

Privacy Policy & System Use Notification and Logging Acknowledgement

Version 0.2

Privacy Policy

Last Modified: 13 Oct 2026

1. Introduction.

10x National Security Inc. ("**Company**" or "**We**") respects your privacy. This policy describes the information we collect when you visit www.10xnationalsecurity.com (our "**Website**") or use any platform, application, software, or other product or service that we make available and that links to this policy, including the ORRIX Marketplace, associated with the Intelligence Community Data Consortium (ICDC) at 10xicdc.com, (together with the Website, the "**Services**"), and how we use, maintain, protect, and disclose it. This policy also applies to information we collect in electronic messages with you and in connection with our business development, recruiting, events, facility visits, and security operations. It does not apply to websites, platforms, or services that we do not control.

This policy is a notice of our practices. It is not a contract and does not create contractual rights or obligations for you or for Company. If you do not want your information handled as described in this policy, please do not use the Services. We may ask you to acknowledge this policy, and we keep a record of that acknowledgment. This policy may change from time to time (see Changes to Our Privacy Policy).

This policy covers information about users of the Services, such as account, contact, and usage information. It does not govern data that vendors or other third parties make available through the Services, such as data offered through the ORRIX platform ("**Vendor Data**"), including any personal information contained in Vendor Data. We handle Vendor Data under our agreements with vendors, including any applicable Data Processing Agreement.

2. Other Agreements.

Your use of certain Services may also be subject to an agreement between Company and the employer, agency, or other organization through which you access the Services ("**Your Organization**"), to platform-specific terms (such as the ICDC Platform Agreement and End User License Agreement), or to an additional privacy or system use notice. Your contractual rights and obligations, including rules about what you may submit to a Service and how platform activity is monitored, logged, and retained, are set out in those terms, which control over this policy to the extent of any conflict.

Where you access a Service on behalf of a U.S. Government agency, that agency may provide its own privacy notice, Privacy Act statement, or other notice governing its collection and use of information, and its handling of information you access through the Services may be subject to its own legal authorities and policies.

3. Information We Collect About You and How We Collect It.

"**Personal Information**" means information that identifies, relates to, or could reasonably be linked, directly or indirectly, with you or your device, such as your name, email address, telephone number, organization, username, internal user ID, or IP address, or as otherwise defined under applicable data protection laws. Aggregated or de-identified information is not Personal Information. We collect information directly from you and automatically as you use the Services, including usage details, IP addresses, log data, and cookie information.

4. Information You Provide to Us.

The information we collect on or through our Services may include:

- Information you provide in forms, problem reports, and correspondence with us.
- Account registration information, such as your name, email address, username, organization, role, and, where required for access to a Service, identity-verification information.
- Information you submit when using features of the Services, including prompts, inputs, and files you provide to any chat agent or other artificial-intelligence-enabled feature, and the outputs generated in response. This information is processed by our third-party AI providers to generate responses, as described in Section 9.
- Recruiting and employment information, such as resume or CV details, education, work history, qualifications, references, interview notes, compensation expectations, and eligibility to work, if you apply for a role with us.
- Security and facility information, such as visitor logs, badge and access records, arrival and departure times, and security camera footage where used, if you visit our facilities or attend our events.
- Compliance and diligence information needed for supplier, subcontractor, partner, customer, export control, sanctions, procurement, security, or regulatory reviews.
- Sensitive information, only where appropriate and permitted, such as government affiliation, citizenship or immigration status, security clearance information, disability or accommodation information, or demographic information voluntarily provided in recruiting or compliance contexts. We do not intentionally collect sensitive information through the Services unless you choose to provide it or it is necessary for a specific business, security, legal, or employment purpose.

We may also receive information from service providers, recruiting platforms, professional networks, references, background check providers, public sources, and customers, suppliers, contractors, partners, government entities, or other organizations involved in our work.

