

# **CITY OF ANDERSON POLICE DEPARTMENT**

## **Anderson, South Carolina**

<b>DIRECTIVE TYPE</b> General Order	<b>EFFECTIVE DATE</b> March 18, 2013	<b>NUMBER</b> 2417
<b>SUBJECT</b> Security of Criminal Justice Information System (CJIS) <b>REVISED</b>		
<b>REFERENCE</b> GO 2412	<b>AMENDS/SUPERSEDES</b> All Others	
<b>DISTRIBUTION</b> All Personnel	<b>RE-EVALUATION</b> DATE Annual	<b>NO.</b> <b>PAGES 9</b>

### **A. Purpose:**

The purpose of this general order is to state the security requirements for all personnel who have physical and electronic access to the City of Anderson Police Department records, data and criminal justice information system. The following provides background on federal and state laws regulating the transmission, dissemination, storage, and disposal of law enforcement records and criminal justice information:

In 1992, Criminal Justice Information Services (CJIS) security policies were included as part of the original National Crime Information Center (NCIC) Security Policy. With growing technological advances in telecommunications and systems architecture, in 1998 the Advisory Policy Board (APB) recommended to the Federal Bureau of Investigation (FBI) that the CJIS Division authorize the establishment of a security management structure. As a result, the CJIS Security Policy was written and approved by the FBI Director in 1999. It required among other things, the implementation of specific technical controls, configuration management activities, and procedures for the documentation and notification of security incidents.....

Since its inception, the CJIS Security Policy has been revised several times to update and expand its requirements. It is now recognized as the 'living document' because future policy changes are expected, based on technology, which will serve to improve the confidentiality, integrity, and availability of CJIS data and systems to authorized users..... Adherence to the protocols and guidance of the CJIS Advisory Process and the

Advisory Policy Board is crucial to the continued development and enhancement of the *CJIS Security Policy*" (Ref: *CJIS Security Policy, July 2012 Version 5.1, 1.0*).

**B. Policy:**

All persons who access City of Anderson Police Department data, records and criminal justice information system(s) must comply with specifications set forth by all governing bodies, including but not limited to the Criminal Justice Information System Security Policy, the South Carolina Law Enforcement Division (SLED), South Carolina State law(s), and any other governing entity.

**C. Procedures:**

1. It is the policy of the Anderson Police Department that all computer programs and record documents will be accessed and used only for criminal justice and law enforcement purposes. Computer screens, program functions, sign on codes and passwords, screen layouts and format, computer and information, and South Carolina Law Enforcement Division (SLED) and Federal Bureau of Investigation (FBI) information will not be accessed, viewed, or shared with non-law enforcement personnel without proper authorization, i.e. Security Service Agreements.
2. The Anderson Police Department is responsible for the security of physical and electronic law enforcement files and documents to include SLED/CJIS/FBI files within our Department and electronic criminal justice information system. Guidelines are in place to enhance security for the use and access of these files. These guidelines include proper storage and limited access to such files. Each employee is responsible for ensuring this policy is adhered to at all times.

Data stored on the law enforcement network, external media or documents printed that include documented criminal justice information must be protected to ensure correct, legal, and efficient dissemination and use. Any individual receiving a request for criminal justice information must ensure the person requesting the information is authorized to receive the information. Stored data on the law enforcement network or external media and printed law enforcement information is sensitive and should be treated accordingly. An unauthorized request or receipt of law enforcement information or CJIS data could result in criminal proceedings or interdepartmental disciplinary action for any infraction, violation, or misuse of the system. This policy includes correct documentation for entry purposes into any information technology system on the law enforcement network as well as inquiries.



Any use of the Anderson City Police Department electronic criminal justice information system for purposes unrelated to law enforcement must be approved in writing by the Chief of Police and the South Carolina Law Enforcement Division (SLED). Use of the APD computer forensic servers and programs to analyze and report technical activity on personal computers, servers, hard drives, cell phones, laptops, etc., for parties involved in civil litigation, is an example where the Chief of Police approval and authorization is required.

3. The Chief of Police will designate a Local Agency Security Officer (LASO) who shall have the general responsibility for managing the physical and electronic security structure of the law enforcement information system. The LASO will report directly to the Chief of Police and the South Carolina Law Enforcement Division (SLED) for matters relating to the criminal justice information system. Specific responsibilities of the LASO include but are not limited to the following:
  - a. Serve as the security point of contact (POC) to the FBI CJIS Division ISO. *(Ref: CJIS Security Policy, July 2012 Version 5.1, 3.2).*
  - b. Document and provide assistance for implementing the security-related controls for the agency and its users. *(Ref: CJIS Security Policy, July 2012 Version 5.1, 3.2).*
  - c. Establish a security incident response and reporting procedure to discover, investigate, document, and report major incidents that significantly endanger the security or integrity of CJIS. *(Ref: CJIS Security Policy, July 2012 Version 5.1, 3.2).*
  - d. Identify who has access to the Anderson Police Department law enforcement information systems including hardware and software for the specific purpose of ensuring that no unauthorized users have access. *(Ref: CJIS Security Policy, July 2012 Version 5.1, 5.5).*
  - e. Confirm that criminal background screenings and fingerprint checks are completed on all personnel. Confirm that fingerprint checks and criminal history requests are sent to the South Carolina CJIS System Agency (CSA), CJIS Security Officer, SLED, Columbia, S.C. for Personnel that have a criminal record and must have special approval from SLED prior to accessing the criminal justice information system *(Ref: CJIS Security Policy, July 2012 Version 5.1, 4.1.1)*
  - f. Ensure each person who is authorized to store, process, and/or transmit criminal justice information and CJIS data is individually identified by use

