

Securin, Inc. PRIVACY POLICY

Effective Date: May 1, 2026

Securin, Inc. ("Securin," "Company," "we," "us," or "our") takes your privacy seriously. This Privacy Policy describes how we collect, use, disclose, and protect Personal Information when you visit our websites at www.securin.io and app.securin.io ("Sites"), use our cybersecurity SaaS platform and related services ("Platform" or "Services"), or otherwise interact with us. This Policy applies to all individuals whose Personal Information is processed by Securin, including website visitors, customers, prospective customers, and contacts. By using our Sites or Services, you agree to the practices described in this Privacy Policy. If you have a separate data processing agreement or Master Services Agreement ("MSA") with Securin, the terms of that agreement govern with respect to your customer data. This Policy governs all other personal information processing.

1. Information We Collect

We collect Personal Information in several ways, depending on how you interact with us.

1.1. Information You Provide Directly

- Contact and account information (name, email address, phone number, job title, company name)
- Payment and billing information
- Information submitted via forms, surveys, event registrations, support requests, or communications with us
- Credentials and authentication data when you register for or use our Platform

1.2. Information Collected Automatically

When you visit our Sites or use our Services, we automatically collect:

- Log data and usage information (IP address, browser type, operating system, pages visited, referring URLs, timestamps)
- Device identifiers and settings
- Cookies, pixel tags, and similar tracking technologies (see Section 3)
- Performance and diagnostic data

1.3. Information from Third Parties

We may receive Personal Information about you from:

- Business partners, resellers, and referral sources
- Data enrichment providers and analytics services
- Publicly available sources
- Third-party authentication providers (e.g., single sign-on services)

1.4. Customer Data and Platform Data

Securin customers may submit data to our Platform in the course of using our Services ("Customer Data"). Customer Data is governed by the customer's MSA and applicable data processing agreements. Securin acts as a data processor with respect to Customer Data and processes it only as directed by the customer and in accordance with those agreements.

2. How We Use Your Information

We use Personal Information for the following purposes:

2.1. Providing and Improving Services

- Creating and managing accounts, authenticating users, and providing access to Services
- Processing transactions and fulfilling orders
- Providing technical support and responding to inquiries
- Developing, maintaining, and improving our Platform and Services
- Conducting research and analytics to better understand usage patterns

2.2. Communications

- Sending transactional and administrative communications (account notices, security alerts, policy updates)
- Marketing communications about our products and services (where you have consented or where otherwise permitted by law)
- Responding to your requests, questions, and feedback

2.3. Security and Compliance

- Detecting, investigating, and preventing fraud, abuse, and security incidents
- Verifying identity and enforcing our terms and policies
- Complying with legal obligations and responding to lawful requests from government authorities

2.4. Artificial Intelligence and Automated Processing

As part of our Platform, Securin may offer AI-powered features including generative AI tools, agentic capabilities, and automated analysis features ("AI Services"). When AI Services process Personal Information, we do so to provide the contracted Services. See Section 6 for a complete description of our AI Services and your rights related to automated processing.

2.5. Artificial Intelligence and Automated Processing

We may use Personal Information to create de-identified or aggregated data that cannot reasonably be used to identify you. We may use and share such data for any lawful business purpose, including product development, research, and benchmarking.

3. Cookies and Tracking Technologies

3.1. Types of Technologies We Use

Securin and our third-party partners use cookies, pixel tags (web beacons), local storage, and similar technologies (collectively, "Technologies") to collect information automatically when you interact with our Sites and Services.

3.2. Categories of Use

Strictly Necessary

Required for core Site and Service functionality, security, and fraud prevention. These cannot be disabled.

Performance and Analytics

Used to understand how visitors interact with our Sites and Services. We use tools including Zoho Analytics, HubSpot, Google Analytics, and similar services to analyze trends and improve user experience.

Google Analytics opt-out: <https://tools.google.com/dlpage/gaoptout>

Functional

Enable enhanced features such as remembering preferences, language settings, and login status.

Advertising and Targeting

Used to deliver relevant content and advertisements. We and our advertising partners may use these Technologies across websites and over time.

