

ILLINOIS STATE POLICE DIRECTIVE

SRV-200, INFORMATION SECURITY AND DISPOSAL OF PERSONAL INFORMATION

RESCINDS: SRV-200, 2022-001, revised 01-24-2022.	REVISED: 12-04-2023 2023-178
RELATED DOCUMENTS: PER-030, ROC-002, SRV-201, SRV-204, SRV-206, SRV-211, SRV-218, SRV-220, SRV-221	RELATED CALEA STANDARDS (6th Edition): 82.1.1, 82.1.3, 82.1.6, 82.2.4, 82.3.4, 82.3.5

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. Provide access for authorized persons to use resources and computing hardware and software to meet the objectives and goals of the Department.
 - I.C.2. 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.3. Establish guidelines for the security and disposal of personal information either in paper form or electronically.

II. AUTHORITY

- II.A. 5 ILCS 140/1 et. seq., "Freedom of Information Act"
- II.B. 5 ILCS 179/1 et seq., "Identity Protection Act"
- II.C. 20 ILCS 450/25, "Mandatory State employee training"
- II.D. 720 ILCS 5/16-30, "Identity theft; aggravated identity theft"
- II.E. 815 ILCS 530/1, "Personal Information Protection Act"
- II.F. 5 U.S.C. § 552a, "The Privacy Act of 1974"
- II.G. 42 U.S.C. 405(c)(2)(c)(x) and (xi), "Social Security Number Protection Act of 2010"

III. DEFINITIONS

- III.A. Custodian - the custodian is responsible for the processing and storage of information.
 - III.A.1. For mainframe applications, the Division of Justice Services (DJS) is the custodian.
 - III.A.2. For assigned computer(s), including the internal hard drive, micro and mini applications, as well as all email messages the assigned user is the custodian.
 - III.A.3. For computer internal hard drive(s), the assigned user will retain custodial responsibilities.
 - III.A.4. For E-mail messages (Inbox, Drafts, Sent), the assigned user will retain custodial responsibilities.
- III.B. Information - information includes documents, telecommunications, electronically stored files, electronically recorded data, and all computer-related activities.
- III.C. ISP security directives - directives that regulate access to, and use of, ISP computing resources, which are as follows:
 - III.C.1. SRV-200, "Information Security and the Disposal of Personal Information"
 - III.C.2. SRV-201, "Use of Illinois State Police Computing Equipment and Resources"
 - III.C.3. SRV-204, "Local Area Network (LAN) Access and Administration"
 - III.C.4. SRV-206, "Use of E-Mail"
 - III.C.5. SRV-208, "Mobile Data Computer Systems"
 - III.C.6. SRV-209, "Illinois State Police Website"
 - III.C.7. SRV-211, "Investigative Indices System"
 - III.C.8. SRV-212, "Law Enforcement Agencies Data System (LEADS) Administrative Messages"
 - III.C.9. SRV-213, "Illinois Secretary of State Data Requests"
 - III.C.10. SRV-214, "Computer Aided Dispatch (CAD) and Traffic Information and Planning System (TIPS) Data Access and Dissemination"
 - III.C.11. SRV-215, "Field Notification Program"
 - III.C.12. SRV-216, "Notification of Suspension/Reinstatement of Personnel"
 - III.C.13. SRV-217, "Law Enforcement Agencies Data System (LEADS) Help Program"
 - III.C.14. SRV-218, "Computer Password Control"
 - III.C.15. SRV-221, "Internet Use"
 - III.C.16. SRV-222, "Social Networking/Media Guidelines"
 - III.C.17. SRV-223, "Access to Criminal Justice Information"
 - III.C.18. SRV-225, "Procedures for the Removal of Information and Destruction of Physical Media"
 - III.C.19. SRV-226, "Infrastructure Security Awareness (ISA) Program"
- III.D. Owner – all information has an owner. A collection of information is owned by the Division/Bureau responsible for the business results of an application, system, or the business use of this information. Data owners of different divisions, bureaus, or organizational units may share ownership of applications or systems.

