ILLINOIS STATE POLICE DIRECTIVE
SRV-229, CYBERSECURITY

RESCINDS:	**REVISED:**
SRV-229, 2024-023, revised 04-15-2024	02-06-2025 **2025-007**
RELATED DOCUMENTS:	**RELATED CALEA STANDARDS (6th Edition):**
PER-008, PER-012, SRV-200, SRV-201, SRV-204, SRV-208, SRV-216, SRV-218, SRV-223, SRV-225, SRV-226, SRV-227, SRV-228	11.4.4

I. POLICY

I.A. The Illinois State Police (ISP):

I.A.1. Will reduce the risk posed to ISP due to the loss, disruption, or corruption of information and information systems, and comply with applicable state, federal, and industry laws, rules, and regulations related to information security.

I.A.2. Is a client agency of the Department of Innovation and Technology (DoIT), and as such, while maintaining appropriate oversight, defers to DoIT to establish a Cybersecurity Program that supports the business mission, goals, and objectives of the ISP while preventing or limiting the adverse effects of a failure, interruption, or security breach of state of Illinois and the ISP's information systems.

I.B. The State of Illinois Cybersecurity Program is owned and controlled by DoIT focusing on the core concepts of confidentiality, integrity, availability, and privacy. The ISP will collaborate with DoIT to ensure its employees and vendors adhere to this program by:

I.B.1. Providing every person who has access to its information technology (IT) resources with a copy of the DoIT Acceptable Use Policy.

I.B.2. Requiring every person who has access to its IT resources to complete DoIT-managed annual cyber awareness training that includes information on where to access DoIT's Acceptable Use Policy.

I.B.3. Working to reduce the security risks posed to its information systems due to unauthorized or unintentional access, while meeting the access requirements for authorized users.

I.B.4. Planning for contingencies by developing a coherent, organized, and strategic plan for continuing business activities in the event of disruptive information system events.

I.B.5. Minimizing the impact of Agency Information Security Incidents within acceptable levels.

I.B.6. Reducing the risk to electronic or physical media containing ISP information and limit potential mishandling or loss while being stored, accessed, or transported to and from the information systems.

I.B.7. Protecting the ISP's IT resources by limiting and controlling physical access to protect the physical environment in which the ISP's IT assets are housed.

I.B.8. Ensuring that planning activities are accomplished to provide protection to the confidentiality, integrity, and availability of the ISP's information resources.

II. AUTHORITY

II.A. 20 ILCS 450/25, "Data Security on State Computers Act," "Mandatory State employee training"

II.B. 5 ILCS 430, "State Officials and Employees Ethics Act"

II.C. DoIT Acceptable Use Policy
II.D. DoIT Security Awareness Training Policy

III. DEFINITIONS

III.A. Dormant account – user accounts that have been inactive for 60 days or more.

III.B. Information System Resiliency – the set of applications, data, and system environments required to be preserved across an outage of the production system.

III.C. Privacy Officer – the ISP Ethics Officer.

III.D. System Administrator – the person identified as having authority to grant access to an information system.

III.E. Users – any employee, contractor, or third-party person who has unescorted access to Illinois IT resources, data, or secured facilities

IV. RESPONSIBILTIES

IV.A. The Division of Justice Services (DJS) Deputy Director is responsible for:

IV.A.1. Assuming responsibility for operating an information system at an acceptable level of risk to operations, assets, individuals, and other organizations.

IV.A.2. Reviewing and approving the data classification and system categorization assigned to the information types and information system.

IV.A.3. Approving security plans and Plans of Actions and Milestones (POAMs).

IV.A.4. Determining whether significant changes require reauthorization.

IV.A.5. Reviewing and updating the Information Security Incident Response Plan in consultation with DoIT. (Refer to Addendum 2 of this directive.)

IV.B. The Deputy Directors of each division and the Chief of Staff (COS) for the Director are responsible for:

IV.B.1. Ensuring system users and support personnel receive requisite training, including but not limited to information security awareness training.

IV.B.2. Documenting and tracking Information Security Incidents consistent with the Department's Information Security Incident Response Plan and protects such plan from unauthorized public disclosure and modification.

IV.B.3. Maintaining an inventory that contains a listing of all programs and information systems under their control identified as collecting, using, maintaining, or sharing Personal Identifiable Information (PII).

IV.B.4. Ensuring the completion of DoIT's initial risk assessment form when a new application for a state mobile device is needed.

IV.C. System Administrators are responsible for:

IV.C.1. Addressing the operational need of the user community and for ensuring compliance with information security requirements, including but not limited to, appropriate background screening consistent with ISP policies and standards as outlined in ISP Directive, PER-008, "Employment Standards."