3.3. Your Cookie Choices

You may manage cookies through your browser settings or by using our cookie preference tool (where available). Please note:

- Disabling certain cookies may affect Site or Service functionality
- Cookie opt-outs are browser- and device-specific; you must opt out separately on each browser and device
- Mobile app ad tracking may be managed through your device settings

3.4. Do Not Track

Our Sites do not currently respond to "Do Not Track" (DNT) browser signals. California law requires us to disclose this practice. Third parties may collect personal information about your online activities over time and across sites when you use our Sites.

4. How We Share Your Information

Securin does not sell your Personal Information. We share Personal Information only as described below.

4.1. Service Providers

We engage trusted third-party vendors to support our operations, including cloud hosting, payment processing, customer relationship management, IT services, and analytics. These vendors access Personal Information only as necessary to perform services on our behalf and are contractually required to protect it.

4.2. Business Partners and Resellers

We may share your information with authorized resellers and channel partners to facilitate the marketing and delivery of our Services. Such partners are required to handle your data in accordance with applicable privacy laws.

4.3. AI and Technology Subprocessors

Our AI Services may involve third-party model providers or infrastructure vendors. When Customer Data is processed through AI Services, applicable subprocessor disclosures are made in the customer's MSA or data processing agreement. We do not permit AI subprocessors to use Customer Data to train their own models except where expressly authorized.

4.4. Legal Compliance and Protection

In the event of a merger, acquisition, reorganization, sale of assets, or similar transaction, Personal Information may be transferred to the successor entity, subject to the same privacy protections described in this Policy.

4.5. With Your Consent

We may share your information for any other purpose with your prior consent or at your direction.

5. How We Share Your Information

We retain Personal Information for as long as necessary to fulfill the purposes described in this Policy, maintain our business relationship with you, comply with legal obligations, resolve disputes, and enforce our agreements.

Retention periods vary based on the type of information and the purpose for which it was collected. When Personal Information is no longer needed, we delete, anonymize, or securely dispose of it in accordance with our data retention schedule. If you would like information about specific retention periods applicable to your data, please contact us at privacy@securin.io.

Customer Data is retained in accordance with the terms of the applicable MSA and data processing agreement.

6. Artificial Intelligence Features and Automated Decision-Making

6.1. Overview of AI Services

Securin's Platform may include AI-powered features, including generative AI capabilities, agentic tools ("AI Agents"), and automated analysis and response features (collectively, "AI Services"). These features are designed to support cybersecurity operations, including network troubleshooting, vulnerability analysis, threat detection, and related use cases.

6.2. How AI Services Work

The AI Services may process data you or your organization submit to the Platform ("Inputs") to generate automated responses, analyses, action plans, and conclusions ("Outputs"). Customer Data submitted as

Inputs remains the customer's confidential information. As between the parties, customers own the content of corresponding Outputs.

Customers may have the option to integrate third-party AI models into certain Platform features. In such cases, the terms of the customer's agreement with that third-party provider govern the use of that model.

6.3. Important Limitations and Customer Responsibilities

Due to the nature of machine learning and artificial intelligence:

- AI Services may generate Output that is similar to output generated for other customers or users
- AI Services may generate Output that is inaccurate, incorrect, incomplete, or otherwise unreliable (sometimes referred to as "hallucination" or "confabulation")
- Customers are responsible for independently verifying any Output before relying on it for any purpose
- Customers are responsible for determining the suitability of AI Services for their specific use case and network environment

Each AI Agent action that a customer authorizes or enables based on Output — including executing troubleshooting steps, performing diagnostics, and implementing configuration changes or feature toggles in the customer's network environment (each, an "AI Agent Action") — is made at the customer's direction and under the customer's control and decision-making authority. Customers are solely responsible for AI Agent Actions as if the customer had performed such actions itself.

The accuracy and quality of, and rights to, the Output and each associated AI Agent Action depend on the quality and context of the data and inputs, in addition to the customer's compliance with their agreement with Securin.

