
REGIONAL INFORMATION SHARING SYSTEMS[®] (RISS) PROGRAM

Privacy Policy



Contents

1. Introduction and Purpose Statement
2. Definitions
3. 28 CFR Part 23 Compliance
4. Policy Applicability and Legal Compliance
5. Governance and Oversight
6. RISS Information Technology Resources
7. New Information Technology Initiatives
8. RISS Database Information Collection
9. Data Quality
10. Collation and Analysis
11. Access
12. Security
13. Use
14. Training
15. Audits
16. Evaluation and Monitoring
17. Accountability
18. Revision and Amendments

August
2009

| | | |
|----------------------------------|-----------------------------------|-----------|
| Approval Date: August 6, 2009 | Effective Date: August 6, 2009 | Revision: |
|----------------------------------|-----------------------------------|-----------|

1. Introduction and Purpose Statement

The Regional Information Sharing Systems (RISS) Program was established almost four decades ago, primarily to promote law enforcement information sharing. Information sharing is a critical element in effectively and efficiently detecting, deterring, apprehending, and prosecuting criminals and terrorists. Because of the focused effort by law enforcement and criminal justice agencies from all levels of government, numerous improvements have been made in recent years to ensure that the right individuals receive the right information at the right time. The way law enforcement conducts business today is much different from just a few years ago, with the information superhighway evolving faster each day. It is vital that the law enforcement community have the capability to instantly communicate and share information. Likewise, law enforcement must also protect, respect, and uphold the privacy, civil rights, and civil liberties of individuals.

RISS supports law enforcement and public safety efforts in a variety of ways, including information sharing, analytical support, equipment and financial loans, training, publications, field services, and technical assistance. The intent of this RISS Privacy Policy is to address the proper handling of personally identifiable information housed in resources operated by the RISS Program to safeguard the rights of individuals.

This privacy policy was developed in accordance with the U.S. Department of Justice's Global Justice Information Sharing Initiative (Global) *State and Local Privacy Policy Development Template: Privacy, Civil Rights, and Civil Liberties Policy Workbook*.

2. Definitions

- A. Authorized User—an individual who has successfully completed the RISS identification and approval process or who is accessing RISS resources through an established federated identity partnership and has been granted permissions to appropriate information technology resources available via RISS.
- B. Electronic Communication—any communication that is broadcast, created, sent, forwarded, replied to, transmitted, stored, held, copied, downloaded, displayed, viewed, read, or printed by one or several electronic systems, devices, or services.
- C. Law Enforcement Investigative Purpose—in the context of a request for information, the situation in which data can be directly linked to a criminal justice or law enforcement agency's active criminal investigation and operational case as a response to a confirmed investigative lead that requires follow-up or an otherwise authorized investigative activity.
- D. Personally Identifiable Information—one or more pieces of information that, when considered together or when considered in the context of how they are presented or how they are gathered, are sufficient to specify a unique individual. The pieces of information include:
 - Personal characteristics such as height, weight, gender, sexual orientation, date of birth, age, hair color, eye color, race, ethnicity, scars, tattoos, gang affiliation, religious affiliation, place of birth, mother's maiden name, distinguishing features, and biometric information such as fingerprints, DNA, and retinal scans.

-
-
- A unique set of numbers or characters assigned to a specific individual, including name, address, phone number, social security number, e-mail address, driver's license number, financial account, or credit card number and associated PIN number, Integrated Automated Fingerprint Identification System (IAFIS) identifier, or booking or detention system number.
 - Descriptions of events or points in time, including information in documents such as police reports, arrest reports, and medical records.
 - Descriptions of locations or places, including geographic information systems (GIS) locations, electronic bracelet monitoring information, etc.
- E. Policy Board—the policy board or executive committee established by each RISS Center and composed of representatives from member criminal justice agencies in the center's geographic service area. The primary purpose of the board is to provide direction affecting center policy, operation, and administration.
- F. RISS ATIX™ Participant—executive and official staff from governmental or nongovernmental entities involved with planning and implementing prevention, response, mitigation, and recovery efforts regarding terrorism, disasters, or other law enforcement and public safety strategic and tactical response efforts who have successfully completed the RISS identification and approval process for access to RISS ATIX resources.
- G. RISS Member Agency—a criminal justice or law enforcement agency or organization approved for membership by a RISS Center Policy Board and provided access to appropriate RISS services and resources.
- H. RISSNET™—the RISS Secure Intranet provides a Web-based nationwide criminal justice network that provides the secure communications backbone and infrastructure for sharing criminal intelligence and other law enforcement and public safety-related information. RISSNET provides a secure platform at the Sensitive but Unclassified (SBU)/Controlled Unclassified Information (CUI) level for communications among agencies, as well as access to various state and federal intelligence and information systems across the country.
- I. RISSNET Node/Node Partner—any local area network (LAN) or wide area network (WAN) electronically connected to RISSNET infrastructure via (1) a dedicated communications circuit and a RISSNET-compliant firewall or (2) an Internet Protocol Security/Virtual Private Network (IPsec VPN) connection and a RISSNET-compliant router.

