridan Police Department policy herein is to enhance and not reduce these standards. Information obtained through criminal justice information systems shall be safeguarded, kept confidential and disseminated only in accordance with policy and the law.

Definitions

CJIS -	Criminal Justice Information Systems is the controlling federal policy division for all National Crime Information Center terminals. Data disseminated through the terminals includes NCIC as well as state and local data.
NCIC -	National Crime Information Center is a computerized index of criminal justice information (i.e. - criminal record history information, fugitives, stolen properties, and missing persons, etc.).
TAC -	Terminal Agency Coordinator is an authorized user, assigned by the chief of police, responsible for maintaining security of the terminal and records, as well as ongoing training for authorized users.
WCJIN -	Wyoming Criminal Justice Information Network refers to state disseminated CJIS information as wells as statewide systems.
DCI -	Division of Criminal Investigation (Control Terminal Section) which houses criminal history information collected in Wyoming.
III -	Interstate Identification Index (III) provides a method for requesting a criminal history record once a person has been associated with an index record, or when the person has been positively identified with a prior record through fingerprint comparison at the local or state level.
ORI -	Originating Agency Identifier is a nine-character identifier assigned by the FBI for identification purposes of an agency.
CHRI -	Criminal History Record Information maintained in a computerized network and housed in NCIC files.
NLETS -	National Law Enforcement Telecommunications System is the message switching network linking local, state, and federal agencies together to provide the exchange of criminal justice and public safety-related information on an interstate basis.
Authorized User -	Those personnel who have completed a background check as approved by the chief of police or his or her designee and who have been authorized by the chief or his or her designee to receive CJIS information.

13.2.1 Personnel Background Screening For System Access

A. State and national fingerprint-based record checks will be conducted for all personnel, including appropriate IT personnel, before granting access to Federal Bureau of Investigation criminal justice information systems.
    1. If a felony conviction of any kind is found, access will not be granted.
    2. A criminal record of any other kind may be grounds for CJIS access denial at the discretion of the state control terminal officer.

B. The Sheridan Police Department will also screen custodial, support, and/or contractor personnel, who access terminal areas unescorted, through established personnel background screening methods including fingerprinting.

13.2.2 Security Standards

A. Authorized users shall access CJIS systems and disseminate CJIS data only for purposes for which they are authorized. CJIS data shall be disseminated only to those personnel authorized to receive the data. Employees receiving information are responsible for maintaining the confidentiality of the information. Under no circumstances shall data be disseminated outside the criminal justice community.

B. Failing to comply with established information security policies and procedures or any violation of CJIS Security Policy, NCIC Policy, and WCJIN Policy are grounds for employee formal discipline. The individual or employee responsible will be subject to department disciplinary actions up to and including termination and criminal prosecution. Improper access, use or dissemination of Interstate Identification Index (III) information is serious and may result in the imposition of administrative sanctions including, but not limited to, civil, state and federal criminal penalties.

C. The FBI authorized ORI will be used in each transaction on CJIS in order to identify the agency sending or requesting data.

D. Any criminal justice agency that receives access to CJIS data shall enter into a signed written agreement with the department and DCI, as established by FBI CJIS. The agreement will specify the systems to which the agency will have access and that the agency will adhere to CJIS policies.

E. Information obtained from the Interstate Identification Index (III), and information obtained as a result of its access, contains CHRI. Access and dissemination from these files are to be consistent with the dissemination policies concerning the III.
    1. The Interstate Identification Index (III) may only be accessed for an authorized purpose.
    2. Dissemination to another agency is authorized only if the other agency has an ORI.
    3. All users will provide a reason for all Interstate Identification Index (III) inquiries.
    4. Interstate Identification Index (III) information is considered sensitive and shall be protected to prevent any unauthorized access, use or dissemination of the information.
    5. Improper access, use or dissemination of Interstate Identification Index (III) or Hot File information is serious and may result in the imposition of administrative sanctions including, but not limited to, termination of services and state and federal criminal penalties.

F. Dissemination to another agency is authorized if (a) the other agency is an Authorized Recipient of such information and is being serviced by the accessing agency, or (b) the other

agency is performing personnel and appointment functions for criminal justice employment applications.

