



# **WISCONSIN TIME SYSTEM**

**Training Materials**

---

## **TIME SYSTEM SECURITY AWARENESS HANDOUT**

---

Revised 1/12  
2012 Security Awareness Handout V2



# **SYSTEM SECURITY**

Data service agencies have agreed to make information available to law enforcement and criminal justice via the TIME and NCIC Systems for the specific purpose of facilitating the administration of criminal justice. This information must be protected to ensure correct, legal and efficient dissemination and use. Any misuse of this information or violation of the understandings and policies of the system jeopardizes the availability of information for all participating agencies. The systems and the information contained therein must be protected from possible physical, natural and hardware vulnerabilities. The FBI's CJIS Security Policy establishes minimum information security requirements, guidelines, and agreements reflecting the will of law enforcement and criminal justice agencies for protecting the sources, transmission, storage, and generation of criminal justice information. The TIME System has adopted the CJIS Security Policy as the TIME System security policy.

## **System Usage**

Users should use the terminal only for those purposes for which they are authorized. The TIME System and CIB/NCIC information is only to be used by authorized law enforcement/criminal justice personnel for law enforcement/criminal justice purposes. Each criminal justice agency authorized to access the TIME/NCIC Systems shall have a written policy for discipline of policy violators. Individuals and agencies are subject to system sanctions for policy violations. Misuse of the TIME System or information obtained from it may be a violation of state or federal laws, and individuals and agencies may be subject to criminal/other penalties.

Any individual authorized to use the TIME System who receives a request for TIME System information from another individual must ensure the person requesting the information is authorized to receive the data. Each data service has its own rules for secondary dissemination of records, which may include requirements for logging, identification of the purpose of the request, and identification of the specific individual receiving the record. Most records may be legitimately disseminated to another criminal justice employee/agency when the purpose of the request is criminal justice related.

Records obtained via the TIME/NCIC systems must be stored in a secure records environment, inaccessible to the public. All records must be properly disposed of by shredding, incineration, degaussing, or another appropriate secure method. Rediscovery of an existing TIME System response contained within a file of the criminal justice agency, when that file is subject to a public records request, must comply with rediscovery restrictions for data sources, the Wisconsin Public Records Law, and other applicable law.

An FBI authorized Originating Agency Identifier (ORI) shall be used in each transaction to identify the agency / user making the request to ensure the proper level of access for each transaction.

## **Physical Access**

Agencies must control physical access to devices that display criminal justice information and shall position information system devices in such a way as to prevent unauthorized individuals from accessing and viewing criminal justice information.

A physically secure location is a criminal justice facility, area, room, group of rooms within a criminal justice agency, or that are under the control of a criminal justice agency through a signed management control/security addendum agreement.

TIME System terminals in police vehicles must be protected with additional security such as advanced authentication and FIPS 140-2 compliant encryption. A police vehicle is defined as an *enclosed* criminal justice conveyance. So while a squad car would meet this definition, a patrol motorcycle would not.

Agencies must control all physical access points (except for those areas within the permanent facility officially designated as publicly accessible) and shall verify individual access authorizations before granting access. The agency shall develop and keep current a list of personnel with authorized access to the physically secure location or shall issue credentials to authorized personnel.

Utilizing 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.

## **Visitors**

Agencies must control physical access by authenticating visitors before authorizing escorted access to the physically secure location. The agency shall escort visitors at all times and monitor visitor activity. The agency must maintain visitor access records to the physically secure location that include name and agency of the visitor, signature of the visitor, form of identification, date of access, time of entry and departure, name and agency of person visited and visit purpose. These visitor access records should be frequently reviewed for accuracy and completeness, and the visitor access records shall be maintained for a minimum of one year.

System users should be aware of their surroundings and take steps to ensure unauthorized users do not access criminal justice information or the TIME/NCIC Systems. This may include challenging or questioning unescorted subjects, verifying credentials of strangers, and/or ensuring visitors and other unauthorized users are not 'shoulder surfing' (shoulder surfing refers to using direct observation techniques, such as 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, terminal location and positioning, etc. Each agency and user accessing the system is responsible for ensuring the security of the system and criminal justice information.

