Charleston County Coroner's Office Policy #11
Title: Criminal Justice Information Services Security **Page:** 1 of 11
Effective Date: 05/17/2018 **Reviewed:** 3/18/2021, 9/15/2023 **Authorized By**: Bobbi Jo O'Neal, Coroner

11.1 POLICY

1. The Charleston County Coroner's Office is an authorized agency to access data from the Criminal Justice Information Service (CJIS). Only the Coroner, Chief Deputy Coroner, and Deputy Coroner(s) may access the system after completing Level 2 CJIS Security Training, which must be updated every two years. Other employees who have access to any documents related to CJIS information will also be subject to completing requirements to satisfy CJIS Information Security in accordance with CJIS regulations.

2. The U.S. Department of Justice published the Criminal Justice Information Services (CJIS) Security Policy, which can be found at https://www.fbi.gov/services/cjis/cjis-security-policy-resource-center.

3. Unauthorized requests, receipt, release, interception, dissemination, or discussion of criminal justice information could result in criminal prosecution and/or termination of employment. Continued misuse of CJI could result in an agency being denied access until the violations have been corrected. Any security incident should be reported to the Charleston County Coroner's Information Security Officer.

11.2 PROCEDURE

1. Only the Coroner, Chief Deputy Coroner, and Deputy Coroner(s) who have completed CJIS security training may request or have access to CJIS information.

2. Any CJI obtained during a medicolegal death investigation, which is uploaded to MDIlog, must be marked "Restricted" by the individual uploading the document to ensure there is no unauthorized access or release of such information. All hard copies of such information shall be shredded by the individual who obtained the information.

3. Queries by the Charleston County Coroner's Office are performed by the Charleston County Consolidated 9-1-1 Center (Center). As such, The Center's policy regarding CJIS Security is attached, as well as the Center's Standard Operating Procedure for CJIS NCIC Disciplinary Measures. Unless otherwise directed by the Coroner, their Disciplinary Measures SOP is used by this office.

CHARLESTON COUNTY CONSOLIDATED 9-1-1 CENTER POLICY ON CRIMINAL JUSTICE INFORMATION SYSTEMS (CJIS) SECURITY EFFECTIVE 2/4/2013

PURPOSE:

A. The Charleston County Consolidated 9-1-1 Center (Center) is tasked with providing support services to various Law Enforcement agencies, which require the use of Criminal Justice Information Services (CJIS). CJIS provides all Criminal Justice Agencies (CJA) and Non-criminal Justice Agencies (NCJA) with a minimum set of security requirements used in accessing Federal Bureau of Investigation (FBI) CJIS Division systems.

B. The Criminal Justice Information Services Security Policy provides guidance on the safeguard of Criminal Justice Information (CJI) and National Criminal Information Center (NCIC) terminals.

C. This procedure is intended to supplement the Criminal Justice Information Services Security Policy, which is regulated by the Federal Information Security Management Act of 2002.

PROCEDURES:

D. Authority:

1. Lead CJIS Systems Officer (CSO):
a. Assumes overall responsibility for managing the security of CJIS systems of all user agencies. b. Approves agency user's access to FBI CJIS systems. c. Delegates responsibilities to subordinate agencies in ensuring appropriate use, enforcement system discipline and ensuring CJIS Division operating procedures are followed by all users of the respective services of information. d. Ensures state/federal agency compliance of user agencies are in compliance with policies approved by the Advisory Policy Board (APB) and adopted by the FBI.

