SECUREX AGENCIES (K) LTD DETAILED PRIVACY POLICY

Last Updated: November 14, 2025

This Privacy Policy describes Our policies and procedures on the collection, use, and disclosure of Your information when You use the Securex mobile application (the "App"), our website, and any associated services (collectively, the "Service"). It tells You about Your privacy rights and how the law protects You. We use Your Personal data to provide and improve this Service. By using this Service, You agree to the collection and use of information in accordance with this Privacy Policy.

1. INTERPRETATION AND DEFINITIONS

1.1. Definitions

For the purposes of this Privacy Policy:

- **You** means the individual accessing or using this Service, or the company, or other legal entity on behalf of which such individual is accessing or using this Service, as applicable.
- **Company** (referred to as either “the Company”, “We”, “Us” or “Our” in this Agreement) refers to **Securex Agencies (K) Ltd**, a company registered in Kenya with its principal place of business at **P.O Box 48399-00100 Nairobi**.
- **Affiliate** means an entity that controls, is controlled by or is under common control with a party, where “control” means ownership of 50% or more of the shares, equity interest or other securities entitled to vote for the election of directors or other managing authority.
- **Service** refers to the Securex mobile application, website, and all associated services for security, response, and monitoring.
- **Country** refers to: **KENYA**.
- **Service Provider** means any natural or legal person who processes the data on behalf of the Company. It refers to third-party companies or individuals employed by the Company to facilitate the Service, to provide the Service on behalf of the Company, to perform services related to the Service or to assist the Company in analyzing how the Service is used.
- **Personal Data** is any information that relates to an identified or identifiable individual.
- **Usage Data** refers to data collected automatically, either generated by the use of the Service or from the Service infrastructure itself (for example, App screen views, connection time).

2. COLLECTING AND USING YOUR PERSONAL DATA

2.1. Types of Data Collected

A. Personal Data (Directly Provided)

While registering or using Our Service, We may ask You to provide Us with personally identifiable information that can be used to contact or identify You. This information may include, but is not limited to:

- Email address
- First name and last name
- Phone number
- Billing and Payment information (stored securely via a third-party payment processor)
- Profile picture
- Account Credentials

B. Data Collected Through Use of the Service (Automatically Collected)

We collect information created during your use of the App and Service:

- **Location Data:** If you access the Service through a mobile device, we collect your precise or approximate geolocation (GPS coordinates) to enable the dispatch of response teams and to verify service delivery. This is collected while the App is running in the foreground or background.
- **Transaction Data:** Information created during your interactions, including the type of service requested, date and time of request, distance/duration of service, and amount charged.
- **Device Data:** When You access the Service, we collect information including, but not limited to:
    - The type of mobile device You use
    - Your mobile device unique ID (UDID) or other unique identifier
    - The IP address of Your device
    - Your mobile operating system and browser type
    - Diagnostic data (crash reports, performance logs)

2.2. Use and Legal Basis for Processing Your Personal Data

The Company uses Personal Data for the following purposes, based on the corresponding legal basis:

Purpose of Processing	Description	Legal Basis for Processing
To Provide and Maintain Service	To operate, monitor, and ensure the functionality, reliability, and security of the Service, including dispatching security personnel.	**Contractual Necessity:** Essential for delivering the security and response services you subscribed to.
To Manage Your Account	To manage Your information, verify identity, and facilitate access to the Service.	**Contractual Necessity:** Essential for providing the requested service interaction.

For Contract Performance	Fulfilling our obligations related to your service subscription or requested security response.	**Contractual Necessity:** Fulfilling our obligations related to your subscription.
To Contact You	To contact You regarding security alerts, service status, security updates, and essential service communications via email, SMS, or in-app notification.	**Contractual Necessity / Legitimate Interest:** Essential communication for service delivery and safety.
For Marketing/Promotions	To provide You with news, special offers, and general information about other goods or services which we offer, similar to those you have already enquired about.	**Consent / Legitimate Interest:** Subject to Your right to opt-out at any time.
To Manage Your Requests	To attend and manage Your requests to Us, including customer support and inquiries.	**Legitimate Interest:** Responding to user requests and improving customer experience.
To Improve and Develop	To analyze usage trends, conduct research, and improve existing and develop new security products and features.	**Legitimate Interest:** Improving the quality and safety of our Service.

2.3. Children's Privacy

The Service is intended for use by individuals who are 18 years of age or older. We do not knowingly solicit or collect Personal Data from children under the age of 18. If we become aware that we have collected Personal Data from a child under the age of 18 without parental consent, we will take immediate steps to delete that information from our servers.

3. RETENTION AND SECURITY OF YOUR PERSONAL DATA

3.1. Retention

The Company will retain Your Personal Data only for as long as is necessary for the purposes set out in this Privacy Policy.