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

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

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

III.E.4.a. Passport number

III.E.4.b. Alien Registration Number

III.E.4.c. Military Identification Numbers

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

III.E.5. Examples of forms/documents containing personal information consist of, but are not limited to:

III.E.5.a. Personnel Forms

III.E.5.a.1) Personnel Evaluations (drafts and finals)

III.E.5.a.2) Personnel Action Requests/Officer Action Requests

III.E.5.a.3) Time verification sheets

III.E.5.a.4) Employment Applications (CMS)

III.E.5.a.5) Tax Withholding Cards (W-4)

III.E.5.a.6) User Identification Attribute Forms

III.E.5.b. Enforcement/Investigative Forms

III.E.5.b.1) Crash Reports

III.E.5.b.2) Citations and Written Warnings

III.E.5.b.3) Field Reports/Incident Reports/Arrest Reports

III.E.5.b.4) Investigative Reports

III.E.5.b.5) Criminal History Records Inquiry (CHRI) printouts

III.E.5.c. Other Applications/Forms

III.E.5.c.1) Background Investigation Request

III.E.5.c.2) Application for Firearm Owner's Identification Card, form ISP 6-181

III.E.5.c.3) Material Request Forms (if payments go to an individual)

III.E.5.c.4) Basic Ordering Agreements

III.E.5.c.5) Applicant Fingerprint Cards

III.E.5.c.6) Uniform Conviction Information Act Inquiries

III.F. Records Compliance Coordinator (RCC) – an individual within each division appointed by the appropriate Deputy Director to ensure compliance with the Identity Protection Act.

III.G. User - the user is any person who has been authorized to read, enter, update, or disseminate information by the owner of the system or application data.

IV. RESPONSIBILITIES

IV.A. All employees share the responsibility for the security, integrity, use, and confidentiality of information obtained from ISP resources. A violation of standards, procedures, or guidelines established pursuant to this directive or relating to other security directives will be reported to the immediate supervisor of the employee discovering the violation.

- IV.A.1. The DJS will make relevant DoIT policies available to its employees via the ISP intranet.
 - IV.A.1.a. The DJS will review the ISP intranet annually no later than October 1 each year to ensure the most current policies are posted and provide notice to the Divisions of any changes.
 - IV.A.1.b. Each division is responsible for ensuring ISP employees are aware of current DoIT policies.
- IV.A.2. The Division of the Academy and Training (DAT) is responsible for making the State's annual cybersecurity training available to the ISP's employees through the State's online training system.
- IV.B. Information processed by a computerized system must have an identified owner.
 - IV.B.1. The owner may delegate ownership responsibility to other individuals.
 - IV.B.2. The owner of the information or data has the responsibility to:
 - IV.B.2.a. Judge the value of the information and classify it
 - IV.B.2.b. Authorize, alter, suspend, and revoke access and assign custody of information
 - IV.B.2.c. Specify the security controls and communicate the control and confidentiality requirements to the custodian and users of the information
 - IV.B.2.d. Determine the statutory requirements regarding retention, use, and privacy; and communicate this information to the custodian
 - IV.B.2.e. Report any unauthorized use of information, data, or resources to the custodian, appropriate supervisors, and the Division RCC
 - IV.B.2.f. Notify Security Administration of changes to the access requirements of the data or a user's access to the data
- IV.C. The custodian is appointed by the appropriate Deputy Director, or designee, and is responsible for the administration of security controls as specified by the Department. This responsibility includes:
 - IV.C.1. Administering access to information or data
 - IV.C.2. Evaluating the cost-effectiveness of controls
 - IV.C.3. Providing physical and technical safeguards
 - IV.C.4. Providing procedural guidelines for the users
 - IV.C.5. Reporting any unauthorized use of information, data, or resources to the owner and the custodian's immediate supervisors
- IV.D. Users are responsible for:
 - IV.D.1. Complying with all controls established by the owner and custodian
 - IV.D.2. Ensuring that classified or sensitive information is not disclosed to anyone without permission of the owner
 - IV.D.3. Ensuring that his/her individual identification and passwords are not disclosed to, or used by, others as defined in ISP Directive SRV-218, "Computer Password Control."
 - IV.D.4. Reading and adhering to all applicable ISP security directives (listed in paragraph II.C.)
 - IV.D.5. Reporting any unauthorized use of information, data, or resources to the owner, custodian, and the immediate supervisor of the user discovering the violation.
 - IV.D.6. Using the information only for the purpose intended by the owner