2. Agency CJIS Systems Officer (CSO):

a. Assumes overall responsibility for managing the security of CJIS systems within their agency. b. Submits recommendations for approval of agency user's access to FBI CJIS systems to the Lead CSO. c. Ensures appropriate use, enforcement system discipline and CJIS Division operating procedures are followed by all users of the respective services of information. d. Ensures agency is in compliance with policies approved by the Advisory Policy Board (APB) and adopted by the FBI. e. Designates a Terminal Agency Coordinator (TAC) within agency that has devices accessing CJIS systems. (CJIS Security Policy 5.1, 3.2.2)

3. Agency Terminal Agency Coordinator (TAC):

a. Serves as the direct point of contact at the Center for matters relating to CJIS information access. b. Administers CJIS systems programs within the Center and oversees the Center's compliance with CJIS systems policies. c. Keeps all Center operators up to date on all policies, procedures and capabilities of the NCIC system. (CJIS Security Policy 5.1, 3.2.3) d. Logs access privilege changes and maintains all logs for a minimum of one (1) year. (CJIS Security Policy 5.1, 5.5.2.1) e. Validates access privileges annually and documents validation process, if applicable. (CJIS Security Policy 5.1, 5.5.1) f. Documents security awareness training and maintains the current status of all Operators training.

4. Local Agency Security Officer (LASO):

a. Identifies who is using the CJIS Systems Agencies (CSA) approved hardware, software, and firmware and ensure no unauthorized individuals or processes have access to the same. b. Identifies and documents how the equipment is connected to the state system. c. Ensures that personnel security screening procedures are being followed as stated in this Policy. d. Ensures the approved and appropriate security measures are in place and working as expected. e. Supports policy compliance and ensure the CJIS Systems Agency Information (CSA ISO) is promptly informed of security incidents. f. The duties of the LASO will be assigned to the Center's Information Technology Manager or qualified designee.

E. Access Control:

1. The Center shall identify authorized users of information systems with specific access rights and privileges. The Center will grant access to the information systems based on the following:

a. Valid need-to-know or need-to-share use, which is determined by assigned official duties. b. Satisfaction of all personnel security criteria. (CJIS Security Policy 5.1, 5.5.1)

2. All visitors without the proper credentials, accessing the designated areas where CJI information may be displayed or where there is access to information systems, will be required to sign into the visitor access log, upon verifying individual's access authorization. (CJIS Security Policy 5.1, 5.9.1.3)

3. All visitors without the proper credentials will be escorted by authorized personnel/staff and their activity monitored at all times where CJI information may be displayed or where there is access to information systems. (CJIS Security Policy 5.1, 5.9.1.7)

4. The TAC will notify the appropriate agency in the following conditions:

a. A user's information system usage, need-to-know or need-to share changes.

b. A user is terminated; transferred or associated accounts are removed, disabled, or otherwise secured.

F. Personnel Security:

1. All personnel will be required to complete the following prior to being granted access to FBI CJIS systems:

a. Certification:

2. All personnel with access to CJI will complete basic security awareness training within six (6) months of initial assignment and biennially thereafter. 2. Listed below are some examples of individuals who are required to take security awareness training in addition to all CJA (Criminal Justice Agency) employees: a. Contractors used by the Center b. Vendors/IT support used by the Center c. Maintenance/Groundskeepers d. Volunteers used by the Center

3. All NCIC Operators will be NCIC certified through the South Carolina Law Enforcement Division (SLED) within six (6) months of hire and will successfully complete reaffirmation every two (2) years. (CJIS Security Policy 5.1, 5.2, APCO CALEA 6.4.4)

b. National Fingerprint-based Record Check:

1. To verify identification, all personnel will complete a fingerprint card within thirty (30) days upon initial employment or assignment. This also applies to all personnel who have authorized access to FBI CJIS Systems and those who have direct responsibility to configure and maintain computer systems and networks with direct access to FBI CJIS Systems. 2. Information obtained through the fingerprint-based record check will be handled as follows:

a. In the event it is determined that any kind of felony conviction exists, access will be denied. However, the TAC may request a review by the CSO in extenuating circumstances where the severity of the offense and the time that has passed would support a possible variance. b. If a record of any other kind exists, system access shall not be granted until the CSO or his/her designee reviews the matter to determine if system access is appropriate. c. If the person appears to be a fugitive or appears to have an arrest history without conviction for a felony or serious misdemeanor, the CSO or his/her official designee shall review the matter to determine if system access is appropriate. d. If the person is employed by a non-criminal justice agency, the CSO or his/her official designee and if applicable, the appropriate board maintaining administrative control, shall review the matter to determine if system access is appropriate. This same procedure applies if this person is found to be a fugitive or has an arrest history for a felony or serious misdemeanor without conviction (Charleston County Sheriff has management control of the Center through a signed Management Control Agreement). e. If the person already has system access from another law enforcement agency, i.e., transitioning operator, the CSO or his/her designee may grant system access prior to the confirmation of the new state of residency and national fingerprint-based record check. This does not implicitly grant hiring/firing authority with the CSO, only the authority to grant FBI CJIS systems access. f. If the CSO or his/her designee determines that CJIS systems access by the person would not be in the public's interest, access shall be denied and the Center's TAC will be notified in writing of those access denials. g. Support personnel, contractors and custodial workers who access computer terminal areas shall be subject to a state of residency and national fingerprint-based record check, unless these individuals are escorted by authorized personnel at all times.

G. Security Measures:

1. Terminal Accessibility:

a. Each terminal capable of accessing the NCIC network is located within the Communications Center within a limited, controlled access area to prevent unauthorized access. b. All ingress/egress doors to the Communications Center are accessed only by approved entry badges. c. All ingress/egress doors are posted with "No Unauthorized Personnel, Restricted Access." d. All NCIC terminals are placed in an area that is not accessible to the public. e. All approved visitors within the Communications Center will be escorted at all times. f. All visitor access records will include the name and agency of the visitor, their signature, form of identification used to identify the visitor, date of access, time of entry/departure, purpose of their visit. g. No terminals will be located in such a place as to be viewed by those who are not certified or authorized to obtain the

information from the system. h. In the event that an operator must leave an accessed terminal, the operator will log off, denying access to anyone, until the certified operator returns. (CJIS Security Policy 5.1, 5.9)

2. Information Security:

a. Any information obtained from the NCIC system will be kept in a secure location to prevent unauthorized access.
b. All printouts, when no longer needed, will be shredded to protect sensitive information.
c. No printouts will be thrown in the garbage can for general disposal.
d. All electronic media will be overwritten at least three (3) times to ensure proper disposal.
e. All information obtained from the NCIC system is confidential and all operators will ensure they appropriately dispose of any information obtained.
f. NCIC information will only be used for criminal justice purposes. Disclosing information to an unauthorized source or failure to follow NCIC procedures is subject to disciplinary action and/or criminal prosecution. Therefore, the operator is responsible for verifying the identity of the requesting party before releasing this information.
g. If at any time the operator is unsure of the identity of the person requesting information, no information shall be disseminated until further checking to verify the person's identity.

3. Authentication:

a. All authorized operators within the Center shall ensure the following secure password attributes:

1. Passwords shall be a minimum length of eight (8) characters.
2. Passwords shall not be a dictionary word or proper name.
3. Passwords and the user name shall not be the same.
4. Passwords shall be changed within a maximum of ninety (90) days.
5. All systems shall prevent password reuse of the last ten (10) passwords.
6. Passwords shall not be transmitted in the clear, outside the secure domain.
7. All wireless links or server access points will be protected by authentication to ensure protection from unauthorized system access. (CJIS Security Policy 5.1, 5.6.2.1)

b. Advanced Authentication (2 Factor):

1. Agencies utilizing the "Risk-based Authentication" shall utilize the typical user identification and include a software token element comprised of a number of factors, such as network information, positive device identification (i.e., device forensics, user pattern analysis and user bindings), user profiling, and high-risk challenge/response questions.

c. Under no circumstances will operators share their passwords or log another operator onto the system using his/her password.

