ICOTS Privacy Policy V4.1 06-2009

Privacy Policy

Interstate Compact Offender Tracking System

Version 5.0

Approved 04/23/2009

Revised on 3/20/2024

1.0 Statement of Purpose

The goal of establishing and maintaining the ICOTS is to further the following purposes of the Commission:

A. Increase public safety and improve national security;
B. Minimize the threat and risk of injury to specific individuals; including but not limited to: law enforcement and others responsible for public protection, safety, or health;
C. Minimize the threat and risk of damage to real or personal property;
D. Protect individual privacy, civil rights, civil liberties, and other protected interests;
E. Protect the integrity of the criminal investigation, criminal intelligence, and justice system processes and information;
F. Minimize reluctance of individuals or groups to use or cooperate with the justice system;
G. Support the role of the justice system in society;
H. Promote governmental legitimacy and accountability;
I. Not unduly burden the ongoing business of the justice system; and
J. Make the most effective use of public resources allocated to justice agencies.

2.0 Accountability

A. The existence of ICOTS will be made public and the system's policies on protection of privacy, civil rights, and civil liberties will be made available to the public upon request.
B. ICAOS will adopt provisions to ensure accountability for compliance with all applicable laws and policies in the collection, use, analysis, retention, destruction, sharing, and disclosure of information.

3.0 Definitions

A. “ICAOS” means the Interstate Commission for Adult Offender Supervision.
B. “ICOTS” means the Interstate Compact Offender Tracking System.
C. “Information” means any data about people, organizations, events, incidents, or objects, regardless of the medium in which it exists.
D. “Law” means any local, state, tribal, territorial, or federal statute, ordinance, regulation, executive order, policy, or court rule, decision, or order, as construed by appropriate local, state, tribal, territorial, or federal officials or agencies.
E. “Member Agency” means those states, and their political subdivisions, that are active members of the Interstate Commission for Adult Offender Supervision and the primary users of the ICOTS system.
F. “Participating Agency” means both member agencies and other justice system partners who share or use the ICOTS system.
G. “Public” means:
    1. Any person and any for-profit or nonprofit entity, organization, or association;
    2. Any governmental entity for which there is no existing specific law authorizing access to the participating agency’s information;
    3. Media organizations; and
    4. Entities that seek, receive, or disseminate information for whatever reason, regardless of whether it is done with the intent of making a profit, and without distinction as to the nature or intent of those requesting information from the participating agency.
H. “Public” does not include:
    1. Employees of the participating agency;
    2. People or entities, private or governmental, who assist the agency in the operation of the justice information system; and
    3. Public agencies whose authority to access information gathered and retained by the participating agency is specified in law. The bulk release of information to either the public, private, or non-profit agencies is permitted only if they are authorized by law and approved in advance by ICAOS.

4.0 Compliance with Laws Regarding Privacy, Civil Rights, and Civil Liberties

A. ICAOS and all participating agencies, employees, and users will comply with all applicable laws protecting privacy, civil rights, and civil liberties in the collection, use, analysis, retention, destruction, sharing, and disclosure of information.
B. ICAOS will adopt internal operating policies requiring compliance with all applicable laws protecting privacy, civil rights, and civil liberties in the collection, use, analysis, retention, destruction, sharing, and disclosure of information in the system.
C. ICAOS will conduct periodic audits to measure compliance with all applicable laws protecting privacy, civil rights, and civil liberties in the collection, use, analysis, retention, destruction, sharing, and disclosure of information in the system.
D. The Health Insurance Portability and Accountability Act (“HIPAA”) exempts certain disclosures of health information for law enforcement purposes without an individual’s written authorization. The various conditions and requirements concerning these exempt disclosures are contained in the regulatory text of the HIPAA privacy rule and may be found at 45 C.F.R 164 et. seq. Under these provisions protected health information may be disclosed for law enforcement purposes when such disclosures are required by law. Thus, disclosure of protected health information required to be furnished by or received from member agencies that administer the Interstate Compact for Adult Offender Supervision (“the Compact”) acting pursuant to the provisions of the Compact and its authorized rules is permissible.

5.0 Expectations Regarding Information Gathered and Shared

A. Member agencies will adopt internal policies and procedures requiring the participating agency, its personnel, contractors, and users to:
    1. Seek or retain only information that is legally permissible for the participating agency to seek or retain under laws applicable to the participating agency;
    2. Use only lawful means to seek information;
    3. Seek and retain only information that is reliably accurate, current, and complete, including the complete, relevant context;
    4. Take appropriate steps when merging information about an individual or organization from two or more sources, to ensure that the information is accurate, complete, and related to the same individual or organization;
    5. Investigate in a timely manner any alleged errors and correct information found to be erroneous within thirty (30) days of discovery;
    6. Retain information sought or received only so long as it is relevant and timely, and delete or return information that is inaccurate, outdated, or otherwise no longer related to known or suspected criminal, including terrorist, activities;
    7. Maintain information and systems containing information in a physically and electronically secure environment and protected from natural or man-made disasters or intrusions;
    8. Engage in collation and analysis of information in a manner that conforms to generally accepted practices;
    9. Establish procedures that comply with the policies and procedures of ICAOS for accessing information through the participating agency;
    10. Allow only authorized users to access the information in ICOTS and only for purposes related to the performance of their official duties;
    11. Share information with authorized users of other justice system partners based only on a “right-to-know” and a “need-to-know” basis; and
    12. Establish and comply with information retention and destruction schedules.

