WISCONSIN DEPARTMENT OF JUSTICE

SECURITY AWARENESS TRAINING
Non-Criminal Justice Agencies

System Security

In our increasingly digital and technologically dependent world security of private and protected information, such as criminal justice information, is a major concern. This Security Awareness training is a means to provide individuals with information about best practices and minimum requirements necessary for securely accessing, processing, and storing criminal justice information.

Data stored in the Crime Information Bureau and Interstate Identification Index criminal history record databases are documented criminal justice records or administrative records containing sensitive personal information. These records must be protected from those who would try to gain unauthorized access to the records and those who would use information obtained from the records for unauthorized purposes.

The FBI requires *minimum* information security requirements to protect information sources, transmission, and storage of criminal justice information. Each agency and user accessing criminal justice information or systems used to access or store criminal justice information is responsible for ensuring the security of their systems and criminal justice information. This training covers these requirements and completion of this training is one of them.

Authorized Personnel

Agencies must restrict access to criminal justice information and systems that process or store criminal justice information to only those personnel with the business need and authority to see, review, and receive criminal justice information.

System Usage

Criminal justice information is only to be used for the purpose specified under the applicable state or federal law under which access was granted. Re-dissemination of criminal justice information is strictly prohibited. A system use notification message must be displayed on all information systems that access criminal justice information as required by FBI policies.

Physical Access & Visitors

Personnel should be aware of their surroundings and take steps to ensure unauthorized persons do not access criminal justice information or the systems used to access or store criminal justice information. This may include challenging or questioning unescorted subjects, verifying credentials of strangers, and/or ensuring visitors and other unauthorized users are not looking over someone's shoulder to get information. Numerous techniques and tools exist to help ensure the security of data. These may include the use of screensavers, screen shields, device (e.g. computer) location and positioning, etc.

Using publicly accessible computers to access, process, store or transmit criminal justice information is prohibited. Publicly accessible computers include but are not limited to hotel business center computers, convention center computers, public library computers, public kiosk computers, etc.

Logins

A unique login ID is required for everyone who is authorized to store, process, and/or transmit criminal justice information. This includes all persons who administer and maintain the system/network that accesses and/or transmits criminal justice information. Users are required to uniquely identify themselves before they are allowed to perform any actions on the system.

A system use notification message must be displayed on all information systems that access criminal justice information as required by FBI policies. *Users should protect their logins and not share them with anyone.* Users are responsible for any and all system activity that happens under their login.

If a user is unable to login after 5 consecutive invalid access attempts, their account will be automatically locked for at least 10 minutes unless released by an administrator. In addition, the system will initiate a session lock after a maximum of 30 minutes of inactivity. The session lock will remain in effect until the user once again establishes access using appropriate login and authentication.

Passwords

Passwords used to access the criminal justice information, or the systems used to access or store criminal justice information must meet criteria to be secure passwords. Passwords must meet one of two sets of criteria. The Basic Password Standards or the Advanced Password Standards. The criteria for both standards can be found in FBI requirements.

Users should protect their passwords and not share them with anyone.

System users should be aware of subjects attempting to obtain computer system access or password/login information by using ‘social engineering’. Social engineering means manipulating people into doing something or divulging confidential information. This may include emails from unknown sources, email attachments containing spyware programs, telephone callers purporting to be from another authorized agency, etc. When in doubt, users should verify the source or identity behind the email, telephone call, etc. before potentially misusing system resources or providing criminal justice information to unauthorized subjects.

Proper Handling of Criminal Justice Information

Criminal justice information, whether in paper form or saved digitally, must be stored in a secure area inaccessible to the public.

Criminal justice information should remain in the secure area unless there is specific authorization and procedures for taking the information out of the secure area. When criminal justice information (paper or digital) is transported outside of the secure areas it must continue to be protected, thus transport of criminal justice information is restricted to authorized personnel.

Criminal justice information must be securely disposed of when no longer needed. Destruction of paper information may be accomplished by shredding, incineration, etc. Digital media storing criminal justice information (hard drives, flash drives, CD’s, etc.)

must be sanitized or degaussed using approved sanitizing software that ensures a minimal 3-pass wipe. Inoperable digital media should be destroyed (cut up, smashed, shredded, etc.). The disposal or destruction of criminal justice information must be witnessed or carried out by authorized personnel to avoid the possibility of inadvertent release of system information to unauthorized persons.

Dissemination of Criminal Justice Information

Information received under this agreement shall only be used for the purpose specified under the applicable state or federal law under which access was granted. Criminal justice information acquired under this agreement shall not be used for any other purpose. Re-dissemination of criminal justice information acquired under this agreement is strictly prohibited. Any misuse of this information or violations of these understandings and policies jeopardizes the availability of information for all participating agencies. The undersigned agency will promptly notify the Crime Information Bureau of any potential misuse or violation of this agreement.