- IV.D.7. Complying with the State's cybersecurity strategy including, but not limited to, the State's annual cybersecurity training.
- IV.E. Supervisors are responsible for:
 - IV.E.1. Ensuring personnel transferring into their unit are instructed to read all security directives at the time of transfer.
 - IV.E.2. Reporting any violation of security directives to their immediate supervisor, and the Division RCC.
 - IV.E.3. Ensuring subordinate personnel comply with the State's cybersecurity strategy and complete annual cybersecurity training as prescribed by DoIT.
 - IV.E.4. Reporting any cybersecurity deficiencies to the appropriate Deputy Director through the chain-of-command.

V. PROCEDURES

- V.A. Users are required to take necessary precautions to ensure the integrity and security of all resources used to accomplish the goals of the ISP and the state of Illinois.
- V.B. Neither the Department nor any individual employed by the Department shall:
 - V.B.1. Publicly post or publicly display in any manner any individual's SSN.
 - V.B.2. Print any individual's SSN on any card required for the individual to access products or services provided by the Department.
 - V.B.3. Require an individual to transmit his or her SSN over the Internet, unless the connection is secure or the SSN is encrypted.
 - V.B.4. Print an individual's SSN on any materials that are mailed in any form whatsoever to the individual, unless state or federal law requires the SSN to be on the document to be mailed.
 - V.B.4.a. However, SSNs may be included in applications and forms sent by mail, including, but not limited to:
 - V.B.4.a.1) Any material mailed in connection with the administration of the Unemployment Insurance Act.
 - V.B.4.a.2) Any material mailed in connection with any tax administered by the Department of Revenue.
 - V.B.4.a.3) Documents sent as part of an application or enrollment process or to establish, amend, or terminate an account, contract, or policy or to confirm the accuracy of the SSN.
 - V.B.4.b. A SSN that may permissibly be mailed under this Section may not be printed, in whole or in part, on a postcard or other mailer that does not require an envelope or be visible on an envelope without the envelope having been opened.
 - V.B.5. Collect, use, or disclose a SSN from an individual, unless:
 - V.B.5.a. Required to do so under state or federal law, rules, or regulations; or
 - V.B.5.b. The collection, use, or disclosure of the SSN is otherwise necessary for the performance of that agency's duties and responsibilities; and
 - V.B.5.c. The need and purpose for the SSN is documented before collection of the SSN; and
 - V.B.5.d. The SSN collected is relevant to the documented need and purpose.
 - V.B.6. Require an individual to use his or her SSN to access an Internet website.
 - V.B.7. Use the SSN for any purpose other than the purpose for which it was collected.

