ILLINOIS STATE POLICE DIRECTIVE
SRV-230, USE OF ARTIFICIAL INTELLIGENCE SYSTEMS

RESCINDS: New Directive	**REVISED:** 06-02-2025 **2025-013**
RELATED DOCUMENTS: SRV-200, SRV-201, SRV-221, SRV-229	**RELATED CALEA STANDARDS (6th Edition):** 40.1.1

I. POLICY

I.A. The Illinois State Police (ISP) is a client agency of the Department of Innovation and Technology (DoIT). In providing services and resources to its client agencies, DoIT operates a robust framework of information technology (IT) security policies including, but not limited to, cybersecurity policies, practices, and training. The State's cybersecurity strategy is compliant with the National Institute of Standards and Technology cybersecurity framework and is adopted herein by reference.

I.A.1. The ISP adopts these policies, as well as the Intergovernmental Agreement (IGA) and Management Control Agreement (MCA) with DoIT, by reference.

I.A.2. The ISP is responsible for exerting management control as is currently documented in the IGA and MCA, especially as it pertains to its Criminal Justice Information Services (CJIS) systems and the data contained therein; and

I.A.3. DoIT shall adhere to these policies, the IGA and MCA, in providing service to the ISP.

I.B. The State of Illinois adopts the FBI's CJIS Security Policy as its minimum-security requirement for criminal justice information. All Information Systems developed, acquired, or utilized as a service by DoIT and/or its Client Agencies containing CJIS regulated information will incorporate this security standard. Entities may develop local security policies; however, the CJIS Security Policy shall be the minimum applicable standard, and local policy shall not detract from this baseline.

I.C. The Illinois State Police (ISP) will:

I.C.1. Establish guidelines, conditions, and restrictions for the use of artificial intelligence (AI) technology.

I.C.2. Provide access for personnel to use AI software to meet the objectives and goals of the Department.

I.C.3. Establish procedures for the security, integrity, use, and confidentiality of information obtained, created, or maintained by the ISP employees and personnel contracted to the ISP.

I.C.4. Ensure the security of personal information.

II. AUTHORITY

II.A. 5 ILCS 179/1 et seq., "Identity Protection Act"

II.B. 815 ILCS 530/1, "Personal Information Protection Act"

II.C. 5 U.S.C. § 552a, "The Privacy Act of 1974"

II.D. 42 U.S.C. 405(c)(2)(c)(x) and (xi), "Social Security Number Protection Act of 2010"

II.E. FBI CJIS Security Policy, Version 5.9.2 12/07/2022, or most current version

II.F. Illinois Administrative Code Title 20, Part 1240 – Law Enforcement Agencies Data System (LEADS)

II.G. LEADS Security Policy, Version 2.2 02/01/2017, or most current version

II.H. All relevant federal and state rules, regulations, laws, and policies that govern the access and use of criminal justice information maintained by the ISP, or accessible to the ISP, despite the method of interface system.

III. DEFINITIONS

III.A. Artificial Intelligence (AI) – refers to the use of computer programs that can perform tasks traditionally requiring human intelligence, such as problem-solving, decision-making, predictions, recommendations, ongoing learning, etc. The use of AI in this document includes, machine learning, natural language processing, deep learning, neural networks, large language models, algorithmic decision support, pattern recognition, anomaly detection, computer vision, generative AI, etc.

III.B. AI system – any software or system or application that uses AI in whole or in part to perform tasks.

III.C. Criminal Justice Information (CJI) – information collected by criminal justice agencies that is needed for the fulfillment of their mission including, but not limited to biometric data, identity history data, biographic data, property data, and case/incident history in all systems housed by ISP and/or accessible to ISP employees.

III.D. Generative AI – the class of AI models that emulate the structure and characteristics of input data to generate derived synthetic content. This can include images, videos, audio, text, and other digital content.

III.E. Law Enforcement Agencies Data System (LEADS) – a statewide, computerized telecommunications information system designed to provide services, information, and capabilities to the law enforcement and criminal justice community in the state of Illinois. LEADS allows access to criminal justice information including, but not limited to, Hot Files (HF), Criminal History Record Information (CHRI), Firearm Owner's Identification (FOID), Concealed Carry License (CCL), Motor Vehicle Registration and Driver's Information and Imaging (SOS), the FBI's National Crime Information Center (NCIC/III), and the International Justice and Public Safety Network (NLETS).

