INTERSTATE COMMISSION FOR
ADULT OFFENDER SUPERVISION

02-2026 - INSITE PRIVACY, ACCESS, AND DATA QUALITY POLICY

POLICY NUMBER	ISSUED
02-2026	July 1, 2026

I. Purpose

This policy establishes standards for privacy, access, visibility, security, and data quality for information maintained in INSITE (Interstate National System for Information, Tracking, and Enforcement), the Interstate Commission's information system supporting the transfer, supervision and return of individuals under the Interstate Compact for Adult Offender Supervision (ICAOS).

This policy defines the governance framework, security controls, and user responsibilities necessary to ensure that information entered in INSITE is collected, accessed, used, shared, retained, and disposed of in a manner that protects confidentiality, integrity, and availability, while supporting public safety and Compact operations.

This policy is intended to:

- Protect individual privacy, civil rights, and civil liberties;
- Ensure information is accessed and used only for authorized purposes;
- Promote data accuracy, integrity, and system reliability; and
- Establish accountability through audit, oversight, and enforcement.

II. Scope

This policy applies to all Member Agencies, Participating Agencies, and all authorized users, contractors, and partners accessing or managing INSITE information.

It applies to all data and system components associated with INSITE, including data entry, transmission, storage, integration, and dissemination.

III. Definitions

Key definitions applicable to this policy include, but are not limited to:

- **Expungement** – The lawful removal or sealing of a record from view in accordance with applicable state law.

- **INSITE** – The Interstate Commission's information system used to support Compact transfer and supervision activities.
- **Information** – Any data about individuals, organizations, or events maintained in INSITE, regardless of format.
- **Member Agency** – The state entity designated under the Interstate Compact for Adult Offender Supervision responsible for administering Compact operations within its jurisdiction, including oversight of INSITE use, enforcement of Commission rules and policies, and coordination with and supervision of participating agencies within the state.
- **Participating Agency** – Any state, local, or other authorized justice agency within a member state that accesses, enters, manages, or shares information in INSITE in support of Compact activities under the authority and oversight of the Member Agency.
- **Public** – Any person or entity not expressly authorized by law or Compact rule to access INSITE information.
- **State Administrator** – A user authorized to delete or modify existing INSITE information as well as manage user administration.
- **State of Record** – The state in which the INSITE record originated.
- **User** – An individual granted access to INSITE.

IV. Policy Statement

INSITE is a restricted-access criminal justice information system.

All information within INSITE shall be:

- Accessed and used only for authorized criminal justice and Compact purposes;
- Protected against unauthorized access, disclosure, alteration, or destruction;
- Maintained to ensure data integrity, accuracy, and completeness; and
- Subject to auditing, monitoring, and enforcement controls.

INSITE is not a public-facing system except as explicitly authorized.

V. Roles and Responsibilities

A. Interstate Commission (ICAOS)

- Establish system security requirements, policies, and minimum control standards;
- Maintain system-wide audit, monitoring, and compliance oversight;
- Conduct audits, assessments, and enforcement actions as necessary.
- Ensure implementation of system backup, recovery, and continuity processes to protect INSITE data and support restoration in the event of data loss, system failure, or disruption, with detailed procedures maintained in system security or operations documentation.

B. Member Agencies

Member Agencies are the primary authority for INSITE compliance within their jurisdiction and shall:

- Enforce access controls that limit users to only the information and system functions necessary to perform their assigned duties, consistent with need-to-know and right-to-know principles;
- Administer user access, authentication, and authorization controls;
- Ensure completion of initial and ongoing training for all users, including INSITE use, security awareness, and the application of state laws, policies, and procedures to interstate Compact cases;
- Maintain training records and user access documentation;
- Immediately disable access for terminated, transferred, or non-compliant users;
- Establish incident reporting procedures for misuse or unauthorized access;
- Ensure compliance with this policy and applicable laws;
- Oversee all Participating Agencies and users within their jurisdiction for adherence to this policy and ICAOS rules.

C. Participating Agencies

- Comply with all INSITE security, privacy, and data requirements;
- Use INSITE only for authorized purposes;
- Report security incidents, misuse, or data errors to the Member Agency;
- Maintain data quality and accuracy for information entered.

VI. Access and Privacy Standards

A. Authorized Access

Access to INSITE shall be limited to authorized users with a validated need-to-know and right-to-know for official duties.

