CITY OF ANDERSON POLICE DEPARTMENT
Anderson, South Carolina

DIRECTIVE TYPE General Order	EFFECTIVE DATE 12-01-2016	NUMBER 912.1
SUBJECT CJI MISUSE	REVISED 7-15-19	
REFERENCE	AMENDS/SUPERSEDES All Others	
DISTRIBUTION All Personnel	RE-EVALUATION DATE Annual	NO. PAGES 4

A. Purpose

The purpose of this policy is to provide employees, both sworn and civilian, of the City of Anderson Police Department with guidelines on the use of the N.C.I.C. database.

B. Policy

In support of the ***Anderson County Sheriff's Office Unified Emergency Communications Center (ACSO/UECC)*** mission of public service to the citizens of the city and county of Anderson, the ***ACSO/UECC*** provides the needed technological resources needed to the personnel of the City of Anderson Police Department to access FBI CJIS systems and information in support of this agency's mission. All agency personnel, with access to FBI Criminal Justice Information (CJI) or any system with stored FBI CJI have a duty to protect the system and related systems from physical and environmental damage and are responsible for correct use, operation, care and maintenance of the information. All technology equipment: computers, laptops, software, copiers, printers, terminals, MDT's, mobile devise, live scan devices, fingerprint scanners, software to include RMS/CAD, operating systems, etc. used to process, store, and/or transmit FBI CJIS is a privilege allowed by the ***ACSO/UECC*** , state CSO, and, the FBI. To maintain the integrity and security of the ***ACSO/UECC*** and the FBI's CJIS systems and data, this computer use privileges requires adherence of relevant federal, state, and local laws, regulations and contractual obligations. All existing laws and ***ACSO/UECC*** regulations and policies apply, including not only those

laws and regulations that are specific to computers and networks, but also those that may apply to personal conduct.

Misuse of computing, networking or information resources may result in temporary or permanent restriction of computing privileges up to employment termination. In some misuse situations, account privileges will be suspended to prevent ongoing misuse while under investigation. Additionally, misuse can be prosecuted under applicable statues. All files are subject to search. Where follow-up actions against a person or agency after an information security incident involves legal action(either civil or criminal), the evidence shall be collected, retained, and presented to conform to the rules of evidence laid down in the relevant jurisdiction(s). Complainants alleging misuse of ***ACSO/UECC*** computing and network resources and FBI CJIS systems and/or data will be directed to those responsible for taking appropriate disciplinary action.

Examples of Misuse with access to FBI CJI

1. Using someone else's login that you are not the owner.
2. Leaving the computer logged in with your login credentials unlocked in a physically unsecure location allowing anyone to access ***City of Anderson Police Department*** or ***ACSO/UECC*** systems and/or FBI/CJIS systems and data in your name.
3. Allowing unauthorized person(s) to access FBI CJI at any time for any reason. Note: Unauthorized use of the FBI CJI is prohibited and may be subject to criminal and/or civil penalties
4. Allowing remote access of ***City of Anderson Police Department*** or ***ACSO/UECC*** issued computer equipment to FBI CJIS systems and/or data without prior authorization by either the ***City of Anderson Police Department*** or ***ACSO/UECC.***
5. Obtaining a computer account that you are not authorized to use.
6. Obtaining a password for a computer account of another account owner.
7. Using either the ***City of Anderson Police Department*** or ***ACSO/UECC's*** network to gain unauthorized access to FBI CJI.
8. Knowingly performing an act which will interfere with the normal operation of FBI CJI systems.
9. Knowingly propagating a computer virus, Trojan horse, worm, and malware to circumvent data protection or compromising existing security holes to FBI CJIS systems.

10. Violating terms of software and/or operating system licensing agreements or copyright laws.
11. Duplication of licenses software, except for backup and archival purposes that circumvent copyright laws for use in either ***City of Anderson Police Department*** or ***ACSO/UECC,*** for home use or for any customers or contractor.
12. Deliberately wasting computing resources to include streaming audio, video for personal use that interferes with either the ***City of Anderson Police Department*** or ***ACSO/EUCC*** network performance.
13. Using electronic mail or instant messaging to harass others.
14. Masking the identity of an account or machine.
15. Posting materials publicly that violate existing laws or ***City of Anderson Police Department*** code of conduct.
16. Attempting to monitor or tamper with another user's electronic mail or files by reading, copying, changing or deleting without explicit agreement of the owner.
17. Using ***City of Anderson Police Department*** or ***ACSO/UECC's*** technology resources to advance unwelcome solicitation of a personal or sexual relationship while on duty or through the use of official capacity.
18. Unauthorized possession of, loss of, or damage to ***City of Anderson Police Department*** or ***ACSO/UECC*** technology equipment with access to FBI CJIS through unreasonable carelessness or maliciousness.
19. Maintaining FBI CJIS or duplicate copies of official ***City of Anderson Police Department or ACSO/UECC*** files in either manual or electronic formats in his or her place of residence or in other physically non-secure locations without express permission.
20. Using ***City of Anderson Police Department*** or ***ACSO/UECC*** technology resources and/or FBI CJIS for personal or financial gain.
21. Deliberately failing to report promptly any known technology-related misuse by another employee that may result in criminal prosecution or discipline under this policy.
22. Using personally owned devices on ***ACSO/UECC*** network to include personally-owned thumb drives, CD's, mobile devices, tablets on Wi-Fi, etc. Personally owned devices should not store ***City of Anderson Police Department or ACSO/UECC*** data, state data or FBI/CJIS

The above listing is not all-inclusive and any suspected technology resource or FBI CJIS system or FBI-CJI misuse will be handled by ***City of Anderson Police Department*** on a case by case basis. Activities will not be considered misuse when authorized by the appropriate by either ***City of Anderson Police Department or ACSO/UECC*** officials for security or performance testing.

Privacy Policy

All ***City of Anderson Police Department*** personnel utilizing agency-issued technology resources funded by ***ACSO/UECC*** expressly acknowledges and agrees that such service, whether for business or personal use, shall remove any expectation of privacy. Use of ***ACSO/UECC*** systems indicates consent to monitoring and recording. The ***ACSO/UECC*** reserves the right to access and audit any and all communications including electronic and physical media at rest, in transit, and at end of life ***ACSO/UECC*** personnel shall not store personal information with an expectation of personal privacy that are under the control and management of ***ACSO/UECC.***

Personal use of Agency Technology

The computers, electronic media and services provided by either the ***City of Anderson Police Department or ACSO/UECC*** are primarily for business use to assist personnel in the performance of their jobs. Limited, occasional or incidental use of electronic media (sending or receiving) for personal non-business purposes is understandable and acceptable, and all such use should be done in a manner that does not negatively the system's use for their business purposes. However employees are expect to demonstrate a sense of responsibility and abuse this privilege.

Misuse Notification

Due to the increase in the number of accidental or malicious computer attacks against both government and private agencies, the ***City of Anderson Police Department*** shall: establish an operational incident handling capability for all information systems with access to FBI CJIS systems and data. This includes adequate preparation, detection, analysis, containment, recovery, and user response activities; (ii) track, document, and report incidents to appropriate agency officials and/or authorities.

By order of:

Jim Stewart, Chief of Police

7-15-19
Date