6.0 Sharing Information with Other Justice System Partners

A. When there is a question or inquiry about shared data, a participating agency will make information available in response to a query either by:
    1. Providing the requested information directly;
    2. Responding with the contact information of a person in the responding agency whom the individual making the query can contact;
    3. Having a person in the responding agency contact the individual making the query; or
    4. Indicating that no information is available.

7.0 Disclosure of Information According to the Originating Agency’s Access Rules

A. A participating agency will not disclose information originating from another participating agency except as provided for in this agreement or in the operational policies of ICOTS.

8.0 Reporting Possible Information Errors to the Originating Agency

A. When a participating agency gathers or receives information that suggests that information may be erroneous, may include incorrectly merged information, or lacks relevant context, the alleged error will be communicated within five (5) business days in writing to the ICOTS Administrator, who will then take necessary corrective action consistent with sections 5.0(A)(5) and 15.0(C).

9.0 Expectations Regarding Accountability and Enforcement

A. Participating agencies will adopt and comply with internal policies and procedures requiring the agency, its personnel, contractors, and users to:
    1. Have and enforce policies for discovering and responding to violations of agency policies and this policy, including taking appropriate action when violations are found;
    2. Provide training about the agency's requirements and policies regarding information collection, use, and disclosure to personnel authorized to use ICOTS;
    3. Make available to the public the agency's internal policies and procedures regarding privacy, civil rights, and civil liberties;
    4. Cooperate with periodic, random audits by representatives of ICAOS; and
    5. Designate an individual within the participating agency to receive reports of alleged errors in the information that originated from the participating agency.

10.0 Enforcement of Provisions of Information Sharing Agreement

A. If a participating agency fails to comply with the provisions of this agreement or fails to enforce provisions in its local policies and procedures regarding proper collection, use, retention, destruction, sharing, disclosure, or classification of information, ICAOS may:
    1. Offer to provide an independent review, evaluation, or technical assistance to the participating agency to establish compliance.
    2. Suspend or discontinue access to ICOTS by a user in the offending agency who is not complying with the agreement or local policies and procedures;
    3. Suspend or discontinue the offending agency's access to ICOTS; or
    4. Offer to provide an independent review, evaluation, or technical assistance to the participating agency to establish compliance.

11.0 Information Sought and Retained

A. Participating agencies will seek or retain only information that is:
    1. Relevant to the interstate compact transfer process and supervision, investigation and prosecution of suspected criminal, incidents; the resulting justice system response; the enforcement of sanctions, orders, or sentences; or the prevention of crime, or that is useful in crime analysis or in the administration of criminal justice.
    2. Collected by criminal justice agencies on specific individuals, consisting of official identifiable descriptions and notations of arrests, detentions, warrants, complaints, indictments, information, or other formal criminal charges, and any disposition relating to these charges, including acquittal, sentencing, pre- or post-conviction supervision, correctional supervision, and release.

B. Participating agencies will not seek or retain information about an individual or organization solely on the basis of religious, political, or social views or activities; participation in a particular organization or event; or race, ethnicity, citizenship, place of origin, age, disability, gender, or sexual orientation unless such information is:
    1. Relevant to whether an individual or organization has engaged in, is engaging in, or is planning a criminal activity; or
    2. Needed by the participating agency:
        a. To identify an individual;
        b. In order for the agency to operate effectively; or
        c. To provide services to the individual or accommodate an individual's religious, ethnic, or cultural requests or obligations.
    3. The participating agency shall keep a record of the source of all information retained by the participating agency.

12.0 Methods of Seeking or Receiving Information

A. Information gathering and investigative techniques used by participating agencies will comply with all applicable laws.
B. Participating agencies will not directly or indirectly receive, seek, accept, or retain information from an individual, non-government or third party information provider, who may or may not receive a fee or benefit for providing the information, if the participating agency knows or has reason to believe that:
    1. The individual or information provider is legally prohibited from obtaining the specific information sought or disclosing it to the agency;
    2. The individual or information provider used methods for collecting the information that the agency itself could not legally use;
    3. The specific information sought from the individual or information provider could not legally be collected by the agency; or
    4. The agency has not taken the steps necessary to be authorized to collect the information.
C. Information gathering and investigative techniques used by participating agencies will be no more intrusive or broad-scale than is necessary in the particular circumstance to gather information it is authorized to seek or retain.