of a unique identifier. A unique identification shall also be required for all persons who administer and maintain the system(s) that access the criminal justice information system and network (*Ref: CJIS Security Policy, July 2012 Version 5.1, 5.6.1*).

- g. Create an "Authentication Mechanism" to verify that users really are who they log-on as once an individual is 'uniquely identified" (*Ref: CJIS Security Policy, July 2012 Version 5.1, 5.6.2*).
- h. Identify and document how the law enforcement equipment is connected to the Anderson Police Departments Information System/Network. (*Ref: CJIS Security Policy, July 2012 Version 5.1, 5.7.1.2*).
- i. Maintain compliance with the CJIS Policy for all attached and installed equipment or software including but not limited to the setup, installation and security of such equipment and/or software. (*Ref: CJIS Security Policy, July 2012 Version 5.1*).
- j. Establish procedures for the documentation, maintaining, and updating of criminal justice information network configurations and ensure the distribution of these procedures. Notify the users of any changes that may affect their access. (*Ref: CJIS Security Policy, July 2012 Version 5.1, 5.7.2*)
- k. Ensure that a complete topological drawing which depicts the interconnectivity of the Anderson Police Department's system configuration is maintained in a current status.... The words "FOR OFFICIAL USE ONLY" shall appear near the bottom of the page containing the drawing. This drawing included all circuits, routers, firewalls, etc. (*Ref: CJIS Security Policy, July 2012 Version 5.1, 5.7.1.2*).
- l. Require signed User Agreements prior to authorization or access to the Anderson Police criminal justice information system by non law enforcement personnel and/or private contractors providing services. (*Ref: CJIS Security Policy, July 2012 Version 5.1, 5.1.1.6*).
- m. Ensure that appropriate security software programs and measures are in place, i.e. anti-virus, warning/banner, etc. (*Ref: CJIS Security Policy, July 2012 Version 5.1, 5.10.4.2-4*).
- n. Develop a lesson plan to ensure that security awareness training is provided at least once every two (2) years to all employees/authorized users (within six months of a new hire, appointment, and/or assignment)



who manage or have access to the Anderson Police Department criminal justice information system and CJIS data. The specifications and length of the lesson plan will be in accordance with SLED standards and protocol. Make sure that all users have signed the security awareness form on completion of the training (*Ref: CJIS Security Policy, July 2012 Version 5.1, 5.2*).

- o. Provide physical security for Anderson Police Department criminal justice information system, network and secure areas to protect against any unauthorized access to or routine viewing of computer devices, access devices, and printed or stored data. (*Ref: CJIS Security Policy, July 2012 Version 5.1, 5.9*).
- p. Establish procedures for the Transit, disposal, destruction, reuse, and/or sanitization of all criminal justice information media, i.e. diskettes, tape cartridges, ribbons, hard copies, printouts, used to process criminal justice information or CJIS data (*Ref: CJIS Security Policy, July 2012 Version 5.1, 5.8*).
- q. Support policy compliance and keep the FBI CJIS ISO and the Chief of Police informed of security incidents. (*Ref: CJIS Security Policy, July 2012 Version 5.1, 5.3*).

- 4. Criminal justice information, data, and resources available to Anderson Police Department employees/authorized users and accessed through all information systems or electronic media are to be used for official use to further the goals and objectives of the Anderson Police Department by providing an effective method to:

- a. Communicate.
- b. Perform research.
- c. Complete reports
- d. Obtain information while performing law enforcement related tasks

- 5. Employees/Authorized users of the Anderson Police Department criminal justice information system are expected to use good judgment while using any and all computer related resources, information systems and electronic media. Employees/authorized users are to abide by the following:

- a. All software licensing agreements and restrictions.
  - b. User agreements between the employee/authorized user and the Anderson Police Department.
  - c. Requirements set forth by South Carolina CJIS Systems Agency (CSA), South Carolina Law Enforcement Division (SLED), National Crime Information Center (NCIC) and CJIS Security Policy.
  - d. All applicable security requirements set forth by the Anderson Police Department, State and Federal Agencies and approved service providers.
6. The unauthorized use of computers, electronic media, information systems or printed documents containing Anderson Police Department law enforcement information and CJIS data for unofficial purposes is a violation of Anderson Police Department security policy and CJIS Security Policy. Unauthorized and unofficial activities which create violations include, but are not limited to, the following:
- a. Using any information system to include any type of computer or server without proper authorization.
  - b. Assisting in, encouraging, or concealing from the Anderson Police Department or other authorities any unauthorized use, or attempted unauthorized use, of any information system to include any type of computer or server.
  - c. Knowingly endangering the security of any criminal justice information system, computer, or server, or willfully interfering with others authorized for usage of these systems.
  - d. Giving away or sharing any password assigned to them to access any criminal justice information system without proper authorization.
  - e. Reading, altering, or deleting any other person's files or electronic mail without specific authorization.
  - f. Downloading or introducing unauthorized programs or files.
  - g. Manipulating or altering current software on Anderson Police Department mobile or desktop computer(s).
  - h. Transmitting any material or messages in violation of Federal, State, local law or City policy, including sexually, racially, or ethnically offensive comments, jokes, slurs, threats, harassment, slanders, or defamation.
  - i. Accessing or distributing obscene or suggestive images or offensive graphical images.
  - j. Distributing sensitive or confidential law enforcement information.
  - k. Distributing unauthorized broadcast messages or solicitations.




- l. Using Anderson Police Department provided electronic media to accomplish personal gain or to manage a business.
  - m. Distributing copyrighted materials not owned by the Anderson Police Department, including software, photographs, or any other media.
  - n. Downloading copyrighted information or software.
  - o. Developing or distributing programs designed to infiltrate computer systems internally or externally.
  - p. Accessing or downloading any resource for which there is a fee without prior, appropriate approval.
  - q. Attempting to access any system an employee is not authorized to access (hacking).
  - r. Listening to voice mail or reading electronic mail of another employee.
  - s. Endorsing political activities.
7. A physically secure location is an area, a room or group of rooms within a facility with both the physical and personnel security controls sufficient to protect Criminal Justice Information (CJI) and associated information systems. Due to the requirement of physical security within the Anderson Police Department the following areas or considered physically secure locations and the doors must remain locked when no authorized user is present in the area. (*Ref: CJIS Security Policy, July 2012 Version 5.1, 5.9.1*).
  - a. Roll Call room
  - b. CID Office
  - c. Front Booking office
8. Controls must be in place for the transportation of documents whether printed or in digital format that contains CJI. These documents must remain with the authorized user at all times. If you are using a form of Electronic media such as CD/DVD, flash drives, external drives, or digital memory card you must maintain control of this item. If possible the item must be encrypted to prevent compromise of the data stored. If encryption of data is not possible then the item must be kept in a secure location or with the authorized user at all times. CJI information cannot be emailed unless the email has been encrypted and the individual receiving the document is an authorized user. (*Ref: CJIS Security Policy, July 2012 Version 5.1, 5.8*).

9. Procedures for disposal, destruction, reuse, and/or sanitization of all CJI data, media and papers must be set to insure that the information is not used by an unauthorized person. The following steps have been set forth to protect the CJI. (Ref: CJIS Security Policy, July 2012 Version 5.1, 5.8).
  - a. *Printed documents* – Once a printed document is no longer needed this document must be placed in the proper shred box to be shredded.
  - b. *Electronic Media* – Once data stored on electronic media (flash drives, CD/DVDs, digital media, external drives and internal hard drives) is no longer needed, the media is retired or the media no longer operates this media must be turned in to the Information Technology Unit or LASO for the data to be erased or wiped. If the media cannot be erased or wiped the media must be destroyed in the proper manner to insure that the data cannot be retrieved. Once the media has been erased or wiped the media can be put back in operation.
10. Shred boxes are located in various areas of the department. These boxes contain CJI that must be shredded before transportation to any other location. When the shred agency arrives to empty and shred the documents the following procedures must be followed:
  - a. The shred agency representative must be accompanied by an authorized user from the department at all times while removing and emptying the shred boxes.
  - b. The authorized user must witness the shredding of the documents before the shred agency leaves the area for transport.
  - c. A document must be kept logging the time, date and the authorized users name.
11. Physical security must be maintained and the Anderson Police Department must control physical access by authenticating visitors before authorizing escorted access to the physically secure locations (except for those areas designated as publicly accessible). The department must escort visitors at all times and monitor their activity while they are in physically secure areas. Access records must be kept for visitors accessing the physically secure areas with the following information: (Ref: CJIS Security Policy, July 2012 Version 5.1, 5.9).
  - a. Name and agency or the visitor
  - b. Form of identification
  - c. Date of access



- d. Time of entry and departure
  - e. Purpose of visit
  - f. Name and agency of person visited
12. Personally owned information systems such as laptops, tablets, mobile phones, etc cannot be authorized to access, process, store or transmit CJI. This is because no terms or conditions can be put in place for the protection of CJI data including proper antivirus, setup and software applications on a personally owned information system. (Ref: CJIS Security Policy, July 2012 Version 5.1, 5.5.6.1).
13. Violations of this General Order and CJIS Security Policy will result in disciplinary action appropriate to the violation. Disciplinary action may include one or more of the following:
- a. Counseling.
  - b. Written reprimand.
  - c. Suspension from duty without pay.
  - d. Termination of employment.
  - e. Criminal prosecution.

By order of:

  
\_\_\_\_\_  
Jim Stewart, Interim Chief of Police

3-18-13  
\_\_\_\_\_  
Date