B. Access Control

Agencies shall implement controls consistent with CJIS-aligned practices, including:

- Unique user identification;
- Role-based or attribute-based access controls;
- Periodic review and validation of user access rights;
- Immediate revocation of access when no longer required; and
- User accounts shall be deactivated within seven (7) calendar days after ninety (90) calendar days of inactivity.

C. Authentication and Account Management

- User accounts shall not be shared;
- Authentication credentials shall be protected and managed in accordance with agency security policies;
- Agencies shall ensure appropriate password and authentication standards are enforced.

D. Sensitive and Health-Related Information

- Entry of sensitive or protected health information shall be limited to the minimum necessary;
- Agencies shall comply with applicable laws, including the Health Insurance Portability and Accountability Act, where applicable;
- Users shall avoid unnecessary or excessive entry of medical or behavioral health information;
- Disclosure or release of medical or health-related information shall be governed by applicable state and local laws and agency policies.

VII. Public Access and Information Visibility

INSITE provides limited public access to data through a public web portal. A member agency may restrict or conceal a supervised individual's information from public view when:

- Disclosure is prohibited by state or federal law; or

- The supervised individual is participating in a state or federal witness protection or comparable program.

Member Agencies may restrict public visibility when required by law or safety considerations. All restrictions shall be documented and subject to audit.

VIII. Data Quality and Integrity Standards

A. Data Integrity

Agencies shall ensure that data entered in INSITE is accurate, timely, complete, and derived from reliable sources.

B. Error Resolution

Alleged errors shall be:

- Investigated and reported within five (5) business days; and
- Corrected within thirty (30) calendar days by the appropriate authority.

C. Identity Management and Duplicate Prevention

- Agencies shall use standardized identifiers to uniquely identify individuals;
- Data entry shall be reviewed to prevent duplication or misidentification;
- Duplicate or merged records shall be corrected within thirty (30) calendar days by the state administrator.

D. Data Minimization and Cleanup

Agencies shall ensure that only relevant and necessary data is maintained and that obsolete or erroneous data is removed.

E. Photographic Identification Standards

Participating Agencies shall make reasonable efforts to ensure that primary photographs of supervised individuals uploaded to INSITE meet the following minimum standards:

- The individual’s face is clearly recognizable and fully visible;
- The image is in portrait orientation (height greater than width);
- The image is in color and of sufficient clarity, without visible pixelation, distortion, or printing artifacts; and
- The background does not obscure or detract from the individual’s face.

Photographs shall be updated as necessary to ensure they support reliable identification, including when an individual's appearance has materially changed. In all cases, photographs should be reviewed periodically and updated at least every five (5) years during active supervision.

IX. Auditing, Monitoring, and Compliance

A. System Monitoring

- INSITE shall maintain audit logs and monitoring capabilities to track user access and activity;
- Member Agencies and users may be subject to audit based on system activity and usage;
- Member Agencies shall support audits and provide requested documentation; and
- Member agencies shall conduct reviews of user access and data quality at least every ninety (90) calendar days.

B. Agency Self-Assessment

- Member agencies shall complete a self-audit or compliance checklist (ADD LINK) reviewing adherence to this policy at least once every two (2) years.
- The Commission may require corrective action for identified deficiencies.

Noncompliance may result in:

- Suspension or termination of access;
- Mandatory corrective action;
- Referral for administrative or enforcement action.

X. Incident Response and Reporting

- Incidents involving unauthorized access, misuse of the system, or suspected data or security breaches shall be reported promptly to the Member Agency;
- Member Agencies shall notify the Commission's national office of significant incidents;
- Agencies shall document, investigate, and remediate all incidents;
- Corrective actions shall be implemented to prevent recurrence.

XI. Information Sharing

- Information sharing shall be limited to authorized criminal justice and Compact purposes;
- Information sharing shall comply with applicable laws, policies, and agreements;
- Unauthorized dissemination is strictly prohibited;
- All external sharing shall be documented and auditable.

XII. Data Retention and Destruction

- Data shall be retained in accordance with applicable legal, regulatory, and operational requirements.
- Record expungement and deletion requests shall be processed and documented in compliance with applicable laws and policies.
- Secure data destruction methods shall be used to prevent recovery of expunged records.

XIII. Transparency and Requests

- Requests for information shall be handled in accordance with applicable law;
- The state of record is responsible for responding to data-specific requests;
- The Commission may respond to system-level inquiries as authorized;
- Agencies shall designate responsible personnel for handling requests.

XIV. Policy Review

This policy shall be reviewed periodically to ensure alignment with:

- Legal and regulatory requirements;
- Compact rules;

- Security best practices; and
- System and operational changes.