1. Communications Technicians will only run III transactions for the Agencies we have User Agreements with.
2. Upon receipt of a request for III, Communications Technicians will fulfill the request at the soonest time possible within a reasonable timeframe.
3. Completed III to be disseminated will be documented with a dissemination log (CHRIS From) and then placed into the appropriate routing folder to be delivered by authorized personnel to the requester.
4. All II and CHRI at rest will be protected with technical and physical safeguards to ensure the security and confidentiality of the information.
5. The Sheridan Police Department does not store any information obtained from the II, except background checks for criminal justice employment purposes for agency personnel. These printouts are kept in the Background Packet and kept in a secure, private, and locked room.

G. To prevent unauthorized viewing or access to the terminal, the terminal sites will not be left unattended while logged into NCIC.

H. Monitors facing windows available to public view must have appropriate physical security (i.e. - blackout screens).

I. All data associated with FBI CJIS records will be securely stored and/or disposed of to prevent access by unauthorized personnel. This includes hard copy and media devices.

J. Criminal history records will be maintained for extended periods only when the III records are key elements for the case files where they are retained.

K. When retention of III records is no longer required, officers, communication operators, and records personnel will dispose of records by shredding or other methods that render them unreadable.

L. A log shall be maintained for a minimum of one (1) year on all III transactions. The log will:

1. Identify the requestor and any secondary recipients;
2. Provide a unique identifier (title and name) for the requestor; and
3. Provide a reason for the inquiry consistent with CJIS policy (Purpose code C, J).

M. Authorized personnel will accompany visitors in the communications center at all times.

N. Firewalls shall be in place to prevent unauthorized access to CJIS data and all network components providing access to the FBI/CJIS wide area network, either directly or indirectly through connections to other networks. The firewall shall secure all forms of access.

1. If a security incident/event does occur on a computer with access to FBI/CJIS information, it will be immediately reported to the City of Sheridan IT manager, TAC, and DCI Control Terminal. The incident will be documented and recorded to report date and time, Communications Operator discovering the incident, plus details of the incident and the reconciliation of the event. The recorded incident will then be submitted to the Operations Lieutenant via the Supervisor on Duty.

O. Any electronic device using radio or voice data may be used to transmit CHRI when an officer determines that there is an immediate need for this information to further an investigation or there is a situation affecting the safety of an officer or the general public.

P. A facsimile can be used to transmit CHRI provided both agencies involved have an NCIC ORI authorized to receive criminal history information. The facsimile must meet the same security considerations for identification and authentication.

Q. E-mail of FBI/CJIS data is not permitted.
R. Adding or storing FBI/CJIS data in G Suite Google Drive is not permitted.

13.2.3 Adding and Removing Employee Access to NCIC / CJIS

A. When a new employee enters NCIC training, his or her assigned field training officer will advise the TAC, or designee. The new employee will complete the "Log-On Activation/Deletion" request form available on the police department intranet.
B. The "New Operator" information will be filled in. The new employee will read rules of behavior available on the police department intranet and the employee and TAC will sign the form and fax it to the DCI control terminal for activation.
C. The DCI control terminal will teletype the new user's unique ID, which will be given to the TAC.
D. A new communication operator will use this ID, upon completion of the NCIC training given by the TAC or designee and satisfactory completion of the NCIC full user exam administered through the WCJIN intranet. The operators shall complete security awareness training within six (6) months of his or her date of hire.
E. A new limited user employee will use his or her ID upon completion of the NCIC training given by the TAC or designee and the satisfactory completion of a NCIC limited user exam administered by the TAC. New limited user employees shall complete security awareness training within six (6) months of their date of hire.
F. Bi-annually the CJIS rules of behavior/security awareness training will be reviewed, initialed and signed by all users and the TAC. This form will be retained in the information security book by the TAC for audit purposes.
G. Upon separation of an employee from the department, the TAC will print out the "Logon Activation/Deletion" request form and fill in the information for removal of the operator and fax it to the DCI control terminal.
H. Upon separation from the department the CJIS security debriefing form will be provided to the employee by the TAC or designee to ensure department employees are apprised of the fact that FBI CJIS information accessed during the course of his or her employment remains sensitive and subject to CJIS security policy. Further, the dissemination of sensitive information could subject the employee to civil and criminal penalties should the information be disseminated without proper authorization. The TAC will document delivery of the form to the employee upon separation in Spillman training files.