5. Information We Collect Through Automatic Data Collection Technologies.

As you use the Services, we automatically collect details of your visits and the resources you access, and information about your device and internet connection, such as IP address, device identifiers, operating system, and browser type. When you are logged in, this information is associated with your account. We use it to secure, maintain, and improve the Services, understand usage patterns, and remember your preferences. These technologies may include cookies, which you can refuse through your browser settings, although some parts of the Services may then not function properly.

Based on the current implementation of our public Website, we do not use third-party advertising pixels, cross-site retargeting tags, or session replay tools. If we add such technologies, we will update this policy and provide any legally required notice, consent, or opt-out mechanism.

6. Security and Audit Logging.

Certain Services, including the ORRIX platform, are monitored systems. On those

Services, we record security and audit logs of user activity, which may include account and user identifiers, authentication events (such as logins, logouts, and failed login attempts), records of your acceptance of terms and acknowledgment of policies and notices, access to features and data, administrative and permission changes, prompts, inputs, and outputs of features of the Services, timestamps, IP addresses, and device and session information. We use these logs to administer and secure the Services, enforce applicable terms, investigate suspected misuse, and meet legal, contractual, security, accreditation, and audit obligations. Logs may be reviewed by authorized personnel and, as described in this policy, disclosed to Your Organization, government customers, and appropriate authorities. A system use notification describing monitoring and logging may be presented on the applicable Service before you access it.

7. Information You Should Not Submit.

The Services are not designed to receive certain types of information, and we ask that you not submit any of the following unless its submission has been expressly authorized in writing by the applicable government customer or Company, is permitted by any applicable executed order document, and is consistent with applicable law: classified information; export-controlled data; protected health information (as defined under the Health Insurance Portability and Accountability Act (“**HIPAA**”)); payment card data or financial account numbers; government-issued identification numbers; biometric information; Personal Information of children; or other highly regulated or sensitive data. The rules that govern what you may submit to a Service are set out in the applicable platform terms. Information submitted through public Website channels may not be treated as confidential unless a separate written agreement applies, so please do not send classified, export-controlled, proprietary, sensitive, or confidential information through those channels.

8. How We Use Your Information.

We use information that we collect about you or that you provide to us, including any Personal Information:

- To provide and present the Services and any information or services you request.
- To carry out our obligations and enforce our rights arising from any contracts entered into between you or Your Organization and us, including the terms that govern your use of the Services.
- To notify you about changes to our Services or any products or services we offer or provide through them.
- To create and administer accounts, authenticate users, and control access to the Services.
- To maintain records of your acceptance of our terms and policies and of your privacy choices.
- To protect the security and integrity of the Services, and to detect, investigate, and prevent security incidents, fraud, misuse, and unauthorized access.
- To comply with our legal, contractual, regulatory, and audit obligations.
- To process job applications, evaluate candidates, and support recruiting.
- To evaluate vendors, subcontractors, partners, and potential business relationships.
- To manage events, facility access, visitor records, and physical security.
- For any other purpose described when you provide the information or with your consent.

9. Disclosure of Your Information.

We do not sell your Personal Information. We may disclose aggregated or de-identified information for any lawful purpose and will not attempt to re-identify it except as permitted by law.

We may disclose Personal Information that we collect or you provide as described in this privacy policy:

- To our subsidiaries and affiliates.
- To contractors, service providers, and subprocessors we use to support our business, such as cloud hosting, cybersecurity, analytics, communications, identity, and artificial intelligence service providers, who are contractually bound to keep Personal Information confidential and use it only for the purposes for which we disclose it.
- To Your Organization, including its account administrators, who may access information about your account and your activity on the Services.
- To customers, partners, suppliers, and contractors, where needed to evaluate, perform, or support business relationships and contracts.
- To professional advisors, such as attorneys, auditors, accountants, insurers, and consultants.
- To government customers, as necessary to administer orders and access, provide usage reporting, and notify them of suspected misuse, security incidents, or violations affecting them. We provide vendors usage metrics and information needed to administer orders, verify compliance with license terms, and address suspected misuse of, or unauthorized access to, their Vendor Data. We do not otherwise disclose your prompts, inputs, or outputs to vendors.
- To potential investors, lenders, acquirers, buyers, or other successors, and their advisors, in connection with a financing, merger, divestiture, restructuring, reorganization, dissolution, or other sale or transfer of some or all of Company's assets, whether as a going concern or as part of bankruptcy, liquidation, or similar proceeding.
- For any other purpose disclosed when you provide the information or with your consent.