6.4. AI and Automated Decision-Making Rights (CCPA/CPRA)

Under the California Consumer Privacy Act (CCPA) as amended by the CPRA, and effective with the 2025 ADMT regulations, consumers have the right to:

- Receive notice when automated decision-making technology (ADMT) is used to make or substantially contribute to significant decisions about them
- Opt out of the use of ADMT for significant decisions in certain contexts, including employment eligibility, credit, housing, and similar decisions
- Request a human review of significant decisions made using ADMT, where applicable

Securin's AI Services are designed for cybersecurity and IT operations purposes, and are not currently used to make significant decisions about consumers in the categories described above (e.g., employment, credit, housing). If this changes, we will update this Policy and provide required notices.

To inquire about or exercise rights related to automated processing, contact privacy@securin.io.

6.5. Training Data

Securin does not use Customer Data to train our AI models without the customer's explicit consent. We take reasonable steps to ensure that AI subprocessors we engage adhere to equivalent restrictions. Aggregate, de-identified, or synthetic data may be used for model improvement purposes.

7. Security

Securin maintains a comprehensive information security program designed to protect Personal Information from unauthorized access, use, disclosure, alteration, and destruction. Our security practices include:

- Encryption of data in transit and at rest
- Access controls restricting data access to authorized personnel on a need-to-know basis
- Contractual confidentiality and security obligations for all employees and contractors
- Regular security assessments, vulnerability management, and penetration testing
- Incident response procedures

No security measure is 100% guaranteed. In the event of a security breach affecting your Personal Information, we will notify you as required by applicable law in the most expedient time possible and without unreasonable delay, consistent with legitimate law enforcement needs or measures to determine the scope of the breach and restore the integrity of the affected systems.

Securin holds cybersecurity certifications and follows industry frameworks. Details are available at www.securin.io or by contacting us directly.

8. Your Privacy Rights

Depending on your location and applicable law, you may have the following rights with respect to your Personal Information:

8.1. General Rights (All Users)

- Access: Request a copy of the Personal Information we hold about you
- Correction/Rectification: Request that we correct inaccurate or incomplete Personal Information
- Deletion/Erasure: Request that we delete your Personal Information, subject to legal exceptions
- Opt-Out of Marketing: Opt out of receiving marketing communications at any time
- Data Portability: In certain circumstances, receive your data in a structured, machine-readable format

8.2. California Residents (CCPA/CPRA)

If you are a California resident, you have additional rights under the CCPA as amended by the CPRA:

- Right to Know: Request disclosure of the categories and specific pieces of Personal Information collected about you, the sources of collection, the business purposes for collection, and the categories of third parties with whom we share it — including for periods beyond the last 12 months (for data collected on or after January 1, 2022)
- Right to Delete: Request deletion of your Personal Information, subject to exceptions
- Right to Correct: Request correction of inaccurate Personal Information
- Right to Opt-Out of Sale or Sharing: We do not sell Personal Information. If we share Personal Information for cross-context behavioral advertising, you have the right to opt out
- Right to Limit Use of Sensitive Personal Information: Request that we limit our use and disclosure of your Sensitive Personal Information to purposes necessary to provide our Services
- Right to Non-Discrimination: We will not discriminate against you for exercising your privacy rights
- Right Regarding Automated Decision-Making: See Section 6.4 above

To submit a California privacy request, email privacy@securin.io with your full name, email address, and a description of your request. We will verify your identity before processing your request and respond within 45 days (with one 45-day extension if needed).

California Civil Code Section 1798.83 also permits California residents to request information about disclosures of Personal Information to third parties for direct marketing purposes. Contact privacy@securin.io to make such a request.

8.3. Residents of Other U.S. States

Several U.S. states have enacted comprehensive privacy laws that may grant you additional rights. As of the effective date of this Policy, states with active privacy laws include (but are not limited to): Colorado, Connecticut, Delaware, Iowa, Montana, Nebraska, New Hampshire, New Jersey, Oregon, Texas, Utah, and Virginia. Where applicable, residents of these states may have rights similar to those described in Section 8.1 above, including rights to access, correct, delete, and port their data, and to opt out of certain processing activities. To exercise your rights, please contact privacy@securin.io and identify your state of residence.

8.4. EEA, UK, and Switzerland Residents

If you are located in the European Economic Area (EEA), United Kingdom, or Switzerland, we process your Personal Information in accordance with the General Data Protection Regulation (GDPR) and applicable national laws.