H. National Crime Information Center (NCIC):

1. Identity History Summary (IdHS): formerly Criminal History Record Information (CHRI)

a. The privacy and security precautions for criminal history record information will only be accessed, released and disseminated under the guidelines described in Title 28, Part 20, Code of Federal Regulations. b. The following files are protected as IdHS:

1. Gang File
2. Known or Appropriately Suspected Terrorist File
3. Convicted Persons on Supervised Release File
4. Immigration Violator File (Formerly the Deported Felon File)
5. National Sex Offender Registry File
6. Historical Protection Order File
7. Identity Theft File

c. All other remaining NCIC files will be considered "hot files."

I. Information Integrity:

1. CJI shall only be accessed and used for authorized purposes and in no circumstances authorized for personal use.

2. Dissemination to another agency is authorized only when the other agency is an Authorized Recipient of such information and is being serviced by the Center.

3. CJI shall not be transmitted unencrypted across the public network, unless the data is immediately protected via cryptographic mechanisms (encryption). Examples of unencrypted transmissions include CJI forwarded through personal email and personal hand held devices, etc. CJI transmitted via facsimile shall be exempt from encryption requirements. (CJIS Security Policy 5.1, 5.10.1, 5.10.1.2 and 5.10.2)

4. A fax machine may be used to transmit IdHS provided both agencies involved are ORI (Originating Agency Identifier) authorized to receive this information. The requestor will be notified prior to transmitting the information via fax.

5. Operators will be responsible for listing the name of the person actually receiving the information in the "Attention" field and for correctly completing the "Justification" field to include the case number. At no time will the word "Criminal Investigation" be used in a response; instead a code for the specific reason for the request will be used, such as "Homicide", "Traffic Stop", "Jail Classification", "Suspicious Person", etc.

6. IdHS will only be disseminated over the radio if the safety of a First Responder or the general public is at risk.

J. NCIC Hit Confirmation & Responses:

1. All hit confirmations will follow NCIC 2000 hit confirmation procedures as mandated in the NCIC Manual, within the required time frames as set forth by the FBI. 2. Officers will advise the telecommunicator to send the hit.

3. The NCIC Operator will determine which priority to use, based on information received from the officer (i.e., if the officer has charges on the subject, in addition to another agency having charges on said subject, a routine hit will be sent in lieu of an urgent hit)

4. Hit confirmation requests will be sent in a timely manner and the request marked as "Urgent" or "Routine" based on the circumstances of the request.

5. If a response is not received in the allotted time, then a second request will be sent.

6. If the allotted time passes again with no response, then a third request will be sent.

7. In the event that an agency does not respond to these requests, an attempt will be made to contact them by phone to determine if there is a problem with receiving the request.

8. Urgent hits will be answered within ten (10) minutes, which is usually when the subject is present.

9. All routine hits will be answered within one (1) hour.

10. All initial confirmations handled by telephone require an NCIC response for documentation purposes and should be completed as soon as possible.

11. All hit confirmation requests received by the Center will be responded to in the allotted time.

K. Delayed Hits:

1. When a delayed hit is received, the information is verified and if it is determined to be the correct information, the operator will note this information on the delayed hit and place the paperwork into the delayed hit folder.

2. In some cases, delayed hits will hit on valid entries and if it was entered by a Center operator, the operator will contact the user agency to ascertain whether they still have the person, vehicle or item.

3. If the user agency still has the person, vehicle or item, the operator will request the agency send a routine hit or ensure all actions taken with the entry are recorded.

4. If the delayed hit is from an inquiry the Center completed on another agency's entry, the Center operator will send a routine hit. This will be completed to ensure the other agency is advised of all actions taken by the Center.

5. Agencies outside of the Center shall handle the required documentation in accordance to their agency-specific written directives.

L. Agency Queries:

1. The Center will handle all queries for the following agencies:

a. Charleston County Sheriff's Office b. City of Charleston Police Department c. Isle of Palms Police Department d. Mount Pleasant Police Department e. North Charleston Police Department f. Sullivan's Island Police Department g. Lincolnville Police Department h. National Park Service i. Charleston County Coroner's Office j. CSX Railroad k. DHEC l. Charleston Parking Services

2. Each respective user agency is responsible for entering, clearing, canceling, modifying, and responding to all Hit Requests.