We may also disclose your Personal Information:

- To government, law enforcement, national security, regulatory, or public authorities where required or appropriate under law, contract, procurement, security, or legal process, including to comply with any court order or to respond to any government or regulatory request, and to report activity that may be unlawful or threaten security or public safety.
- If we believe disclosure is necessary or appropriate to protect the rights, property, or safety of Company, our customers, or others.
- To Third-Party AI Providers, certain features of 10x's Services use artificial-intelligence models provided by third parties. The ORRIX Chat Assistant uses models provided by OpenAI, L.L.C. ORRIX DataSense uses models hosted by Amazon Web Services, Inc. through Amazon Bedrock in AWS GovCloud (US). When you use these features, your prompts, inputs, and files, and the resulting outputs, are transmitted to the applicable provider for processing. Our account settings with OpenAI do not permit it to use your content to train or improve its models. OpenAI may retain inputs and outputs for up to 30 days for abuse monitoring.

10. Choices About How We Use and Disclose Your Information.

You can set your browser to refuse cookies or alert you when they are sent. We do not use the Services to serve interest-based advertising. We do not respond to Do Not Track signals, but where legally required we recognize opt-out preference signals such as Global Privacy Control. Where we ask for your consent to a specific use, such as marketing communications, you may withdraw it at any time by contacting us, and we will record that choice.

11. Your State Privacy Rights.

State consumer privacy laws may provide their residents with additional rights regarding our use of their Personal Information.

Company is the controller (or business) for Personal Information about users of the Services that we collect for our own purposes, including account, authentication, usage, log, and acceptance-record information, and you may submit requests regarding that information to us. Where we process Personal Information on behalf of Your Organization or a government customer, we act as its service provider or processor, and you should submit requests regarding that information directly to that entity. If you submit such a request to us, we will refer it to that entity and will not respond to it on that entity's behalf without its authorization.

Depending on your state of residence (including California, Colorado, Connecticut, Delaware, Florida, Indiana, Iowa, Kentucky, Maryland, Minnesota, Montana, Nebraska, New Hampshire, New Jersey, Oregon, Rhode Island, Tennessee, Texas, Utah, and Virginia), you may have rights to confirm whether we process your Personal Information; to access, correct, delete, or obtain a portable copy of it; to opt out of targeted advertising, sales, and profiling in furtherance of decisions that produce legal or similarly significant effects; and to limit, or require consent for, processing of sensitive personal information.

To exercise these rights, contact us at privacy@10xnationalsecurity.com. We may need to verify your identity and authority, and you may use an authorized agent where permitted by law. Some information may be exempt from a request where permitted or required by law. You may appeal our decision, and we will not discriminate against you for exercising your rights.

12. Categories of Personal Information.

The following describes the categories of Personal Information we have collected in the preceding twelve (12) months, the sources, and the categories of recipients to whom we disclose it for a business purpose. We do not sell or share Personal Information for cross-context behavioral advertising.

- Identifiers (e.g., name, email address, username, internal user ID, IP address). Collected: Yes. Source: you; automatically. Disclosed to: affiliates; service providers; Your Organization; government customers and, for order administration, vendors as described above; government authorities as required by law.
- Customer records information (Cal. Civ. Code § 1798.80(e)) (e.g., name, telephone number, employer). Collected: Yes. Source: you. Disclosed to: affiliates; service providers; Your Organization.
- Professional, employment-related, and education information (e.g., organization, title, role, access authorization, and resume, work history, and education information if you apply for a role). Collected: Yes. Source: you; Your Organization; references and recruiting providers. Disclosed to: service providers; Your Organization; professional advisors.
- Internet or other electronic network activity (e.g., log data, browsing and usage

information, interactions with the Services, and prompts, inputs, and outputs of features of the Services). Collected: Yes. Source: you; automatically. Disclosed to: service providers; Your Organization; government customers as described above; government authorities as required by law.