3. 28 CFR Part 23 Compliance

- A. RISS complies with the *National Criminal Intelligence Sharing Plan* (NCISP). RISS and the NCISP firmly recognize the need to ensure that individuals' privacy, other civil liberties, and civil rights are protected throughout the intelligence and information sharing process.
- B. RISS endorses the NCISP guideline that ensures that "the collection, submission, access, storage, and dissemination of criminal intelligence information conforms to the privacy and constitutional rights of individuals, groups, and organizations" and that "law enforcement agencies shall adopt, at a minimum, the standards required by the Criminal Intelligence Systems Operating Policies federal regulation (28 CFR Part 23)."
- C. RISS Centers have adopted policy guidelines that fully comply with 28 CFR Part 23. All RISS member agencies have also agreed, in writing, to comply with the requirements of 28 CFR Part 23 with respect to any criminal intelligence information they submit into or receive from applicable RISS criminal intelligence databases.

-
-
- D. All RISS intelligence-related support activities are conducted in compliance with the 28 CFR Part 23 criminal intelligence system operating policies. This includes requirements governing receipt, storage, and maintenance of criminal intelligence information; exclusion of illegally obtained information; restrictions on dissemination; observance of administrative, technical, and physical safeguards (including establishment of audit trails); review and purge requirements; and forbidding the purchase or use of any electronic, mechanical, or other device for surveillance that is in violation of the provisions of the Electronic Communications Privacy Act of 1986 or applicable state law related to wiretapping or surveillance.

4. Policy Applicability and Legal Compliance

All RISS Center staff as well as participating agency users, private contractors, and other appropriate parties comply with the RISS Privacy Policy and applicable laws protecting privacy. A copy of this policy is available upon request and posted at the RISS public Web site, www.riss.net.

5. Governance and Oversight

RISS is a federally funded grant program administered by the U.S. Department of Justice (DOJ), Office of Justice Programs (OJP), Bureau of Justice Assistance (BJA). BJA establishes RISS service and operational guidelines in the BJA *Funding and Administration Guidelines of the RISS Program*, which governs provision of RISS services.

The RISS National Policy Group (RNPG) is composed of the six RISS Center Directors and the chair of each RISS Center's policy board (see Section 2. G.). The primary purpose of the RNPG is to provide direction affecting center policy, operation, and administration. The RNPG is responsible for strategic planning, resolution of operational issues, advancement of information sharing, and other matters affecting the RISS Program and RISS Centers.

The RISS Chief Executive Officer (CEO) serves under the authority of the RNPG. The CEO coordinates and consults with the RISS Directors. Under the direction of the CEO, the RISS Office of Information Technology (OIT) maintains RISSNET and develops and implements RISS resources provided via RISSNET. RISS OIT consists of three groups—the Applications Development Group (ADG), the Intranet Operations Group (IOG), and the Projects Support Group (PSG).

6. RISS Information Technology Resources

The following resources include electronic systems or databases available to authorized users via the RISS Secure Intranet (RISSNET):

- RISS National Criminal Intelligence Database (**RISSIntel**), as well as various state, regional, federal, and specialized criminal justice information systems.
- The 7th Instance of the RISS Suite of Applications (RISSApps), known as **RISS7**—an alternate criminal intelligence database for deployment and use in law enforcement agencies to store collected criminal intelligence data.
- **RISS National Gang Program (RISSGang)**—consists of a gang-related criminal intelligence database, secure bulletin board, and secure Web site.