3. The Center will run ICHS for deputies and officers upon request; however, divisions within each agency who have access are encouraged to run their own or utilize their agency's Records Department.

4. The Center will send Hit Requests on behalf of deputies and officers, as well as the subsequent Locate, using the following general guidelines.

a. When a potential hit is received, the Law Dispatcher will send the hit request (YQ) to the agency entering the record b. The Law Dispatcher will then contact the user agency's Records Department by phone, advising that a hit request (YQ) has been sent and that they should receive the hit response (YR) in the allotted timeframe c. The Law Dispatcher will also notify the NCIC Dispatcher of the impending hit response (YR) via fax d. Upon receiving the hit response (YR), the user agency will fax the hit response (YR) to the CDC NCIC fax machine. e. The NCIC Dispatcher will deliver the hit response (YR) to the Law Dispatcher. If the hit response (YR) is not received within a few minutes of the required timeframe of sending the hit, the Law Dispatcher will contact the user agency and determine if they have received the hit response (YR) f. The Law Dispatcher will advise the deputy or officer of the response and send the locate, if required by NCIC g. The Law Dispatcher will fax the additional paperwork to the user agency

5. The Center will contact the user agency's Warrants/Records office by telephone to confirm hits on user agency warrants showing in RMS or NCIC. The Law Dispatcher will notify the deputy or officer of the result, whether it is confirmed or not.

6. If the hit is on a vehicle located within the area the Center services, a Law Enforcement unit will be sent out to physically recover the vehicle and complete a supplemental report.

M. Discipline:

1. Improper access, use or dissemination of IdHS and NCIC Non-Restricted Files information is serious and may result in administrative sanctions including, but not limited to, termination of services and state and federal criminal penalties. For example: Center staff disclosing information obtained through NCIC to unauthorized users for personal gain or knowledge or using another employee's password to access the system.

2. Violations within the Center will be handled on a case-by-case basis and in conjunction with the South Carolina Law Enforcement Division's CJIS/NCIC Disciplinary Policy (Attachment A) and will be used at the discretion of the Agency CSO or their delegated authority.

Approved by the Consolidated Dispatch Board on April 11, 2018.

NCIC Disciplinary Measures

VIOLATION	1ST OFFENSE	2ND OFFENSE	3RD OFFENSE
Unauthorized disclosures or receipt of SLED/CJIS-FBI/NCIC criminal justice information	2-5 days suspension to dismissal	5-10 days suspension to dismissal	15 days suspension to dismissal
Release of driver's license or vehicle information to other than criminal justice employees	2-5 days suspension	5-10 days suspension	15 days suspension to dismissal
Release of information to private security guards or firefighters	2-5 days suspension	5-10 days suspension	15 days suspension to dismissal
Allowing the use of the systems by personnel not certified by SLED, except for job training toward certification	3 days suspension to dismissal	5 days suspension or dismissal	Dismissal
Failure to comply with policies and procedures established in the Center and SLED/CJIS-FBI/NCIC Operations and Procedures Manual	Written reprimand to 3 days suspension	3-5 days suspension	5 days suspension or dismissal
Failure to log information supplied to the Solicitor's office, or any other criminal justice employee who does not have a user agreement with the Center	Written reprimand to 3 days suspension	3-5 days suspension	5 days suspension or dismissal
Unauthorized modification or destruction of system data; loss of computer system processing capabilities	3 days suspension to dismissal	5-10 days suspension or dismissal	15 days suspension to dismissal
Loss by theft of any computer system media including: chip ROM memory, optical or magnetic storage medium, hard copy printouts, etc.	3 days suspension to dismissal	5-10 days suspension to dismissal	15 days suspension to dismissal
Improper recordkeeping	Oral reprimand to 3 days suspension	1-3 days suspension	3 days suspension or dismissal