COLLECT System Security Awareness Training & Confidentiality Agreement

This agreement and certification ensures the security and confidentiality of computerized record data consistent with applicable laws and regulations, provides for sanctions, and contains other provisions as required by the Connecticut On-Line Law Enforcement Communication Teleprocessing (COLLECT) System and National Crime Information Center (NCIC). The Criminal Justice Information Services (CJIS) Policy requires Security Awareness Training for all persons who have access to COLLECT System information (in any form).

Criminal history record information and related data, by its very nature, is sensitive and has potential for great harm if misused. All information from COLLECT must be kept in a **physically secure location**. A physically secure location is a facility or an area, a room, or a group of rooms, within a facility with both the physical and personnel security controls sufficient to protect criminal justice information and associated information systems.

Under no circumstances is COLLECT to be used for personal reasons or curiosity. All information from COLLECT/NCIC (in any form) must be protected from unauthorized use, view, or disclosure until the information is released to the public via authorized dissemination, purged, or destroyed in accordance with applicable record retention rules. Information can only be given to authorized personnel. Individuals that are authorized to access COLLECT must be employed by law enforcement or a criminal justice agency and must be currently certified. **Authorized personnel** are individuals or group of individuals, who have been appropriately vetted through a national fingerprint-based record check and have been granted access to criminal justice information.

DMV record data from COLLECT must be used strictly for the criminal justice and law enforcement community. Persons with access to this data are not authorized to release DMV information to a member of the public. The Driver's Privacy Protection Act of 1994, Title XXX of the Violent Crime Control and Law Enforcement Act, is a United States federal statute governing the privacy and disclosure of personal information gathered by state Departments of Motor Vehicles. The statute prohibits the disclosure of personal information without the express consent of the person to whom such information applies, with the exception of certain circumstances set forth in 18 U.S.C. § 2721. This rule applies to Departments of Motor Vehicles as well as other "authorized recipient[s] of personal information", and imposes record-keeping requirements on those "authorized recipients". The act makes it illegal to obtain drivers' information for unlawful purposes or to make false representations to obtain such information. It establishes criminal fines for noncompliance, and establishes a civil cause of action for drivers against those who unlawfully obtain their information.

Agencies that are authorized to access the COLLECT/NCIC System must meet the definition of a law enforcement or criminal justice agency as defined by 28 CFR Part 20 of the Federal Regulations. An **authorized recipient** is (1) A criminal justice agency or federal agency authorized to receive Criminal History Record Information (CHRI) pursuant to federal statute or executive order; (2) A nongovernmental entity authorized by federal statute or executive order to receive CHRI for noncriminal justice purposes; or (3) A government agency authorized by federal statute or executive order, or state statute which has been approved by the United States Attorney General to receive CHRI for noncriminal justice purposes.

Agencies with electronic media must meet the security standards set forth in the Criminal Justice Information Services (CJIS) Policy. "Electronic media" means electronic storage media including memory devices in laptops and computers and any removable, transportable digital memory media, such as magnetic tape or disk, optical disk, flash drives, external hard drives, or digital memory card. **Access to electronic and physical media in all forms (printed documents, printed imagery, etc.) must be restricted to authorized individuals.** Agencies must protect and control electronic and physical media during transport outside of controlled areas and restrict the activities associated with transport of such media to authorized personnel.

COLLECT System Security Awareness Training & Confidentiality Agreement

All information from the COLLECT System must be securely disposed of when no longer required to minimize the risk of access/dissemination by unauthorized individuals. Physical media must be destroyed by shredding or incineration. **All disposal or destruction must be monitored or performed by authorized personnel.**

All **visitors** must be authenticated by the associated agency and be escorted by authorized personnel. **Escorts** are authorized personnel who accompany a visitor at all times while within a physically secure location to ensure the protection and integrity of the physically secure location and any Criminal Justice Information therein. The use of cameras or other electronic means used to monitor a physically secure location does not constitute an escort. **Unescorted personnel** with access to record information must be subjected to state and national fingerprint-based record checks.

Sometimes an off duty employee may call in on a day off requesting information. You must be sure that s/he is seeking this information as part of the job, not for personal reasons. Persons with access to record data must be aware of social engineering. **Social Engineering** is the act of manipulating people into performing actions or divulging confidential information. While similar to a confidence trick or simple fraud, the term typically applies to trickery or deception for the purpose of information gathering, fraud, or computer system access; in most cases the attacker never comes face-to-face with the victim. Information can only be given to authorized personnel when they are performing their jobs. **Persons who request information for unauthorized purposes can be prosecuted for computer crimes.**

Sections 29-11 through 29-16 of the Connecticut General Statutes provides for the release of criminal history data to the general public. The criminal history data must be obtained from the State Police Bureau of Identification (SPBI), NOT from the COLLECT System.

All persons with access to COLLECT record information must be aware of Computer Related Offenses under Sections 53a-250 through 53a-261.