-
-
- RISS Automated Trusted Information Exchange™ (RISS ATIX™)—includes secure Web pages, a bulletin board, a document library, and secure e-mail for law enforcement and public safety entities.
 - RISS Officer Safety Event Deconfliction System (RISSafe™)—stores and maintains data on planned law enforcement events with the goal of identifying and alerting affected law enforcement agencies to potential conflicts with other law enforcement agencies' events.
 - RISS Investigative Leads Bulletin Board (RISSLeads)—provides a secure electronic bulletin board that allows users to post information on a case or raise or respond to other law enforcement issues.
 - Data Visualization and Link Analysis Tool (RISSLinks™)—provides a data visualization tool that creates an analytical chart when a record is viewed by a user in RISSIntel or other connected databases.
 - Other resources include the RISS search engine (RISSearch), RISSTraining Web site (RISSTraining), individual RISS Center Web sites, and secure e-mail.
 - Other information technology resources operated by individual RISS Centers, such as investigative databases.

7. New Information Technology Initiatives

- A. The RNPG or individual RISS Centers may partner with other criminal justice entities to enhance information sharing programs or develop new programs and initiatives that further the RISS Program mission and goals. In these instances, the RNPG or RISS Center will conduct a privacy assessment of the new or emerging initiatives to ensure that they meet the tenets of this privacy policy. RISS will utilize the Global Privacy Impact Assessment (PIA) located at the Justice Information Sharing Web site (www.it.ojp.gov).
- B. This form will be completed, as appropriate, by the RNPG, appropriate RISS Center, or a designee and will be maintained by the RISS Chief Executive Officer, RISS Center, or designee.
- C. As needed, RISS will adjust the project strategy, technology specifications, this privacy policy, and/or other appropriate operating policies and procedures to ensure that privacy, other civil rights, and civil liberties are protected in the implementation of the new information sharing program or initiative.

8. RISS Database Information Collection

- A. Data submitted to RISSIntel, the RISSGang intelligence database, RISSafe, RISS7 instances, or any other RISS-maintained database is owned by the submitting member or nonmember agency.
- B. Appropriate information gathering and investigative techniques shall be conducted in compliance with and adhere to regulations and guidelines, including, but not limited to:
 - 1. 28 CFR Part 23 regarding collection of criminal intelligence information.
 - 2. The Organisation for Economic Co-operation and Development's Fair Information Principles (FIPs) (http://it.ojp.gov/documents/OECD_FIPs.pdf), which include:

-
-
- Collection Limitation Principle
 - Data Quality Principle
 - Purpose Specification Principle
 - Use Limitation Principle
 - Security Safeguards Principle
 - Openness Principle
 - Individual Participation Principle
 - Accountability Principle

3. NCISP recommendations regarding information and intelligence sharing.
4. Applicable constitutional, statutory, regulatory, and administrative rules and other legal provisions, as well as any other DOJ regulations that apply to multijurisdictional criminal intelligence databases.

- C. External agencies that access and share information with the RISS Program comply with the laws and rules governing those individual agencies in addition to this privacy policy, other RISS policies, and applicable federal and state laws and local ordinances.
- D. RISS will partner only with commercial database entities that provide appropriate assurances that their methods for gathering personally identifiable information comply with applicable local, state, territorial, federal, and tribal laws, statutes, and regulations and that these methods are based on lawful information collection practices.
- E. RISS will not seek or retain information about individuals or organizations solely on the basis of their religious, political, or social views or activities; their participation in a particular noncriminal organization or event; or their race, ethnicity, citizenship, place of origin, age, disability, gender, or sexual orientation.

9. Data Quality

- A. RISS will make every reasonable effort to ensure that information sought or retained is derived from dependable and trustworthy sources; accurate, current, and complete, including the relevant context in which it was sought or received and other related information; and properly merged with other information about the same individual or organization.
- B. Originating agencies external to RISS are responsible for the quality and accuracy of the data accessed by or provided to RISS. If data is alleged, suspected, or found to be inaccurate, incomplete, out of date, or unverifiable, RISS will advise the appropriate contact person in the originating agency. The originating agency is responsible for then confirming (as accurate), correcting, or purging the information from the RISS resource within a reasonable time. Recipients of the information will be notified of errors or deficiencies that may affect the rights of the subject of the information.
- C. Depending upon the resource (e.g., RISSIntel, RISSGang, RISSafe), data provided by authorized users to RISS-supported systems shall:
 - Be based on proper criminal predicate or threat to public safety;
 - Be based on reasonable suspicion that an identifiable individual or organization has committed a criminal offense or is involved in or planning criminal or terrorist activity that presents a threat to any individual, the community, or the nation and that the information is relevant to the criminal (including terrorist) conduct or activity;

-
-
- Be relevant to the investigation and prosecution of suspected criminal or terrorist incidents; the enforcement of sanctions, orders, or sentences; or the prevention of crime;
 - Be relevant in a criminal analysis or in the administration of criminal justice and public safety (including topical searches);
 - Support authorized public safety and private sector efforts, as appropriate, and facilitate information sharing and communications among these entities; or
 - Protect officer safety and ensure the integrity of investigative efforts.