III.F. Personal information – an individual's first name or first initial and last name with any one or more of the following data elements, when either the name or the data elements are not encrypted or redacted:

III.F.1. Social Security Number (SSN)

III.F.2. Driver's license number or state identification card number

III.F.3. Account number or credit or debit card number, or an account number or credit card number in combination with any required security code, access code, or password that would permit access to an individual's financial account

III.F.4. Any other identifying number including, but not limited to:

III.F.4.a. Passport number
III.F.4.b. Alien Registration Number
III.F.4.c. Military Identification Numbers
III.F.4.d. Biometric data
III.F.4.e. Username/email address

NOTE: Personal information does not include publicly available information that is lawfully made available to the public from federal, state, or local government records.

NOTE: Refer to ISP Directive SRV-200, "Information Security and the Disposal of Personal Information," for examples of personal information.

III.G. Public AI – public AI refers to AIs trained on user data and various open-source platforms. A public AI is an AI service, program, or algorithm that's openly accessible to anyone on the internet. Public AIs are typically general-purpose applications that serve the global population, providing AI solutions for problems and tasks that would normally require many man-hours to accomplish. Examples of public AI include search engines, social media algorithms, language translators, and text-to-speech engines.

III.H. Secure AI – secure AI systems have established security protocols which prohibit user data from being shared with public AI systems. User data is encrypted and maintained on a secured server system with access controls that are restricted to usage only by the client agency of the secure AI system.

IV. RESPONSIBILITIES

IV.A. All employees share the responsibility for the security, integrity, use, and confidentiality of information entered into and/or obtained from AI system resources.

IV.B. The Division of Justice Services (DJS) will review all requests for AI system applications for use on Department-issued electronic devices.

IV.B.1. DJS will forward requests for AI applications to DoIT and the ISP Legal Office for review.

IV.B.2. AI applications installed on Department-issued devices and operating systems must be secure AI systems and comply with Criminal Justice Information System (CJIS) requirements.

IV.C. The Division of the Academy and Training (DAT) will be responsible for providing initial training regarding acceptable usage of AI technology to all Department personnel. The DAT will provide additional AI training as deemed necessary by the Director.

V. PROCEDURES

V.A. AI system applications installed on Department-issued devices and operating systems must be approved by DoIT, ISP Legal Office, and DJS.

V.B. Prohibited uses of AI systems

V.B.1. ISP personnel are prohibited from using public AI applications, except those listed in Section V.C. below, on Department-issued devices that are used to access personal information or CJI.

V.B.2. ISP personnel are prohibited from entering any CJI, information contained within LEADS, and personal information into any public AI system from any device.

V.B.3. Personnel are prohibited from using ChatGPT, Gemini, Grok, or other text-based artificial intelligence systems for law enforcement report drafting functions. This does not prohibit the use of artificial intelligence technologies in research and investigative functions in accordance with Section V.C. below.

V.C. Acceptable uses of AI systems

V.C.1. Secure AI systems may be used for the following purposes:

V.C.1.a. Analyze intelligence information
V.C.1.b. Crime-scene analysis
V.C.1.c. Interview dictation
V.C.1.d. Evidence tracking
V.C.1.e. Analyze criminal/investigative reports
V.C.1.f. Analyze ISP administrative reports
V.C.1.g. Analyze ISP data and findings from ISP review boards
V.C.1.h. Conduct searches of ISP databases, report systems, and records
V.C.1.i. Draft administrative (non-criminal) reports
V.C.1.j. Language translation and processing
V.C.1.k. Improve automation of ISP databases and electronic operating systems
V.C.1.l. Enable chatbots and virtual assistants on public interfacing electronic systems
V.C.1.m. Initial/cursory review of video evidence

V.C.1.n. Any other purpose approved by the Director

V.C.2. Public AI systems may be used for services which do not involve the use of any CJI, information contained within LEADS, and personal information. Examples may include maps, weather, public web searches, calendar apps, etc.

V.D. Human oversight and validation of AI system usage

V.D.1. All official work products using AI technology in accordance with this directive shall include human oversight and validation.

V.D.2. Published ISP documents produced using generative AI must include a statement indicating the use of generative AI was utilized in the creation of the document, the document was reviewed, and content was verified as accurate.

NOTE: Sample statement – “Parts of this document have been produced through the use of generative AI technology. All content of this document has been reviewed and is deemed accurate through human oversight.”

-End of Directive-