- Geolocation data (general location derived from IP address). Collected: Yes. Source: automatically. Disclosed to: service providers.
- Sensitive personal information (account log-in credentials and, where appropriate for recruiting, security, or compliance purposes, government identification, citizenship or immigration status, security clearance, or accommodation information). Collected: Yes, only as needed for those purposes. Source: you. Disclosed to: service providers; government authorities as required by law. We do not use sensitive personal information to infer characteristics about you.
- Audio/visual information (security camera footage and recorded calls or meetings, where used). Collected: Yes. Source: automatically; you. Disclosed to: service providers; government authorities as required by law.
- Inferences drawn from the above (e.g., security risk indicators and usage patterns). Collected: Yes. Source: automatically. Disclosed to: service providers; Your Organization; government authorities as required by law.
- Biometric information. Collected: No.

13. Data Retention.

We retain Personal Information for as long as reasonably necessary for the purposes described in this policy, including to provide the Services, comply with legal and contractual obligations, support security and audit requirements, resolve disputes, and enforce agreements. When it is no longer needed, we delete, de-identify, aggregate, or securely archive it as permitted or required by law.

Examples of typical retention periods include: security and audit logs and records of acceptance of terms and acknowledgment of policies are retained for at least the period required by applicable government security, accreditation, and contract requirements, and generally at least three years; website logs are generally retained for up to two years; recruiting records are generally retained for up to three years after the recruiting process ends; visitor records are generally retained for up to two years; security camera footage, where used, is generally retained for up to ninety days; and business contact and contract records are retained for the life of the relationship and a reasonable period afterward. Any of these periods may be extended where information is needed for security investigations, incident response, legal holds, or compliance requirements.

14. Data Security.

We implement administrative, technical, and physical safeguards designed to protect Personal Information from loss, misuse, and unauthorized access, use, alteration, disclosure, or destruction. These safeguards may include access controls, logging, encryption, security monitoring, personnel training, vendor diligence, and incident response procedures. However, no electronic transmission or storage is completely secure, and we cannot guarantee absolute security. Please keep your account credentials confidential and notify us promptly of any actual or suspected unauthorized use of your account.

15. Job Applicants.

If you apply for a role with us, we use your application materials to evaluate your candidacy, communicate with you, verify qualifications, perform background or reference

checks where appropriate, and comply with employment-related obligations. We may use automated tools, including AI-assisted systems and service providers, to help organize, summarize, or process candidate information. We do not make solely automated employment decisions without human involvement.

16. Children's Privacy.

The Services are not directed to, and we do not knowingly collect Personal Information from, individuals under 18 years of age. If you believe that a minor has provided us with Personal Information, please contact us at privacy@10xnationalsecurity.com, and we will take steps to delete it.

17. Location of Processing and International Users.

Company is based in the United States, and the Services are intended primarily for users located in the United States. If you access the Services or interact with us from outside the United States, your information may be processed in the United States and other countries where we or our service providers operate, where data protection laws may differ from those in your jurisdiction.

If you are located in the European Economic Area, the United Kingdom, Switzerland, Australia, or another jurisdiction with similar laws, you may have rights to access, correct, delete, restrict, or object to the processing of your Personal Information, to data portability, to object to direct marketing, to withdraw consent where processing is based on consent, and to lodge a complaint with your local supervisory authority. We process Personal Information as necessary to perform our agreements, for our legitimate interests (such as operating and securing the Services, business communications, recruiting, partner and supplier management, and protecting our personnel, facilities, systems, and information), to comply with legal obligations, to protect vital interests, safety, security, national security, or the public interest where applicable, or with your consent. Withdrawal of consent does not affect prior processing or processing based on another lawful basis. Company is the controller of Personal Information about users of the Services that we collect for our own purposes. Where we process Personal Information on behalf of a government customer or Your Organization, that entity is the controller, and you should direct requests regarding that information to it.