The data shall also be derived from a source that is reliable and information that has been verified or where limitations on the information's quality are identified. The information must be collected in a lawful manner, with the knowledge and consent of the individual, if appropriate.

10. Collation and Analysis

- A. Users submitting information to RISS-supported systems are authorized individuals from member agencies or appropriate nonmember law enforcement, public safety, or private sector entities. These individuals are sworn law enforcement officers, intelligence analysts, criminal justice officials, public safety officials, and appropriate critical infrastructure and private entity officials. As necessary, RISS may provide limited information, such as contact phone numbers, to appropriate RISS members to facilitate communications and enhance information sharing. For example, ATIX Participant information is provided at the secure ATIX Web site for participants to obtain phone numbers of individuals addressing similar public safety issues.
- B. Users are permitted to access only information and systems specifically authorized for their use.
- C. Information acquired or received by RISS or accessed from other sources will be analyzed only by qualified individuals who have successfully completed a background check and appropriate security clearance, if applicable, and who have been selected, approved, and trained accordingly.
- D. Information acquired or received by RISS or accessed from other sources is analyzed according to priorities and needs to:
 - 1. Further crime prevention (including terrorism), law enforcement, force deployment, or prosecution objectives and other priorities established by RISS;
 - 2. 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 or terrorist activities;
 - 3. Support investigations, including those of gang activity, criminal violence, illegal narcotics, cybercrime, terrorism, human trafficking, identity theft, and other appropriate crimes;
 - 4. Support and facilitate public safety and private sector efforts safeguarding critical infrastructure and responding to disasters; or
 - 5. Ensure officer safety.

11. Access

- A. Use of RISSNET is limited to those individuals who have successfully completed the RISS identification and approval process and have received appropriate training (users).
- B. Users must complete an Individual User Agreement or equivalent application or acknowledgement or be covered by an interagency Memorandum of Understanding, in conjunction with training provided.
- C. RISS retains the right to suspend or withdraw membership and user privileges, as deemed appropriate, in instances of violation of this or any other RISS policy.
- D. Authorized users are subject to the RISSNET Security Policy, RISSNET Electronic Communications Policy, the RISSNET Remote User Authentication and Access Control Policy, and other RISS-related policies.
- E. In order to confirm the identity of individual RISSNET users and to ensure that user impersonation is prevented, RISSNET users must provide a variety of personal information about themselves to enable RISS to ensure that only appropriate individuals are permitted access to information for which they have a “need to know” and “right to know.”
- F. Personal identifying information provided by authorized users for the purpose described in Section 11. E., including membership and user information, shall be protected under this policy.
- G. RISS employs and continuously reviews and refines appropriate security and privacy control measures—including physical, electronic, and organizational measures—to ensure that individual identification information is safeguarded and is not compromised.
- H. All individuals having access to RISS resources agree to the following:
 - 1. Criminal intelligence and law enforcement databases accessible via RISSNET will only be used to perform official law enforcement investigative-related duties in a manner authorized by the user’s employer.
 - 2. Individual passwords will not be disclosed to any other person.
 - 3. Individual passwords will be changed if authorized personnel of the agency suspect the password has been improperly disclosed or otherwise compromised.
 - 4. Use of RISS in an unauthorized or illegal manner will subject the user to denial of further use of RISS resources, discipline by the user’s employing agency, and/or criminal prosecution. Each authorized user understands that access to RISS can be denied or rescinded for failure to comply with the applicable restrictions and use limitations.

12. Security

- A. RISS will operate secure facilities, whereby personnel maintain appropriate identification to enter the facility and visitors are required to check in and sign in upon entry. The facilities must also meet all appropriate local and state ordinances.
- B. RISS will ensure that security procedures are in place in order to safeguard human life and property.
- C. RISS will employ secure internal and external safeguards against network intrusion.
- D. Access to RISSNET resources will be allowed using only secure networking technologies, such as RISSNET’s IPsec VPN or RISSNET’s Multi-Protocol Label Switching (MPLS) circuits.

