

Security Awareness Acknowledgment

In the course of carrying out this agency's mission, Criminal Justice Information (hereafter referred to as CJI) is collected on individuals that may include, but is not limited to, criminal history record information, notations of arrest, detention, release, or other formal criminal charges; and any disposition arising from them, driving records, addresses, birthdates, social security numbers, personal descriptors and other personal information. Any information, whether on an official agency report, computer screen, printout, etc., sufficient to identify individuals and notations regarding any criminal justice transaction, as well as information regarding the systems used to access CJI and the Kansas Criminal Justice Information System (KCJIS) is considered sensitive and confidential and must be protected.

Your authorization to access CJI is based on your official duties and roles in association with this criminal justice agency as marked below.

- Direct Access Authorized.** You may personally use information systems to directly request CJI or have CJI provided to you. You may use or disseminate criminal and/or juvenile history record information and other official documents, such as investigative files, intelligence data, driver's license information, vehicle registrations and other confidential work related documents. *You are required to read and sign this document and undergo additional Security Awareness Training to be familiar with the agency and KCJIS policies regarding systems use and security policies to protect CJI and other sensitive information.*
 - The use of this information must be necessary for work assignments to be completed or for proper dissemination and cannot be obtained for a personal desire to know.

- Direct Access Not Authorized.** You will not personally use information systems to request CJI. However in your role with this agency you may:
 - Have need to use CJI that was obtained by others (indirect access)
 - Use computer equipment on a network with the capability to access CJI.
 - Be inadvertently exposed to CJI.*You are required to read and sign this document and undergo additional Security Awareness Training to be familiar with the agency and KCJIS policies regarding systems use and security policies to protect CJI and other sensitive information.*
 - Your receipt and use of CJI must be necessary for work assignments to be completed and cannot be obtained or used for your personal benefit.

- CJI Access Not Authorized** Your association with this agency does not involve access to CJI in any format or access to systems that may be used to access CJI and furthermore does not constitute a "right to know" for any law enforcement sensitive information. However, you may be exposed to such information through your involvement with this agency. *You are required to read and sign this document.*

Because not all security threats involve technology, **all** personnel granted access to facilities where CJI is used must be aware of some basic security principals as follows.

- Dissemination or disclosure of any information seen, heard, or otherwise obtained through your agency association to anyone outside of this agency is prohibited except when necessary for the administration of criminal justice, and for criminal justice agency employment. And then only in accordance with Title 28, Part 20, Code of Federal Regulations, FBI and KCJIS Policy and Procedures. ***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.***

Security Awareness Acknowledgment

- Only personnel who have successfully been screened using a finger-print based record check and other investigative tools to determine appropriate access are authorized for unescorted access to some areas of the facilities or to have access to data processing systems that may process, store, or transmit CJI. Visitors are individuals who have not undergone the screening procedures and must be escorted in restricted areas. ***You should be familiar with how restricted access areas are identified, how authorized personnel are identified, and the proper procedures to safely challenge and report unknown unescorted persons.***
- Social Engineering occurs when individuals present themselves as someone they are not such as a repairman, or other service personnel and engage personnel in various communications channels (phone, email, or personal) in hopes of collecting information regarding individuals, events, or details of technologies in use, etc. ***To prevent Social Engineering, never discuss ANY agency information with anyone other than authorized agency personnel known to you.***
- To prevent unauthorized access, misuse or pre-mature destruction of media (printed documents, hard drives, compact discs, etc.). All media must be stored in a secure manner when not in use until it is no longer needed and is properly sanitized or disposed of according to KCJIS Policies and Procedures. ***If you notice media that appears to be out of place you should alert your agency supervisor or other responsible agency personnel immediately.***
- Unattended file storage and telecommunications wiring areas should be locked at all times.
- Be aware of environmental hazards such as storing media near heat sources or liquids. Excessive heat, humidity, or other climate extremes may be harmful to electronic systems and media. Overloaded electrical circuits (too many or too big of a device plugged into power strips) may cause power outages or fire and render systems unavailable. ***If you encounter extreme environmental conditions, alert your supervisor or other responsible agency personnel immediately.***

Report any situation you suspect may be a security risk to your agency supervisor or other responsible agency personnel immediately!

Failure to protect information and systems may be a risk to public safety or expose the agency and personnel to litigation, and loss of public confidence in the agency. That is why it is EVERYONE's responsibility to ensure the protection of information used in the operations of this agency.

Your signature below certifies that you:

- ✓ Have read this document,
- ✓ Agree to abide with the provisions of this document and other relevant documents,
- ✓ Understand the consequences of violating agency, KCJIS or FBI security policies.

Associate Signature

Date

Printed Name

Agency Name

Check box when Personnel screening checks are complete.

Date

Initials