13.2.4 Computer System Level and User Level Passwords

Passwords shall:

A. Be a minimum length of eight (8) characters on all systems
B. Not be a dictionary word or proper name
C. Not be the same as the UserID
D. Expire within a maximum of 90 calendar days
E. Not be identical to the previous ten (10) passwords
F. Not be transmitted in the clear outside the secure location
G. Not be displayed when entered
H. A minimum of four (4) alpha characters will be used
I. Two (2) of the alpha characters will need to be "UPPER CASE"
J. Two (2) of the alpha characters will need to be "lower case"

K. Use a minimum of two (2) digits (numbers)
L. Use a maximum of one (1) repeated character
M. Passwords, VPN's, Key Cards, (any information system authenticator) will have reasonable measures taken to safeguard them. No loaning or sharing of authenticators are permitted. Lost or compromised authenticators will immediately be reported to the IT Administrator or Systems Manager.

13.2.5 Event Logging in Spillman

A. The following events in Spillman shall be logged
    1. Successful and Unsuccessful System log-on attempts
    2. Successful and Unsuccessful attempts to use"
        a. Access permission on a user account, file, directory or other system resource
        b. Create permission on a user account, file, directory or other system resource
        c. Write permission on a user account, file, directory or other system resource
        d. Delete permission on a user account, file, directory or other system resource
        e. Change permission on a user account, file, directory or other system resource
    3. Successful and unsuccessful attempts to change account passwords
    4. Successful and unsuccessful actions by privileged accounts
    5. Successful and unsuccessful attempts for users to:
        a. Access the audit log file
        b. Modify the audit log file
        c. Destroy the audit log file
B. The following events will be logged with the applications of SYLOG and APLOGIN
C. Logs will saved in a '.pdf' format on an external hard drive device and reviewed on a weekly basis by the Spillman SAA/SSA for a period of 4 years per the State of Wyoming Retention Schedule.

13.2.6 Event Logging in Google G Suite

A. The following events in Google shall be logged
    1. Successful and Unsuccessful System log-on attempts
    2. Successful and Unsuccessful attempts to use"
        a. Access permission on a user account, file, directory or other system resource
        b. Create permission on a user account, file, directory or other system resource
        c. Write permission on a user account, file, directory or other system resource
        d. Delete permission on a user account, file, directory or other system resource
        e. Change permission on a user account, file, directory or other system resource
    3. Successful and unsuccessful attempts to change account passwords
    4. Successful and unsuccessful actions by privileged accounts
    5. Successful and unsuccessful attempts for users to:
        a. Access the audit log file
        b. Modify the audit log file
        c. Destroy the audit log file
B. These events will be logged with the applications of G Suite Admin Console Reports
    1. Google Vault logs all information and data in Google G Suite
        a. Google Vault Retention is set to never expire

C. Logs can be saved in a '.pdf' format on an external hard drive device. They are reviewed on a weekly basis by either the Sheridan Police Department Google G Suite Administrator, or the City of Sheridan Google G Suite Administrator. Physical copies made will be retained for a period of 4 years per the State of Wyoming Retention Schedule.

13.2.7 Virtual Escorting and Permitting Remote Access

A. The following refers to computers, software, and databases that contain or have access to FBI NCIC/CJIS information:

1. Remote access shall be permitted for privileged functions only for compelling operational needs.

2. Permitted remote access will be documented and will include basis for the access, date, time, the name of the monitor for the session and the process used for enabling remote access for the privileged functions for the remote access.

3. Virtual escorting of privileged functions will be permitted only when all of the following conditions are met:

   a. The session shall be monitored at all times by an authorized escort
   b. The escort shall be familiar with the system/area in which work is being performed
   c. The escort shall have the ability to end the session at any time
   d. The remote administrative personnel connection shall be via an encrypted (FIPS 140-2 certified) path
   e. The remote administrative personnel shall be identified prior to access and authenticated prior to or during the session.