- **Account Data:** We will retain Your Personal Data as long as you have an active account with us. If your account is closed, personal data will be deleted unless required to be retained for accounting, dispute resolution, or fraud prevention purposes (typically for a period of up to 7 years for financial records).
- **Incident History:** Data related to security incidents and service responses will be stored for 3 years, after which the data may be anonymized.
- We will retain and use Your Personal Data to the extent necessary to comply with our legal obligations (e.g., for financial records or tax purposes), resolve disputes, and enforce our legal agreements and policies.

3.2. Security Measures

We are committed to safeguarding your information. We employ **reasonable administrative, physical, and electronic measures** designed to protect your information from unauthorized access, use, or disclosure. These measures include, but are not limited to, **data encryption (in transit and at rest)**, access controls, and regular security assessments.

4. SHARING AND DISCLOSURE OF YOUR PERSONAL DATA

4.1. Categories of Third-Party Recipients

We may share your personal information in the following situations with third-party recipients, which may include, but are not limited to, the following categories:

- **With Service Providers:** Companies providing essential services on our behalf, such as **IT hosting and cloud service providers**, **payment processors**, **email service providers**, and **data analytics firms**. These providers are contractually bound to maintain confidentiality and use the Personal Data only for the purposes specified by the Company.
- **With Affiliates:** We may share Your information with Our Affiliates (parent company, subsidiaries, joint venture partners, or other companies under common control) for internal business administration purposes related to providing the Service.
- **With Business Partners:** To jointly offer You certain products, services, or promotions.
- **Business Transactions:** In the event of a merger, acquisition, or asset sale, Your Personal Data may be among the assets transferred. We will provide notice before Your Personal Data is transferred.

4.2. Cross-Border Data Transfer and Safeguards

Your information may be transferred to and maintained on computers located outside of Your jurisdiction where the data protection laws may differ.

- The Company will take all steps reasonably necessary to ensure that Your data is treated securely in accordance with this Privacy Policy.
- For transfers outside of Kenya, we ensure that adequate safeguards are in place, which may include the use of **Standard Contractual Clauses (SCCs)** approved by relevant authorities, or other legal mechanisms to protect the data.

4.3. Law Enforcement and Other Legal Requirements

The Company may disclose Your Personal Data if required to do so by law or in the good faith belief that such action is necessary to:

- Comply with a legal obligation or respond to valid requests by public authorities (e.g., a court or a government agency).
- Protect and defend the rights or property of the Company.

- Prevent and identify fraud or other unlawful activity in connection with this Service.
- Protect the personal safety of Users of this Service or the public.
- Protect against legal liability.

5. YOUR DATA PROTECTION RIGHTS

Depending on your location and applicable law (including the Kenya Data Protection Act, 2019), you may have the following rights regarding the Personal Data we hold about you:

- **The Right to Access:** The right to request copies of your Personal Data.
- **The Right to Rectification:** The right to request that we correct any information you believe is inaccurate or complete information you believe is incomplete.
- **The Right to Erasure (Right to be Forgotten):** The right to request that we erase your Personal Data, under certain conditions (e.g., withdrawal of consent or data no longer needed for the original purpose).
- **The Right to Restrict Processing:** The right to request that we restrict the processing of your Personal Data, under certain conditions.
- **The Right to Object to Processing:** The right to object to our processing of your Personal Data, under certain conditions, particularly when based on our legitimate interests or for direct marketing.
- **The Right to Data Portability:** The right to request that we transfer the data that we have collected to another organization, or directly to you, under certain conditions.
- **The Right to Withdraw Consent:** Where we rely on your consent as the legal basis for processing, you have the right to withdraw that consent at any time. Withdrawal of consent will not affect the lawfulness of processing before the withdrawal.

To exercise any of these rights, please contact us using the details in the "Contact Us" section below.

6. CHANGES TO THIS PRIVACY POLICY

We reserve the right to change, modify, add or remove portions of this Privacy Policy at any time.

- We will notify You of any material changes by posting the new Privacy Policy on this page.
- We will let You know via email and/or a prominent notice on Our Service, prior to the change becoming effective and update the **"Last Updated"** date at the top of this Privacy Policy.
- You are advised to review this Privacy Policy periodically for any changes. Changes to this Privacy Policy are effective when they are posted on this page.

7. CONTACT US

If you have any questions about this Privacy Policy, your data protection rights, or wish to make a complaint, You can contact us:

- **By email:** info@securexafrica.com (We have 30 calendar days to respond to you).
- **By Mail:** Securex Agencies (K) Ltd, P.O Box 48399-00100 Nairobi, KENYA.