CYBER SECURITY newsletter

CRIMINAL JUSTICE

Problem

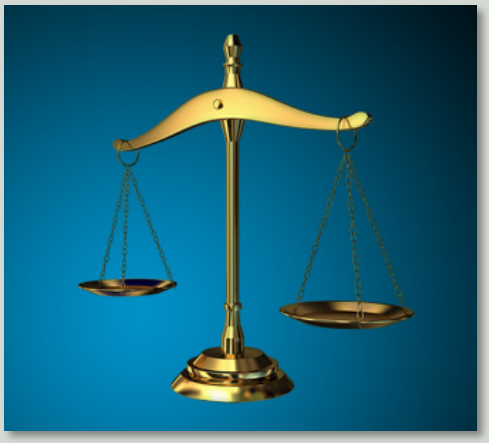
The information in our criminal justice system must be kept secure and confidential. Law enforcement decisions depend on data reliability and integrity. While sharing of information is necessary within the criminal justice community, controls must prevent information from falling into the wrong hands. Disclosure to the wrong people can threaten investigations and harm innocent people.

Solution

Disclosure to the wrong people can threaten investigations and harm innocent people. As a trusted member of the criminal justice community, and to ensure we remain compliant with rules and regulations, you should follow these guidelines for handling information.

Be on the lookout for people or activities that can abuse the information in our systems. If you witness people, even police officers or members of your department, looking at records without authority say something to higher management or your security team.

Do not share information or access to computer systems outside approved procedures. It may be tempting to help a friend who is curious about this case or that person, but until your friend gets authority that information is off-limits to him. If he really needs the information, he will be able to obtain the authorization he needs.



Criminal Justice

A fair and orderly system of criminal justice is central to our democracy. As a trusted member of the criminal justice community, and to ensure we remain compliant with rules and regulations, you should follow these guidelines for handling information.

University of Colorado
Boulder | Colorado Springs | Denver | Anschutz Medical Campus

This newsletter is published by the University of Colorado Office of Information Security. For more information please send email to security@cu.edu or visit https://www.cu.edu/information-privacy-and-security

Misconduct Cases

Law enforcement personnel have been punished for inspecting official records without authority. Unfortunately for some, the temptation to look at files regarding family, enemies or celebrities has been too great. Three cases:

1. Prosecutors filed criminal charges against Jacqueline Hankle, a latent fingerprint examiner employed by the New York State Division of Criminal Justice Services, for unlawfully accessing confidential databases. She especially focused on records of her nephew's ex-wife.

2. Toronto Police Sargent Wayne Lakey faced criminal charges for conducting background searches on his neighbors.

3. University of Florida Police arrested one of their officers, Adam Paul Treinen, on charges that he inspected the records of a former girlfriend (with whom he had fathered a child) and her boyfriend.

Access to law enforcement computers without justification can end an employee's career and even lead to a criminal conviction and incarceration.

Respect data classifications. When you come in contact with information that is marked or intended for other people and not you, stop looking at it or listening to it.

Use common sense. The entry of false data into our information systems can cause great damage. Lives and reputations can be at stake. If you are not sure about the accuracy of data, then ask questions or make your suspicions known to a supervisor or other responsible people.

Be skeptical. When someone contacts you claiming to be an officer looking for information or help in accessing a computer system, make sure you really know who they are. Watch for tricks. You do not want the local television news to announce that they tricked you into revealing details about a pending investigation.

Keep quiet. It is your job to deal with a lot of sensitive information. It is not your job to spread that information as rumors and gossip.

Effective law enforcement is about vigilance. We must always remember that someone is waiting to take advantage, waiting to steal a laptop from a patrol car or eavesdrop on official communications. You must always take security precautions. Make sure doors are locked. Turn computers or communications devices off when they are not in use. Guard log-on credentials. Actively think about how hidden cameras or listening devices could be snuck into your work area.

Pay attention to security risks. If you see a shortcoming, you should recommend how procedures can be improved.

A fair and orderly system of criminal justice is central to our democracy. As electronic data assumes an ever-greater place in that system, it is your duty to protect that data from misuse.