

Security Awareness For Non-Computer Users of CJI

Criminal Justice Information (CJI) is information provided by FBI CJIS and/or KCJIS necessary for agencies to perform their missions. It includes Criminal History Record Information (CHRI) and Personally Identifiable Information (PII). PII can be used to distinguish or trace an individual's identity (ie. date and place of birth, or mother's maiden name). You may also have information about the personnel, procedures and systems used to carry out the agency's mission. All of this information is sensitive and confidential and must be protected.

Responsibilities and expected behavior with regard to CJI usage This agency provides information to personnel as needed in order to complete their work assignments. Don't ask for or accept information unless you need it to complete your work. You are responsible to safeguard information you receive to prevent unauthorized access, use or dissemination of it.

Penalties for noncompliance Misuse or disclosure of CJI and other sensitive information may result in disciplinary action, including immediate dismissal, civil and criminal penalties including confinement and fines up to \$11,000 in accordance with: Title 28, Part 20, Code of Federal Regulations; state statutes, FBI and KCJIS Policies.

Threats, vulnerabilities, and risks associated with and Proper handling and marking of CJI Unprotected information is vulnerable to alteration, destruction or illegal/improper dissemination and use. You are responsible to protect any information you receive. Use folders or envelopes marked in a way you know is confidential and protected from prying eyes.

Media protection You are responsible to keep all media containing agency information safe! Most media can be misplaced or easily concealed by thieves. Beware of environmental threats. Some paper is sensitive to sunlight. Extreme heat is harmful to most media. Static electricity may adversely affect some media. Water will destroy the usefulness of most media.

Protect information subject to confidentiality concerns — hardcopy through destruction CJI and agency information must be treated with confidentiality. Don't let unauthorized people read any printouts or browse files on CDs or flash drives. Once you're finished with agency information it should be returned to the proper agency location and personnel for secure storage or destroyed.

Dissemination and destruction Dissemination of information to other people is only authorized if (a) the other person has a legitimate need and is authorized to receive such information, or (b) the other person is performing personnel and appointment functions for criminal justice employment applicants.

Physical media must be *destroyed by shredding or incineration* when no longer required.

Social engineering Beware of people that may be trying to trick you to get information from you! Do not respond to phone calls, email, or other requests for information until you have personally and physically verified they are who they say and that they are authorized to receive information.

Visitor control and physical access to spaces Be aware of your surroundings when using agency information. Know everyone entering your space and don't let anyone (even family and friends) see what you are working on unless they are authorized by the agency to see it. Put all printouts and media into locked containers when not using it. Know what to do and who to call if strangers appear.

Incident response (Points of contact; Individual actions) Report any situation you suspect may be a security risk to your agency supervisor or other responsible agency personnel immediately!

Security Awareness For Non-Computer Users of CJI

Please answer the following True or False questions to determine your understanding of the topics discussed on page 1.

Please Print:		
		_____ Date
_____ First Name	M.	_____ Last Name
_____ Agency		
_____ ORI		

- _____ 1. You are responsible to take care of information you receive to prevent unauthorized access, use or dissemination of it.
- _____ 2. Misuse of CJI may result in disciplinary action, including immediate dismissal, civil and criminal penalties including confinement and fines up to \$11,000.
- _____ 3. Unprotected information is vulnerable to alteration, destruction or illegal/improper dissemination and use. You are responsible to protect any information you receive.
- _____ 4. Folder or envelopes containing CJI should not be marked. It is a security theory called “security through obscurity”.
- _____ 5. You’re responsible to keep all media safe from being misplaced, stolen, or environmental dangers.
- _____ 6. You should not let unauthorized people read any printouts. Information should be returned to the agency for secure storage or destroyed.
- _____ 7. Dissemination of information to another person can be authorized if that person has a legitimate need for knowing the information.
- _____ 8. To avoid being a victim of social engineering, don’t respond to any requests for sensitive information until you have personally and physically verified they are who they say and that they are authorized to receive information.
- _____ 9. When in your personal work space, you can focus closely on sensitive information without a need to worry about your surroundings.
- _____ 10. Report any situation you suspect may be a security risk to your agency supervisor or other responsible agency personnel immediately!