- V.B.8. The above prohibitions in V.B.5., V.B.6., and V.B.7. do not apply in the following circumstances:
- V.B.8.a. The disclosure of SSNs to agents, employees, contractors, or subcontractors to another governmental entity or its agents, employees, contractors, or subcontractors if disclosure is necessary in order for the entity to perform its duties and responsibilities; and, if disclosing to a contractor or subcontractor, prior to such disclosure, the ISP must first receive from the contractor or subcontractor a copy of the contractor's or subcontractor's policy that sets forth how the requirements imposed under this Act on a governmental entity to protect an individual's SSN will be achieved.
 - V.B.8.b. The disclosure of SSNs pursuant to a court order, warrant, or subpoena
 - V.B.8.c. The collection, use, or disclosure of SSNs in order to ensure the safety of:
 - V.B.8.c.1) State and local government employees
 - V.B.8.c.2) Persons committed to correctional facilities and local jails
 - V.B.8.c.3) Other law-enforcement facilities or retention centers
 - V.B.8.c.4) Wards of the state
 - V.B.8.c.5) All persons working in or visiting a state government agency facility
 - V.B.8.d. The collection, use, or disclosure of SSNs for internal verification or administrative purposes
 - V.B.8.e. The disclosure of SSNs to any entity or a governmental agency for the collection of:
 - V.B.8.e.1) Delinquent child support
 - V.B.8.e.2) Any state debt
 - V.B.8.e.3) Information to assist with an investigation or the prevention of fraud
 - V.B.8.f. The collection or use of SSNs to:
 - V.B.8.f.1) Investigate or prevent fraud
 - V.B.8.f.2) Conduct background checks
 - V.B.8.f.3) Collect a debt
 - V.B.8.f.4) Obtain a credit report from a consumer reporting agency under the federal Fair Credit Reporting Act
 - V.B.8.f.5) Undertake any permissible purpose that is enumerated under the federal Gramm Leach Bliley Act
 - V.B.8.f.6) Locate a missing person, a lost relative, or a person who is due a benefit, such as a pension benefit or an unclaimed property benefit
- V.C. The Academy will develop and provide training to all Cadets on:
- V.C.1. Protecting the confidentiality of personal information including SSNs.
 - V.C.2. Redacting personal information including SSNs.
 - V.C.3. Proper handling/storage of information (both printed and electronic) that contains personal information and/or SSNs from the time of collection through the destruction of the information.
- V.D. The Department will prepare and disseminate initial department training on the confidentiality of personal information and SSNs.
- V.E. New code employee hires will review this ISP directive and sign a receipt acknowledging they have read and understood the Department's information security policy.
- V.F. The Department adheres to the State's cybersecurity strategy and will disseminate annual cybersecurity training as prescribed by DoIT.

NOTE: Each contractor or vendor will read this directive and sign a form acknowledging they have read and understood the Department’s information security policy as part of their background paperwork submission.

V.G. Each Deputy Director, or designee, will ensure:

- V.G.1. Only employees required to use or handle information or documents that contain SSNs have access to such information or documents.
- V.G.2. SSNs are easily redacted from a document if the document containing the SSN could be released as part of a public records request.
- V.G.3. When requesting a SSN, or upon request by an individual, that the purpose(s) for collecting and using the SSN is provided.
- V.G.4. Documents containing personal information are safely stored where names and personal information of individuals are not easily visible and/or accessible to persons outside the work unit.
- V.G.5. Drafts and/or originals of documents containing personal information are shredded or otherwise destroyed to protect the personal information.

V.H. Prior to returning copy machines to the vendor, the Division RCC will ensure the storage device/hard drive is cleared of all information as required by standards for media sanitization.

- V.I. Personnel will **not** place documents containing personal information in a garbage can or a recycle bin.
 - V.I.1. All forms and documents containing names and other personal information must be shredded or otherwise destroyed to protect the personal information.
 - V.I.2. Contact your supervisor if you need to dispose of documents containing personal information and do not have access to a shredder.

V.J. Notification of a security breach

If/when there has been a breach in the security of personal information, the Department will notify, at no charge, those Illinois residents so affected.

- V.J.1. The Division of Internal Investigation will be notified to begin an investigation into the breach of security and take appropriate disciplinary action.
- V.J.2. The Legal Office will be notified to handle the notification to Illinois residents.
 - V.J.2.a. Notification to Illinois residents must be made in the most expedient and timely method possible and without unreasonable delay.
 - V.J.2.b. Notice to Illinois residents of the security breach of personal information may be through the following methods:
 - V.J.2.b.1) Written notice
 - V.J.2.b.2) Electronic notice
 - V.J.2.b.3) If the cost of providing notice would exceed \$250,000, notice may be made by:
 - V.J.2.b.3)a) E-mail notice if the ISP has the e-mail address of those affected
 - V.J.2.b.3)b) Conspicuous notice on the ISP website
 - V.J.2.b.3)c) Notification to major statewide media

NOTE: If the ISP must notify more than 1,000 Illinois citizens of the breach of security, the ISP will also notify, without undue delay, all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis of the security breach of personal information.

- V.K. Failure to abide by ISP security directives will subject the user to appropriate discipline as indicated in ISP Directive PER-030, "Complaint and Disciplinary Investigations," PER-103, "Code Employee Disciplinary Rules," or ROC-002, "Rules of Conduct."

| Indicates new or revised items.

-End of Directive-