When we transfer Personal Information from the European Economic Area, the United Kingdom, or Switzerland to countries that have not been found to provide an adequate level of protection, we rely on appropriate safeguards, such as the European Commission's Standard Contractual Clauses and their UK and Swiss equivalents, or another lawful transfer mechanism.

18. Third-Party Links and Services.

The Services may link to third-party websites, platforms, job boards, social media pages, or other services. We are not responsible for the privacy practices, security, or content of third-party services, and you should review their privacy notices before providing information to them.

19. Changes to Our Privacy Policy.

We may update this privacy policy from time to time. We will post any changes on this page and update the date at the top of this policy. If we make material changes to how we treat our users' Personal Information, we will notify you through the Services or by email before the changes take effect and, where required by law or our agreements, ask you to acknowledge the updated policy or obtain your consent. We encourage you to keep your

email address current with us and to review this privacy policy periodically.

20. Contact Information.

To ask questions or comment about this privacy policy and our privacy practices, or to make a data rights or deletion request, contact us at privacy@10xnationalsecurity.com.

System Use Notification and Logging Acknowledgment

Version 0.2

Last Modified: 13 Oct 2026

Applies to: ORRIX Platform / ICDC Program

You are accessing a 10x National Security Inc. ("10xNatSec") information system (the "System") that may support United States Government customers. Only authorized users may access this System, and only for authorized purposes.

This is a notice, not a contract. By clicking "I Acknowledge," you confirm that you have been notified of the following:

1. **Monitored System.** This System and all activity on it are monitored, recorded, and audited for security, administration, compliance, accreditation, and audit purposes.

2. **What is logged.** Your activity on this System is logged and associated with your account.

This may include:

- your user identity and account details;
- logins, logouts, and failed login attempts;
- your acceptance of terms and acknowledgment of notices;
- the features, data, and records you access;
- administrative and permission changes;
- prompts, inputs, files, and outputs of any chat agent or AI-enabled feature;
- timestamps, IP addresses, and device and session information.

3. **No expectation of privacy.** You have no reasonable expectation of privacy in any communication or data that you transmit through, process on, or store on this System.

4. **Review and disclosure.** 10xNatSec may review, retain, and preserve logs and System activity. It may disclose them to the following, consistent with applicable law and agreements:

- your sponsoring organization or Government customer;
- appropriate Government security or program officials;
- the provider of data you access, where needed to verify license compliance or address suspected misuse; and
- law enforcement or other competent authorities.

5. **Retention.** Logs are retained as required by applicable Government security, accreditation, and contract requirements, and generally at least three years. They may be kept longer when needed for investigations, enforcement, audits, legal holds, or legal defense, including after your access ends.

6. **Misuse.** Please be aware that unauthorized use of this System, or any attempt to circumvent its security controls or guardrails, is inconsistent with the terms that govern your access. Activity of this kind may lead to suspension or termination of access, notification of your organization and Government points of contact, and, where appropriate, referral to law enforcement or other competent authorities.
7. **Consent to monitoring.** Your use of this System, authorized or unauthorized, constitutes consent to monitoring, logging, review, and disclosure as described in this notice.
8. **Related terms.** This notice supplements the 10xNatSec Privacy Policy and the terms that govern your access to this System (for example, the ICDC Platform Agreement for the ICDC Platform). Your rights and obligations are set out in those governing terms, not in this notice or the Privacy Policy. Acknowledging this notice does not bind your organization or the United States Government. The sponsoring Government organization may require additional or different system use notice language.

If you do not wish to be monitored as described in this notice, do not access or use this System.