## **Authorized Users/Logins**

Thorough background screening by the employing agency of personnel is required. State and national criminal history record checks by fingerprint identification must be conducted within 30 days upon initial employment or assignment for all personnel who have authorized access to FBI CJIS Systems or data and those who have direct responsibility to configure and maintain computer systems and networks with direct access to FBI CJIS Systems. The minimum check must include submission of completed applicant fingerprint cards to the FBI CJIS Division and the CIB through the state identification bureau. CIB and NCIC Wanted Person Files must also be checked. Sworn personnel who have been fingerprinted and certified by the law enforcement standards board already meet this requirement. Background re-investigations are recommended every 5 years as good business practice.

When identification of the applicant or employee has been established by fingerprint comparison and he/she appears to be a wanted person or to have an arrest history for a felony or serious misdemeanor, the employing agency must delay granting NCIC access until the matter is reviewed by the CJIS Systems Officer (CSO) or designee. If a felony conviction of any kind exists, the hiring authority in the agency shall deny systems access. However, the hiring authority may ask for a review by the CSO in extenuating circumstances where the severity of the offense and the time that has passed would support a possible variance. Other offenses may be disqualifying at the discretion of the agency or the CSO. (Note: A denial of NCIC access may not be sufficient grounds for denial of employment. Agencies must consider the provisions of Chapter 111, Wisconsin Statutes, relating to employment discrimination). If the person already has access to CJIS systems and is subsequently arrested and or convicted, continued access to CJIS shall be determined by the CSO.

Each individual who is authorized to store, process, and/or transmit criminal justice information shall be uniquely identified. A unique identification shall also be required for all persons who administer and maintain the system(s) that access criminal justice information or networks leveraged for criminal justice information transit. The unique identification can take the form of a full name, badge number, serial number, or other unique alphanumeric identifier. Agencies shall require users to identify themselves uniquely before the user is allowed to perform any actions on the system. Agencies shall ensure that all user IDs belong to currently authorized users. Identification data shall be kept current by adding new users and disabling and/or deleting former users.

Where technically feasible, the system shall enforce a limit of no more than 5 consecutive invalid access attempts by a user attempting to access criminal justice information or systems with access to criminal justice information. The system will automatically lock the account for at least a 10 minute period unless released by an administrator.

The information system shall initiate a session lock after a maximum of 30 minutes of inactivity, and the session lock remains in effect until the user reestablishes access using appropriate identification and authentication procedures. Users can directly initiate session lock mechanisms to prevent inadvertent viewing when a device is unattended. A session lock is not a substitute for logging out of the information system. In the interest of officer safety, devices that are: (1) part of a police vehicle; or (2) used to perform dispatch

functions and located within a physically secure location, are exempt from this requirement. Note: an example of a session lock is a screen saver with password.

By logging in to and accessing the system and the information contained therein, users are signifying their agreement to abide by all system policies and procedures and acknowledging the possible consequences of misuse of system resources or criminal justice information.

## **Passwords**

Passwords used to access criminal justice information systems must have secure password attributes. Passwords must be a minimum length of 8 characters, must not be a dictionary word or proper name, cannot be the same as the userid. Passwords must expire within a maximum of every 90 calendar days and cannot be identical to the previous ten (10) passwords. Passwords cannot be displayed on screen when entered, and must not be transmitted in the clear outside the secure location.

System users should be aware of subjects attempting to obtain computer system access or password/login information by using 'social engineering'. Social engineering is the act of manipulating people into performing actions or divulging confidential information, rather than by breaking in or using technical hacking techniques. 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, system 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.

## **Information Storage & Disposal**

The agency shall securely store physical media/system printouts within physically secure locations or controlled areas. The agency shall restrict access to physical media to authorized individuals. During transport out side of controlled areas, the agency shall protect and control physical media and restrict the transport of such media to authorized personnel.

Physical media shall be securely disposed of when no longer needed. Formal procedures for the secure disposal or destruction of physical media shall minimize the risk of sensitive information compromise by unauthorized individuals. Physical media shall be destroyed by shredding, incineration, etc. Agencies shall ensure the disposal or destruction is witnessed or carried out by authorized personnel.

## **Incident Response**

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. Agencies shall: (i) establish an operational incident handling capability for agency information systems that includes adequate preparation, detection, analysis, containment, eradication, recovery, and user response activities; (ii) track, document, and report incidents to appropriate agency officials and/or authorities. The agency shall monitor physical access to the information system to detect and respond to physical security incidents.