Security Incidents & Response

A security incident is a violation or possible violation of policy that threatens the confidentiality, integrity or availability of criminal justice information. There has been an increase in the number of accidental or malicious computer attacks against both government and private agencies, regardless of whether the systems are high or low profile. Indicators of a security incident may include system crashes without a clear reason, new files with novel or strange names appearing, changes in file lengths or modification dates, unexplained poor system performance, etc.

Personnel should know how to report a security incident, who to report an incident to, when to contact that person, and what basic actions to take in case of a suspected compromise of the system. This may include contacting a supervisor, contacting on-call information technology staff, disconnecting the affected computer from the network, etc.

Agency staff should document any security incidents/possible security incidents, and promptly report incident information to the Crime Information Bureau. Evidence of the security incident may need to be collected and retained to conform to the rules of evidence in case of legal action (either civil or criminal).

Agencies must monitor physical access to the information system to detect and respond to physical security incidents, and wherever feasible the agency shall employ automated mechanisms to make security alert and advisory information available throughout the agency as appropriate.

Virus/Spam/Spyware & Malicious Code Protection

To ensure information security, agencies are required to have in place malicious code protection, virus protection, spam protection and spyware protection on the devices or systems used to access or store criminal justice information. Users should be cautious when downloading internet content or clicking on web-based pop-ups/windows, unknown emails, email attachments or embedded objects. Removable devices such as flash drives, CDs, etc. may also possibly introduce viruses/malware and caution should be used before they are introduced to the system. Follow your agency’s policies regarding use of such items.

Technical Considerations

Mobile Devices – Handheld Devices, Laptops, etc.

As digital handheld devices continue to become more integrated into the mobile workforce, security measures must be employed since such devices may be used outside of physically secure locations. Wireless devices, even in physically secure areas, are susceptible to penetration, eavesdropping and malware. Furthermore, compromised or lost wireless devices may introduce risk to the overall security of an agency's network, criminal justice information, or the systems used to access or store criminal justice information. The use of digital handheld devices and/or laptops to access criminal justice information is allowed, provided the agency implements the security requirements for such access as outlined in FBI policies. This would include advanced authentication, encryption, security-related updates, official use guidance, data at rest encryption, and prevention of data compromise in case of possible loss of the device. The requirement to use or not use advanced authentication is dependent upon the physical, personnel and technical security controls associated with the user location as specified in FBI policies.

All personnel of the undersigned agency are prohibited from accessing, processing, storing or transmitting criminal justice information from publicly accessible computers (i.e. hotel business centers, public library computers, etc.) and personally owned devices.

A personal firewall must be employed on all devices that are mobile by design (i.e. laptops, handhelds, personal digital assistants, etc.).

Account Management

User logins/accounts should be kept current. When a user is terminated, leaves employment or job duties no longer require criminal justice information access the user's system account should be disabled. An agency must validate system accounts at least annually.

User accounts will be assigned according to the principle of 'least privilege'. Least privilege means giving a user account only those privileges which are essential to perform assigned duties. Assigned authorizations will control access to the system and system information.

Users may only have one active computer session accessing criminal justice information at a time. Multiple concurrent active sessions for one user are prohibited unless the agency can document a business need for such multiple session access.

System Updates

Malicious code protection, virus protection, spam protection and spyware protection must be in place at critical points throughout the networks and on all workstations, servers, and mobile computing devices on the network. Malicious code protection must be enabled and must include automatic updates for all systems with Internet access. Agencies with systems not connected to the Internet must implement local procedures to ensure malicious code protection is kept current (i.e. most recent definitions update available). Resident scanning must be employed.

Agencies must monitor applications, services, and information systems containing software or components affected by recently announced software flaws and potential vulnerabilities resulting from those flaws. System patches shall be installed in a timely manner.

Backup & Storage Procedures

Agencies must consider the requirements for secure storage of digital media and hardware containing criminal justice information, and ensure that such backup procedures, archiving, and storage, whether centralized or de-centralized (off site) meet the security requirements outlined in FBI policies.

System Security Awareness Certification Statement

I certify that I have read and understand the contents of the Security Awareness Non-Criminal Justice Agencies training and agree to follow all FBI requirements regarding the proper access to, use of, storage, and disposal of criminal justice information or systems used to access or store criminal justice information.

I understand that criminal justice information is sensitive and has potential for great harm if misused; therefore, access to this information is limited to authorized personnel. I understand that misuse of criminal justice information or systems used to access or store criminal justice information may subject me to system sanctions/penalties and may also be a violation of state or federal laws, subjecting me to criminal and/or other penalties. Misuse of the criminal justice information or systems used to access or store criminal justice information includes accessing the systems without authorization or exceeding my authorized access level, accessing the systems for an improper purpose, using or disseminating information received from the systems for a non-work related or unauthorized purpose, etc.

Your signature:____

Print your name:____

Agency name:____

Date:____