13.0 Classification of Information Regarding Validity and Reliability

A. At the time of retention in the system, the information will be categorized regarding:
    1. Content validity;
    2. Nature of the source; and
    3. Source reliability.
B. The categorization of retained information will be reevaluated when new information is gathered that has an impact on the validity and reliability of retained information.

14.0 Classification of Information Regarding Limitations on Access and Disclosure

A. At the time a decision is made to retain information, it will be classified pursuant to the applicable limitations on access and sensitivity of disclosure in order to:
    1. Protect confidential sources and police undercover techniques and methods;
    2. Not interfere with or compromise pending criminal investigations;
    3. Protect an individual’s right of privacy and civil rights; and
    4. Provide legally required protection based on the status of an individual as victim.
B. The classification of existing information will be reevaluated whenever:
    1. New information is added that has an impact on access limitations or the sensitivity of disclosure of the information; or
    2. There is a change in the use of the information affecting access or disclosure limitations.
C. The access classifications will be used to control:
    1. What information a class of users can have access to;
    2. What information a class of users can add, change, delete, or print; and
    3. To whom the information can be disclosed and under what circumstances.

15.0 Information Quality

A. Participating agencies will make every reasonable effort to ensure that information sought or retained is:
    1. Derived from dependable and trustworthy sources of information;
    2. Accurate;
    3. Current;

4. Complete and verified, including the relevant context in which it was sought or received and other related information; and
5. merged with other information about the same individual or organization only when the applicable standard has been met.

B. Participating agencies will ensure that only authorized users are allowed to add or change information in the system.
C. Participating agencies will ensure that information will be deleted from the system no later than 30 calendar days when the agency learns that the:
    1. information is erroneous, misleading, obsolete, or otherwise unreliable;
    2. source of the information did not have authority to gather the information or to provide the information to the participating agency; or
    3. source of the information used prohibited means to gather the information.
D. Participating agencies will make every reasonable effort to ensure that photographs of supervised individuals uploaded to ICOTS meet the following criteria:
    1. the supervised individual's face is recognizable and visible;
    2. the photo is displayed in 'portrait' view (height is greater than width);
    3. the photo is in color and is sharp with no visible pixels or printer dots; and
    4. the background does not detract from the supervised individual's face.

16.0 Collation and Analysis of Information

A. Information sought or received by participating agencies or from other sources will only be analyzed:
    1. by qualified individuals;
    2. to provide tactical and/or strategic intelligence on the existence, identification, and capability of individuals and organizations suspected of having engaged in or engaging in criminal, including terrorist, activities generally; and
    3. to further crime, including prevention, terrorism, enforcement, force deployment, or prosecution objectives and priorities established by participating agencies.
B. Information sought or received by participating agencies or from other sources will not be analyzed or combined in a manner or for a purpose that violates Section 17.0 Merging of Information from Different Sources.

17.0 Merging of Information from Different Sources

A. Information about an individual from two or more sources will not be merged unless there is sufficient identifying information to reasonably conclude that the information is about the same individual or organization.
B. The set of identifying information sufficient to allow merging will consist of at least four of the fields, including: first name, last name, date of birth, ICAOS identifier, FBI identifier, and/or sending state identifier.

18.0 Sharing Information

A. The ICAOS national office shall not confirm the existence or nonexistence of information to any person or agency that would not be eligible to receive the information itself.
B. Access to information retained by ICOTS will be provided only to participating agencies that are authorized to have access and only for legitimate law enforcement, public protection, public prosecution, public health, or justice purposes, and only for the performance of official duties in accordance with the law and procedures applicable to participating agencies for whom the person is working.
C. Information retained by ICOTS may be disseminated to individuals in public or private entities only for public protection, safety, or public health purposes and only in the performance of official duties in accordance with applicable laws and procedures. Nothing in this policy shall

limit the dissemination, including unsolicited, of an assessment of criminal intelligence information to a government official or to any other individual, when necessary to avoid imminent danger or certain danger to life or property.