Where a follow-up action against a person or an agency after an information security incident involves legal action (either civil or criminal), evidence shall be collected, retained and presented to conform to the rules of evidence.

An agency shall track and document information system security incidents on an ongoing basis. The agency shall promptly report incident information to the Crime Information Bureau. Information security events and weaknesses associated with information systems shall be communicated in a manner allowing timely corrective action to be taken. Formal event reporting and escalation procedures shall be in place. Wherever feasible, the agency shall employ automated mechanisms to assist in the reporting of security incidents. All employees, contractors and third party users shall be made aware of the procedures for reporting the different types of event and weakness that might have an impact on the security of agency assets and are required to report any information security events and weaknesses as quickly as possible to the designated point of contact.

## **Controlling Hardware/Electronic Media**

The agency shall authorize and control information system-related devices entering and exiting the physically secure location. In addition, the agency shall control physical access to information system distribution and transmission lines within the physically secure location.

The agency shall securely store hardware/electronic media within physically secure locations or controlled areas. The agency shall restrict access to electronic media to authorized individuals. The agency shall protect and control electronic media during transport outside of controlled areas and restrict the transport of such media to authorized personnel.

Prior to disposal or release for reuse of electronic media, the agency shall sanitize or degauss the electronic media. Inoperable electronic media shall be destroyed (cut up, shredded, etc.). The agency shall maintain written documentation of the steps taken to sanitize or destroy electronic media. Agencies shall ensure the sanitization or destruction is witnessed or carried out by authorized personnel.

## **Virus/Spam/Spyware & Malicious Code Protection**

The agency shall implement malicious code protection that includes automatic updates for all systems with Internet access. Agencies with systems not connected to the Internet shall implement local procedures to ensure malicious code protection is kept current (i.e. most recent update available). The agency shall employ virus protection mechanisms to detect and eradicate malicious code (e.g., viruses, worms, Trojan horses) at critical points throughout the network and on all workstations, servers and mobile computing devices on the network. The agency shall ensure malicious code protection is enabled on all of the aforementioned critical points and information systems and resident scanning is employed.

The agency shall implement spam and spyware protection. The agency shall employ spam protection mechanisms at critical information system entry points (e.g., firewalls, electronic mail servers, remote-access servers), shall employ spyware protection at workstations, servers or mobile computing devices on the network, and use the spam and spyware protection mechanism to detect and take appropriate action on unsolicited messages and spyware/adware, respectively, transported by electronic mail, electronic mail attachments, Internet access, removable media (e.g., diskettes or compact disks) or other removable media.

The agency shall identify applications, services, and information systems containing software or components affected by recently announced software flaws and potential vulnerabilities resulting from those flaws.

The agency shall receive information system security alerts/advisories on a regular basis, and issue alerts/advisories to appropriate personnel. The agency shall document the types of actions to be taken in response to security alerts/advisories and take appropriate actions in response. The agency shall employ automated mechanisms to make security alert and advisory information available throughout the agency as appropriate.

## **Controlling Access to System**

The agency shall manage information system accounts (establishing, activating, modifying, reviewing, disabling, and removing accounts). The agency shall validate information system accounts at least annually and shall document the validation.

The agency shall approve individual access privileges and shall enforce physical and logical access restrictions associated with changes to the information system; and generate, retain, and review records reflecting all such changes. The agency shall assign the most restrictive set of rights/privileges or access needed by users for the performance of specific tasks. The agency shall implement least privilege based on specific duties, operations, or information systems as necessary to mitigate risk to criminal justice information. Logs of access privilege changes shall be maintained for a minimum of one year or at least equal to the agency's record retention policy – whichever is greater.

The information system shall enforce assigned authorizations for controlling access to the system and contained information. The information system controls shall restrict access to privileged functions (deployed in hardware, software and firmware) and security-relevant information to explicitly authorized personnel.

Access controls must be in place and operational for all IT systems to: prevent multiple concurrent active sessions for one user identification, for those application accessing criminal justice information, unless the agency grants authority based upon operational business needs. Agencies shall document the parameters of the operational business needs for multiple concurrent active sessions. Access controls must also ensure only authorized personnel can add, change, or remove component devices, dial-up connections and remove or alter programs.