Legal Bases for Processing

We process your Personal Information on the following legal bases:

- Contract: Where processing is necessary to perform a contract with you or to take steps at your request before entering a contract
- Legitimate Interests: Where processing is necessary for our legitimate business interests (such as security, fraud prevention, and product improvement), provided those interests are not overridden by your rights
- Legal Obligation: Where processing is required by applicable law
- Consent: Where you have provided explicit consent, which you may withdraw at any time

Additional EEA/UK/Swiss Rights

- Right to object to processing based on legitimate interests or for direct marketing
- Right to restrict processing in certain circumstances
- Right to data portability
- Right to lodge a complaint with your local supervisory authority

A list of EEA supervisory authorities is available at https://edpb.europa.eu/about-edpb/about-edpb/members_en.

To contact our Data Protection Officer or exercise EEA/UK/Swiss rights, email privacy@securin.io.

9. International Data Transfers

Securin is headquartered in the United States. By using our Sites or Services, you acknowledge that your Personal Information may be transferred to, stored in, and processed in the United States and other countries where our service providers operate, which may have different data protection laws than your jurisdiction.

For transfers of Personal Information from the EEA, UK, or Switzerland to the United States, we rely on appropriate transfer mechanisms as required by applicable law, including Standard Contractual Clauses (SCCs) where required. If you have questions about the safeguards applicable to your data transfers, please contact privacy@securin.io.

Any disputes relating to this Privacy Policy or data collected under it will be governed by the laws of the State of New Mexico, United States.

10. Children's Privacy

Our Sites, Platform, and Services are not directed to individuals under the age of 18. We do not knowingly collect Personal Information from children under 18. If we learn that we have collected Personal Information from a child under 18 without parental consent, we will promptly delete that information.

If you believe a child under 18 has provided us with Personal Information, please contact privacy@securin.io.

California residents under 18 who have registered for our Services may request removal of content they have publicly posted by contacting privacy@securin.io with a detailed description. Note that removal may not be complete in all circumstances as required or allowed by law.

11. Third-Party Links and Integrations

Our Sites and Platform may contain links to third-party websites, services, or integrations. This Privacy Policy does not apply to third-party sites or services. We encourage you to review the privacy policies of any third-party services you access. Securin is not responsible for the privacy practices of third parties.

12. Changes to This Privacy Policy

We may update this Privacy Policy from time to time. If we make material changes, we will notify you by posting the updated Policy on our Sites with a revised effective date, and where required by law, by providing additional notice (such as email notification or in-app notice) prior to the changes taking effect.

Your continued use of our Sites or Services after the effective date of any changes constitutes your acceptance of the updated Policy. We encourage you to review this Policy periodically.

13. How to Contact Us

If you have questions, requests, or concerns regarding this Privacy Policy or our privacy practices, please contact us:

Email : privacy@securin.io

Mail :

Securin, Inc.

Attn: Privacy Officer

8801 Horizon Blvd NE, Suite #200,

Albuquerque, NM 87113

Definitions

The following terms have the meanings set forth below when used in this Privacy Policy:

"AI Services" means generative AI features, AI Agents, automated analysis tools, and related capabilities offered as part of the Platform.

"ADMT" means Automated Decision-Making Technology, as defined under the CCPA/CPRA, which refers to technology that replaces or substantially replaces human decision-making.

"Customer Data" means data that a Securin customer submits to the Platform in the course of using the Services.

"Personal Information" means any information relating to an identified or identifiable natural person, as defined under applicable law.

"Platform" means Securin's cloud-based SaaS cybersecurity platform and all associated features, tools, and services.

"Process" or "Processing" means any operation performed on Personal Information, whether or not by automated means, including collection, storage, use, disclosure, and deletion.

"Sensitive Personal Information" means a subset of Personal Information deserving heightened protection under applicable law, including (depending on jurisdiction) racial or ethnic origin, health information, financial information, biometric data, geolocation data, precise location, sexual orientation, immigration status, and similar categories.

"Services" means all online and offline offerings provided by Securin, including the Platform.

"Sites" means www.securin.io, app.securin.io, and any other websites, social media pages, or blogs operated by Securin.

"Third Party" means any person or entity other than you or Securin.