D. Information gathered and retained by ICOTS may be disseminated for specific purposes upon request by persons authorized by law to have such access and only for those uses or purposes specified in the law.
E. Information gathered and retained by ICOTS may be disclosed to a member of the public only if the information is defined by law to be a public record and is not exempt from disclosure by law, and it may only be disclosed in accordance with the law and procedures applicable to participating agencies for this type of information.
F. Upon satisfactory verification of identity and subject to the conditions specified, an individual is entitled to know the existence of and to review the information that has been gathered and retained by ICOTS. The individual may obtain a copy of the information for the purpose of challenging the accuracy or completeness of the information. A participating agency's response to the request for information will be made within a reasonable time and in a form that is readily intelligible to the individual.
    1. The existence, content, and source of the information will not be made available to an individual when:
        1. Disclosure would interfere with, compromise, or delay an ongoing investigation or prosecution;
        2. Disclosure would endanger the health or safety of an individual, organization, or community;
        3. The information is considered criminal intelligence; or,
        4. The information is considered to be victim-sensitive.
G. When there is a question of inquiry about the accuracy or relevance of shared data, the participating agency will:
    1. Respond to the query directly;
    2. Inform the requestor of the procedure for review of any objections and will be given reasons if a request for correction is denied; and,
    3. Inform the requestor of the procedure for appeal if the participating agency declines to correct challenged information.
H. An audit trail will be kept of access by or dissemination of information to such persons.
I. Participating agencies may charge a fee to those requesting information per applicable law and procedures.

19.0 Review of Information Regarding Retention

A. Information will be reviewed periodically for purging.
B. When information has no further value or meets the criteria for removal under applicable law, it will be purged, destroyed, deleted, or returned to the submitting source.

20.0 Destruction of Information

A. Information in ICOTS will not be purged, destroyed, deleted or returned without the written permission of the agency that submitted the information.
B. Notification of proposed destruction or return of records will be provided to the agency submitting the information.
C. A record that information has been purged or returned shall be maintained by ICAOS.

21.0 Information System Transparency

A. The ICOTS Privacy Policy is available to the public on request and on the ICAOS website.
B. The Compact Commissioner in each state is responsible for receiving and responding to inquiries and complaints about privacy, civil rights, and civil liberties protections in ICOTS and will provide

to the public the contact information.

22.0 Accountability for Activities

A. The primary responsibility for the operation of ICOTS, including operations; coordination of personnel; receiving, seeking, retaining and evaluating information quality; the analysis, destruction, sharing, and disclosure of information; and the enforcement of this policy are assigned to the Commission's Executive Director.
B. ICAOS will establish procedures, practices, and system protocols and use software, information technology tools, and physical security measures that protect information from unauthorized access, modification, theft, or sabotage, whether internal or external, and whether due to natural or human-caused disasters or intrusions. The methods and techniques used shall be consistent with industry standards.
C. ICOTS will store information in a manner such that it cannot be added to, modified, accessed, destroyed, or purged except by personnel authorized to take such actions.
D. ICAOS will adopt and follow procedures and practices by which it can ensure and evaluate the compliance of users and the system itself with the provisions of this policy, industry standards and applicable law.
E. ICAOS will require any individuals authorized to use the system to agree in writing to comply with the provisions of this policy.
F. ICAOS will periodically conduct audits and inspections of the information contained in ICOTS. The audits will be conducted randomly by a designated representative of the participating agency or by a designated independent party. The audit will be conducted in such a manner so as to protect the confidentiality, sensitivity, and privacy of the agency's information.
G. ICAOS will periodically review and update the provisions protecting privacy, civil rights, and civil liberties in its policies and make appropriate changes in response to changes in applicable law and public expectations.
H. ICAOS will notify an individual about whom unencrypted personal information was or is reasonably believed to have been obtained by an unauthorized person and access to which threatens physical or financial harm to the person The notice will be made promptly and without unreasonable delay following discovery or notification of the access to the information, consistent with the legitimate needs of law enforcement to investigate the release or any measures necessary to determine the scope of the release of information and to reasonably restore the integrity of ICOTS.

27.0 Enforcement

A. If a user is suspected of or found to be not in compliance with the provisions of this policy regarding the collection, use, retention, destruction, sharing, classification, or disclosure of information, the participating agency or ICAOS will:
    1. suspend or discontinue access to information by the user;
    2. suspend, demote, transfer, or terminate the person as permitted by applicable personnel policies;
    3. apply other sanctions or administrative actions as provided in the participating agency's personnel policies;
    4. request the participating agency, organization, contractor, or service provider employing the user to initiate proceedings to discipline the user or enforce the policy's provisions; or
    5. refer the matter to appropriate authorities for criminal prosecution, as necessary, to effectuate the purposes of the policy.

28.0 Training

A. Member agencies will require the following individuals to participate in training programs regarding the implementation of and adherence to the privacy, civil rights, and civil liberties

policy:

1. its personnel;
2. personnel providing information technology services to the agency;
3. staff in other public agencies or private contractors providing services to the agency; and
4. users who are not employed by the agency.

B. The training program will cover:

1. purposes of the privacy, civil rights, and civil liberties protection policy;
2. substance and intent of the provisions of the policy relating to collecting, use, analysis, retention, destruction, sharing, and disclosure of information retained by the agency;
3. the impact of improper activities associated with information accessible within or through the agency; and
4. the nature and possible penalties for policy violations, including possible transfer, dismissal, civil and criminal liability, and immunity, if any.