Agencies shall control access to criminal justice information based on one or more of the following: job assignment or function, physical location, logical location, network addresses, time-of-day and day-of-week/month.

Access controls shall use one or more of the following: Access Control Lists (ACLs), resource restrictions (i.e. menus, database views and network devices), encryption, or controlling access at the application level.

### **Technical Considerations**

Each agency having access to CJIS data through their own network must designate someone as Local Agency Security Officer (LASO). The LASO is responsible for identifying who is using the CJIS Systems Agency (CSA) approved hardware/software/firmware and ensure that no unauthorized individuals or processes have access to the same. The LASO must identify and document how the equipment is connected to the state system. The LASO is responsible for ensuring that personnel security screening procedures are being followed, and ensuring the approved and appropriate security measures are in place and working as expected. The LASO is also responsible for supporting policy compliance and ensuring that the CSA / Information Security Officer (ISO) is promptly informed of security incidents.

The agency shall ensure that a complete topological drawing depicting the interconnectivity of the agency network to criminal justice information systems and services is maintained in a current status. The network topological drawing must at least include the following:

- All communication paths, circuits and other components used for the interconnection, beginning with the agency owned system(s) and traversing through all interconnected systems to the agency end-point.
- The logical location of all components (e.g. firewalls, routers, switches, hubs, servers, encryption devices, and computer workstations). Individual workstations (clients) do not have to be shown; the number of clients is sufficient.

- “FOR OFFICIAL USE ONLY” markings.
- The agency’s name and date (day, month, and year) drawing was created or updated.

Advanced authentication provides for additional security to the typical user identification and authentication of login ID and password, such as: biometric systems, user-based public key infrastructure (PKI), smart cards, software tokens, hardware tokens, paper (inert) tokens, or “Risk-based Authentication” that includes a software token element comprised of a number of factors, such as network information, user information, positive device identification (i.e. device forensics, user pattern analysis and user binding), user profiling, and high-risk challenge/response questions. The requirement to use or not use advanced authentication is dependent upon the physical, personnel and technical security controls associated with the user location.

When criminal justice information is transmitted outside the boundary of the physically secure location, the data shall be immediately protected via cryptographic mechanisms (encryption). Encryption shall be a minimum of 128 bit. When encryption is employed, the cryptographic module used shall be certified to meet FIPS 140-2 standards. For agencies using public key infrastructure technology, the agency shall develop and implement a certificate policy and certification practice statement for the issuance of public key certificates used in the information system. Registration to receive a public key certificate shall include authorization by a supervisor or a responsible official, be accomplished by a secure process that verifies the identity of the certificate holder, and ensure the certificate is issued to the intended party.

A personal firewall shall be employed on all devices that are mobile by design (i.e. laptops, handhelds, personal digital assistants, etc.). For the purpose of this policy, a personal firewall is an application that controls network traffic to and from a computer, permitting or denying communications based on policy. At a minimum, the personal firewall must manage program access to the Internet, block unsolicited requests to connect to the PC, and filter Incoming traffic by IP address or protocol. In addition, the personal firewall must filter incoming traffic by destination ports and maintain an IP traffic log.

The network infrastructure shall control the flow of information between interconnected systems. Information flow control regulates where information is allowed to travel within an information system and between information systems (as opposed to who is allowed to access the information) and without explicit regard to subsequent accesses to that information. In other words, controlling how data moves from one place to the next in a secure manner. Examples of controls are preventing criminal justice information from being transmitted unencrypted across a public network, blocking outside traffic that claims to be from within the agency, and not passing any web requests to the public network that are not from the internal web proxy.

Agencies employing data backup and storage procedures must consider the requirements for secure storage of electronic 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 here and in the CJIS Security Policy.

# **TIME System Security Awareness Certification Statement**

I certify that I have read and understand the contents of the TIME System Security Awareness handout and agree to follow all TIME/CJIS Systems requirements regarding the proper access to, use of, storage, and disposal of TIME/CJIS System information.

I understand that the criminal justice information made available via the TIME/CJIS Systems 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 the TIME/CJIS systems or information received from these systems 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 TIME/CJIS Systems 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 non-criminal justice purpose, etc.

Your signature: \_\_\_\_\_

Print your name: \_\_\_\_\_

Agency name: \_\_\_\_\_

Date: \_\_\_\_\_