> A person is guilty of the computer crime of unauthorized access to a computer system when, knowing that he is not authorized to do so, he accesses or causes to be accessed any computer system without authorization.
>
> A person is guilty of the computer crime of theft of computer services when he accesses or causes to be accessed or otherwise uses or causes to be used a computer system with the intent to obtain unauthorized computer services.
>
> A person is guilty of the computer crime of interruption of computer services when he, without authorization, intentionally or recklessly disrupts or degrades or causes the disruption or degradation of computer services or denies or causes the denial of computer services to an authorized user of a computer system.
>
> A person is guilty of the computer crime of misuse of computer system information when: (1) As a result of his accessing or causing to be accessed a computer system, he intentionally makes or causes to be made an unauthorized display, use, disclosure or copy, in any form, of data residing in, communicated by or produced by a computer system; or (2) he intentionally or recklessly and without authorization (A) alters, deletes, tampers with, damages, destroys or takes data intended for use by a computer system, whether residing within or external to a computer system, or (B) intercepts or adds

data to data residing within a computer system; or (3) he knowingly receives or retains data obtained in violation of subdivision (1) or (2) of this subsection; or (4) he uses or discloses any data he knows or believes was obtained in violation of subdivision (1) or (2) of this subsection.

A person is guilty of the computer crime of destruction of computer equipment when he, without authorization, intentionally or recklessly tampers with, takes, transfers, conceals, alters, damages or destroys any equipment used in a computer system or intentionally or recklessly causes any of the foregoing to occur.

Computer crime in the 1st degree is a Class B felony.
Computer crime in the 2nd degree is a Class C felony.
Computer crime in the 3rd degree is a Class D felony.
Computer crime in the 4th degree is a Class A misdemeanor.
Computer crime in the 5th degree is a Class B misdemeanor.

Security violations shall be reported to the Terminal Agency Coordinator (TAC) for the associated agency. Violations can also be reported to:

Mail: **State of Connecticut**
Department of Emergency Services and Public Protection
COLLECT Unit
1111 Country Club Road
Middletown, CT 06457

Phone: **860-685-8020**

Fax: **860-685-8636**

Email: **dps.collect.unit@ct.gov**

COLLECT System Security Awareness Training & Confidentiality Agreement

Example of Unauthorized Disclosure

Police were conducting surveillance on a house when they called the dispatch center to conduct a check on the vehicle of a resident. Following the resident's arrest, officers received a tip that the resident had been alerted to the surveillance by a dispatcher and launched an investigation the following day. Officers viewed the resident's cell phone, which contained a message from the dispatcher's family member alerting the resident of the investigation. The dispatcher can be charged with second-degree hindering prosecution, conspiracy to commit second-degree hindering prosecution and interfering with an officer. The family member can be charged with hindering prosecution and interfering with an officer.

Example of Unauthorized Request for Information

Lieutenant A told Dispatcher B to run a check on Susie Public with a date of birth of 8-12-1957. When the dispatcher asks for a case number, Lieutenant A told her that he did not have one. It was later discovered that Susie Public was a potential babysitter for the Lieutenant's children. An internal investigation was initiated the same day.

Example of Unauthorized Dissemination

A city police department apprehended a wanted person. The wanted person later challenged the arrest. The city attorney who represents the police department requested all criminal history information related to the arrest. The department forwarded all criminal history information to the attorney. The city attorney is not entitled to this information and must request the documents by an Order of Discovery. The criminal history was obtained for the administration of criminal justice and the attorney wanted the documents for civil purposes. Criminal histories cannot be re-purposed once obtained. Also, the attorney's office did not meet the FBI's definition of an authorized recipient. The department was cited for unauthorized dissemination.

Examples of Unauthorized Access

Case 1: Officer A looked up the personal information of a woman that he had passed while in his marked police car from his MDT. He waved at her in passing. He confirmed her name and address and found her on a Social Media Site. The officer later contacted the women and identified himself as the officer from the previous day. The woman told a co-worker and the co-worker contacted the local police department. The police officer can be charged with two felonies-computer theft and violation of the Motor Vehicle Record Law.

Case 2: Citizen B had a couple of run-ins with his local police department. He asked his friend, Officer C to run his name and see if he would qualify for a pistol permit. The officer found no criminal history. The pistol permit application was subsequently denied by the Permits Unit. Citizen B appealed his denial, citing that Office C verified that he had no criminal history. The Appeals Board agreed that no criminal history existed. However, Citizen B was prohibited from having a pistol permit because he voluntarily committed himself to a mental health facility. An internal investigation was initiated the same day.

Case 3: Dispatcher D left the dispatch area to use the bathroom without logging out. Dispatcher E used the terminal to check the registration status of her boyfriend. A week later, the boyfriend was pulled over for speeding and the officer saw that he was run by the department. When asked if he was pulled over in the past week, the boyfriend said no, but that his girlfriend; a dispatcher ran his information to make sure that his registration was current. An internal investigation was initiated the same day.

Confidentiality Agreement

I am aware that the COLLECT/NCIC policy prohibits the dissemination or re-dissemination of data contained in the COLLECT/NCIC to unauthorized personnel. **I hereby agree** not to violate the confidentiality of any data or record information that may come to my attention and not to use such information for personal purposes. **I further understand** that the occurrence of misuse does not depend upon whether or not I receive additional compensation for such unauthorized activity.

I understand that violations of this agreement could result in termination of COLLECT/NCIC system access for the associated agency; individual termination of access COLLECT/NCIC system; criminal and/or administrative investigation; arrest; and/or prosecution and conviction for violation of State and Federal crimes designed to protect the confidentiality and integrity of criminal history record information and related data.

System Security Awareness Training Certification

I agree that I have received the System Security Awareness Training and understand that the COLLECT and NCIC systems are to be used for criminal justice and law enforcement purposes only.

Read and agreed to on:

Date: _____

Agency Name: _____

Title/Position: _____

Print Name: _____

Sign Name: _____

**Please fax the Certification Form only to the
State Police COLLECT Unit at:
860-685-8636**