-
-
- E. RISS will grant access to its resources only to RISS staff or appropriate personnel whose positions and job duties require such access.

13. Use

- A. Use of RISS resources is limited to those individuals who have successfully completed the RISS identification and approval process or who are part of an interagency Memorandum of Understanding and have received appropriate training.
- B. Information obtained through RISS can be used only for the lawful performance of duties and/or for the purposes necessary for effective administration of RISSNET and RISSNET resource authentication and access control procedures.
- C. Information obtained through or stored by RISS cannot be (1) sold, published, exchanged, or disclosed for commercial purposes; (2) disclosed or published without prior approval of the contributing agency; or (3) disseminated to unauthorized persons.

14. Training

- A. RISS will ensure that staff, users, member agencies, and partners are trained and understand this privacy policy. Training will address the substance of the policy and its importance to the entity's mission and user responsibility, including potential consequences of violating the policy.
- B. Training may occur in any way that the RISS Center and member agency determines to be appropriate, based on available resources, the number of individuals to be trained, and other relevant factors.

15. Audits

- A. Section 3 of this privacy policy addresses RISS criminal intelligence databases regarding 28 CFR Part 23. RISS shall abide by the auditing requirements within that guideline.
- B. Systems that are not 28 CFR Part 23-compliant, such as investigative databases, will maintain an appropriate electronic log or auditing capability where available.
- C. RISS will routinely monitor logs for indications of unusual activity and take appropriate action, if necessary.

16. Evaluation and Monitoring

- A. RISS will continuously evaluate and monitor its resources, technologies, security practices, and associated processes to ensure compliance with this and all appropriate RISS policies.
- B. RISS will, through its six RISS Centers, conduct 28 CFR Part 23 compliance reviews of member agency processes. DOJ or RISS may request a third party to conduct additional reviews, as needed and appropriate.
- C. RISS will ensure that only appropriate personnel have access to staff, member, and user information.
- D. RISS will revise its practices, as appropriate, to ensure continued compliance and to stay abreast of issues impacting the privacy policy arena in order to ensure that all RISS policies and practices are up to date and appropriate.

-
-
- E. RISS will adopt and follow procedures and practices to ensure and evaluate the compliance of users with the provisions in abiding by this policy and applicable law. This will include periodic auditing.
 - F. If any individual has a complaint or objects to the accuracy or completeness of information about him or her that originates with another agency, RISS will acknowledge the complaint and, if appropriate, notify the originating agency of the complaint or request.

17. Accountability

- A. RISS Center staff or authorized users shall report violations or suspected violations of this policy to their immediate supervisor, as well as to the in-region RISS Center. The in-region RISS Center Director may resolve the matter as appropriate or engage assistance and consultation from the other Directors, the RISS CEO, and/or legal support to resolve the issue. Items arising that may impact all of the centers or the RISS Program's national initiatives shall be discussed and deliberated by the RNPG for resolution.
- B. If an authorized user is found to be in violation of the provisions of this policy, the RISS Center reserves the right to suspend or discontinue access to information by the user and/or request that the relevant member or nonmember agency, organization, contractor, or service provider employing the user initiate proceedings to discipline the user or enforce the policy's provisions.
- C. If any RISS Center staff member is found to be in violation of any provision of this policy, the RISS Center will reprimand, suspend, demote, transfer, or terminate the individual, as authorized by applicable personnel policies.
- D. In case of user or staff violations of the law, the RISS Center will refer the matter to appropriate authorities for criminal prosecution, as necessary, to comply with the law and effectuate the purposes of this policy.

18. Revision and Amendments

- A. The RNPG has the authority to amend any part(s) of this policy, as appropriate.
- B. At least annually, the RNPG will review this policy for content, relevancy, and effectiveness.
- C. A representative from a RISS Center, a RISS Director, the RISS CEO, RISS OIT, or other appropriate entity may request a change or revision to this policy by contacting the chair of the RNPG and will provide details regarding the proposed change and the reason/justification for the change. The requestor will provide feedback/discussion on the issue. Once any change is approved by the RNPG, the change will be made to this policy and a new version of this policy will be distributed. The staff, users, members, and other participants and partners will adhere to the most recent version of this privacy policy.
- D. If changes occur to related policies or regulations, such as other RISS policies or 28 CFR Part 23, the RNPG may revise this policy, as appropriate.
- E. Approved amendments to this policy shall be documented in meeting minutes, and the date of such action shall be logged herein.