IV.C.2. Assigning and documenting the initial information classification and periodically reviewing the classification to ensure it accurately reflects the risks associated with the potential loss of the confidentiality, integrity, and availability of the information and information system.

IV.C.3. Integrating the minimum baseline security controls based on the categorization of the information.

IV.D. The Privacy Officer is responsible for developing, implementing, and maintaining a privacy program to ensure compliance with applicable laws and regulations regarding the collection, use, maintenance, sharing, and disposal of PII.

IV.E. Pursuant to the current Intergovernmental Agreement (IGA) between DoIT and the ISP, DoIT has accepted responsibility for:

IV.E.1. Developing policies, standards, and procedures to manage compliance requirements and prevent or limit the adverse effects of a failure, interruption, or security breach of the ISP's information systems.

IV.E.2. Focusing its cybersecurity efforts on the core concepts of confidentiality, integrity, availability, and privacy in compliance with all applicable Illinois and federal laws.

IV.F. The ISP Legal Office is responsible for:

IV.F.1. Reviewing all submitted DoIT initial risk assessment forms.

IV.F.2. Approving or denying the requested application(s) based on their final review of DoIT's findings and recommendations. The ISP Legal Office should work with the Chief Information Officer (CIO) when necessary.

IV.F.3. Providing the final determination to the requestor whether ISP is going to utilize the application based on the findings and recommendations from DoIT's review.

V. PROCEDURES

V.A. The Deputy Director of each division and the Office of the Director (OOD) COS will:

V.A.1. Provide access to DoIT's Acceptable Use Policy to every person under their command who accesses IT resources as part of the onboarding process; and

V.A.2. Require employees under their command to complete DoIT-managed annual cyber awareness training that includes information on where to access DoIT's Acceptable Use Policy.

V.A.3. The Division of the Academy and Training (DAT) will track and report the completion of DoIT-managed cybersecurity training on an annual basis. Security Awareness Training is listed as a mandatory training within ISP Directive PER-012, "Education and Training." Each Deputy Director's office will assist the DAT to ensure all employees under their command have completed the training by calendar year-end, or before.

V.A.4. Ensure that only employees who are required to use or handle information or documents that contain social security numbers shall have access to such information or documents.

V.A.5. Ensure employees under their command adhere to the requirements of:

V.A.5.a. The FBI's Criminal Justice Information Services (CJIS) Security Policy.
V.A.5.b. The Health Insurance Portability and Accountability Act (HIPAA).
V.A.5.c. The guidance set forth in the Internal Revenue Service's Publication 1075: Tax Information Security Guidance – for Federal, State and Local Agencies (Publication 1075).

V.A.6. Obtain the results of vulnerability scans from DoIT, when available, to ensure timely corrective actions are taken to correct identified vulnerabilities. Documentation of corrected actions implemented shall be retained at the Division level.

V.A.7. Document actions taken to remediate the risk(s) identified in the ISP Office of Inspections and Audits (OIA) risk assessments of design of major new systems or major modifications to systems. Documentation of the corrected actions shall be retained by the OIA.

V.A.8. Review any completed DoIT initial risk assessment forms submitted through the chain-of-command for state mobile device applications for inclusion on the Apps@Work store.

V.A.8.a. The form is located on the ISP Document Library and must be approved by both the ISP Chief Legal Counsel and the Agency CIO.

V.A.8.b. Before submitting the completed form to the ISP Legal Office, the Deputy Director's Office will email the ISP Telecommunication Section at ISP.TelcoRequests@illinois.gov to confirm the application requested is not already approved.

V.A.8.c. If the application has not been previously approved, the Deputy Director's Office will send the completed form to the ISP Legal Office. Once the required signatures have been obtained, the form shall be submitted to DoIT Security Engineering for review at DoIT.Security.Engineering@illinois.gov.

V.B. The DJS will:

V.B.1. Identify System Administrators that can grant approval for access to information systems.

V.B.2. Create a process for removing access to information systems when no longer required.

V.B.3. Create a process for removing dormant accounts.

V.B.4. Schedule and complete a Business Impact Analysis with DoIT every other year, at a minimum.

V.B.5. Identify an internal contact (Incident Response Breach Designated Contact) to coordinate breach response/reporting efforts for the Agency.

V.B.6. Create and maintain a Breach Notification Plan that incorporates the requirements of Illinois 815 ILCS 530/12 – Notice of breach; State agency. (Refer to Addendum 1 of this directive.)

V.B.7. Establish background screening criteria for individuals requiring unescorted access to agency facilities and IT resources.

V.B.8. Utilize security solutions such as BitLocker, Zscaler, Beyond Trust, or similar, to manage the security and resilience of our assets.

V.B.9. Ensure the ISP Telecommunication Section checks with DoIT to confirm if mobile device applications have already been approved when requested. The Telecommunication Section will inform the requesting Deputy Director's Office of their findings.

V.C. System Administrators will:

V.C.1. Work with appropriate staff to remediate control deficiencies.

V.C.2. Establish and maintain Information System Resiliency Requirements based on business impact analyses.

V.C.3. Serve as the approval authority for access requests from other business units or delegates approval authority to a representative in the same business unit.

V.D. The Privacy Officer will:

V.D.1. Review an inventory that contains a listing of all programs and information systems identified as collecting, using, maintaining, or sharing PII.

V.D.2. Define techniques or methods to ensure secure deletion or destruction of PII (including originals, copies, and archived records).

V.E. Users will:

V.E.1. Report suspected Information Security Incidents to ISP.Security@illinois.gov immediately following the discovery of a suspected Information Security Incident.

V.E.2. Complete DoIT-managed annual cyber awareness training that includes information on where to access DoIT's Acceptable Use Policy.

V.E.3. Adhere to the requirements of:

V.E.3.a. All applicable ISP policy for authorizing, tracking, and destroying any data extracted from systems.
V.E.3.b. The FBI's Criminal Justice Information Services (CJIS) Security Policy.
V.E.3.c. The Health Insurance Portability and Accountability Act (HIPAA).
V.E.3.d. The guidance set forth in the Internal Revenue Service's Publication 1075: Tax Information Security Guidance - for Federal, State and Local Agencies (Publication 1075).

V.E.4. Only request social security numbers for the purpose of collection/use when supported by Illinois law. Employees who are required to use or handle information or documents that contain social security numbers shall:

V.E.4.a. Ensure they are placed in a manner that makes the social security number easily redacted if required to be released as part of a public records request.
V.E.4.b. Complete mandator DoIT Security Awareness training that includes the proper handling of information that contains social security numbers from the time frame of collection through the destruction of the information. Users will also review and follow ISP Directive SRV-200, "Information Security and Disposal of Personal Information."

V.F. The ISP Legal Office will:

V.F.1. Review all DoIT initial risk assessment forms submitted by the OOD or the Deputy Director's Office. If approved, ISP's Legal Office will obtain the Agency CIO's approval and will return the completed form to the requestor for submission to DoIT.

V.F.2. Inform the requesting Deputy Director's Office of their final determination based on the findings and recommendations from DoIT's review.

Indicates new or revised items.

-End of Directive-

ILLINOIS STATE POLICE DIRECTIVE
SRV-229, CYBERSECURITY
ADDENDUM 1, BREACH NOTIFICATION PLAN

RESCINDS:	**REVISED:**
SRV-229, 2024-023, revised 04-15-2024	02-06-2025 **2025-007**
RELATED DOCUMENTS:	**RELATED CALEA STANDARDS (6th Edition):**
PER-008, PER-012, SRV-200, SRV-201, SRV-204, SRV-208 SRV-216, SRV-218, SRV-223, SRV-225, SRV-226, SRV-227, SRV-228	11.4.4

I. PURPOSE

This addendum will establish a Breach Notification Plan for the Illinois State Police (ISP) by providing a guideline in the event of a personal information breach or a breach of the security of the system data requiring Illinois residents and other entities and persons to be notified in accordance with the Personal Information Protection Act (815 ILCS 530).

II. Definitions

II.A. Breach – any unauthorized access to or release of such information, whether intentional or accidental.

II.B. Personal identifiable information (PII):

II.B.1. An individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted or redacted or are encrypted or redacted but the keys to unencrypt or unredact or otherwise read the name or data elements have been acquired without authorization through the breach of security:

II.B.1.a. Social security number.
II.B.1.b. Driver's license number or state identification card number.
II.B.1.c. 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.
II.B.1.d. Medical information.
II.B.1.e. Health insurance information.
II.B.1.f. Unique biometric data generated from measurements or technical analysis of human body characteristics used by the owner or licensee to authenticate an individual, such as a fingerprint, retina or iris image, or other unique physical representation or digital representation of biometric data.

II.B.2. Username or email address, in combination with a password or security question and answer, that would permit access to an online account, when either the username or email address or password or security question and answer are not encrypted or redacted or are encrypted or redacted but the keys to unencrypt or unredact or otherwise read the data elements have been obtained through the breach of security.

II.B.3. Personal information does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.

III. Responsibilities – whenever a Breach of PII occurs as a result of a breach of the security of ISP's system data, the ISP will coordinate its response with Department of Innovation and Technology (DoIT), Division of Information Security.

IV. Procedures – all breaches of PII will be handled in accordance with the Personal Information Protection Act (PIPA), 815 ILCS 530.

IV.A. Any employee who becomes aware of a breach will report it to their supervisor who will notify the Deputy Director's Office through their chain-of-command without delay, but no later than 24 hours following the discovery.

IV.B. DoIT will:

IV.B.1. Consider the nature of the compromise, the type of information taken, and the extent of the breach and provide the ISP with a summary of their findings consistent with the current Intergovernmental Agreement (IGA) between the two agencies; and

IV.B.2. Will make all required notifications to the Office of the Chief Information Security Officer of DoIT.

IV.C. The Deputy Director of the Division responsible for the breach will:

IV.C.1. Consider the likelihood of misuse, the potential damage arising from misuse, and consult with ISP Legal regarding ISP's obligations to report the breach consistent with state and federal law.

IV.C.2. Notify the Deputy Director of DJS to ensure appropriate actions are taken by DoIT on behalf of ISP.

IV.C.3. Notify the Office of the Director (OOD) without delay, but no later than 24 hours following the discovery of the breach, as well as the recommendation of ISP Legal regarding reporting responsibilities; and

IV.C.4. Upon approval from the OOD, make all required notifications to affected individuals and coordinate notification to the General Assembly with the ISP Office of Governmental Affairs.

IV.D. ISP Legal will provide guidance and direction regarding any notifications that must be made pursuant to the Personal Information Protection Act (815 ILCS 530).

IV.E. ISP Governmental Affairs will make notification to the General Assembly where necessary.

IV.F. Depending upon the nature of the breach, ISP may elect to defer to DoIT, Division of Information Security, to make all required notifications but only upon approval from the Director of the ISP.

-End of Addendum-

ILLINOIS STATE POLICE DIRECTIVE
SRV-229, CYBERSECURITY
ADDENDUM 2, INFORMATION SECURITY INCIDENT RESPONSE PLAN

RESCINDS:	**REVISED:**
SRV-229, 2024-023, 04-15-2024	02-06-2025 **2025-007**
RELATED DOCUMENTS:	**RELATED CALEA STANDARDS (6th Edition):**
PER-008, PER-012, SRV-200, SRV-201, SRV-204, SRV-208 SRV-216, SRV-218, SRV-223, SRV-225, SRV-226, SRV-227, SRV-228	11.4.4

I. PURPOSE

This addendum will establish capability to effectively manage Information Security Incidents with the objective of minimizing impacts and maintaining or restoring normal operations.

II. DEFINITIONS

II.A. Information Security Incident – A violation or imminent threat of a violation of information security policies, acceptable use policies, or standard security practices. The definition of an Information Security Incident includes, but is not limited to:

II.A.1. Attempts (either failed or successful) to gain unauthorized access to a system or its data

II.A.2. Unwanted disruption or denial of service

II.A.3. Discovery of network intrusions including botnet

II.A.4. Malware events

II.A.5. Unauthorized use of a system for the processing or storage of data

II.A.6. Changes to system hardware, firmware, or software characteristics without the owner's knowledge, instruction, or consent

II.A.7. Unplanned, unauthorized, or unexpected change to security baselines, including an unauthorized change to security controls, technologies, or processes

II.A.8. Inappropriate release of personally identifiable or other confidential information

II.A.9. Theft or loss of information technology (IT) equipment that could contain non-public information

II.A.10. Violation of information security policies

II.B. Information Security Incident Response Plan – A predetermined set of instructions or procedures to detect, respond to, and limit consequences of a malicious cyberattack against state of Illinois information systems.

III. PROCEDURES

III.A. Employees of the ISP shall report any Information Security Incidents to their immediate supervisor without delay, but no later than 24 hours following the discovery of an Information Security Incident.

III.B. The immediate supervisor will notify the respective Deputy Director's Office through the chain-of-command without delay, but no later than 24 hours following the discovery.

III.C. Third-party providers of the ISP's information systems will develop and maintain an applicable Information Security Incident Response Plan that meets or exceeds the requirements defined in this addendum, which shall be protected from unauthorized public disclosure.

.

III.D. Information Security Incident response training will be provided to ISP employees by DoIT on an annual basis.

-End of Addendum-