

Thorax T5 Secure

Privacy Policy

Effective Date: 5 March 2026

Issued by: Etion Create PTY(LTD)

1. Introduction

Etion Create ("we", "us", or "our") operates Thorax T5 Secure, a secure messaging and Voice over IP (**VoIP**) application distributed exclusively to licensed clients ("**the Application**"). This Privacy Policy describes how we handle information in connection with your use of the Application.

By using the Application, you acknowledge that you have read and understood this Privacy Policy. If you are using the Application in the course of your employment or as part of a licensed client organisation, your organisation's separate data processing agreement with Etion Create may also apply.

2. Who This Policy Applies To

The Application is not available to the general public. Access is restricted to individuals who have been provisioned with an account by a licensed client organisation. This Privacy Policy applies to all such authorised end users of the Application, regardless of their location.

The Application is not directed at children. Access requires valid credentials issued by a licensed client organisation, and no self-registration is available within the Application.

3. The Self-Hosted Architecture

T5 Secure is designed as a client-hosted application. This means:

- Your organisation operates and controls its own server infrastructure on which the Application's backend services run.
- Etion Create does not operate, access, or control your organisation's server. Message content, call data, and communications are routed through your organisation's own infrastructure.
- Etion Create does not have access to the content of your messages or calls.

As a result, the data handling practices described in this policy relate to the Application itself (the iOS, Android, Huawei client) and any data that passes through or is processed by infrastructure operated by your organisation. Your organisation is separately responsible, as an independent data controller, for all data processed on its own servers.

4. Information We Collect

4.1 Information Collected or Transmitted by the Application

The Application collects or transmits the following categories of information:

- **Account credentials:** Your username and password are used to authenticate you against your organisation's self-hosted server. Passwords are never stored in plaintext on the device or transmitted to your organisation.
- **Device identifiers:** Push notification tokens (such as Apple Push Notification Service tokens, Google push tokens or Huawei push tokens) are used to deliver incoming call and message alerts to your device. These identifiers are processed solely for the purpose of notification delivery and are not used for tracking or advertising.
- **Encrypted message and call content:** All messages and voice/video calls are end-to-end encrypted by the Application before transmission. This encrypted content is transmitted to your organisation's self-hosted server. Etion Create cannot access, read, or listen to the content of any messages or calls at any time.
- **IP addresses and network metadata:** Your device IP address and connection metadata are processed transiently when establishing encrypted connections to your organisation's server. This data is retained by your organisations system for the purpose of system health monitoring. Etion Create does not have access to any of the IP address or network metadata.

4.2 Information We Do Not Collect

Etion Create does not collect, store, or have access to:

- The content of any messages or voice/video calls.
- Your device contacts or address book.
- Your location data.
- Advertising identifiers or behavioural usage data.
- Any data for advertising, marketing profiling, or sale to third parties.

4.3 Third-Party SDKs and Services

T5 Secure uses the following third-party SDK's and Services:

1. APNS - Apple Push Notification Service.
2. GMS - Google Mobile Service.
3. HMS - Huawei Mobile Service.
4. Firebase - Firebase Crashlytics.

4.4 Device permissions

T5 Secure will request the following permissions from the user:

1. Camera, allows the T5 Secure to take photos and enable video calling.
2. Microphone, allows the T5 Secure to record voice notes, enable video and audio calling.
3. Location, allows the T5 access to the device location in order to share a pin location (only when you choose to send this in a chat).
4. Photos and videos, allows the T5 Secure to access your device storage to send, receive and save media files.
5. Notifications, allows the T5 Secure to indicate to a user when there are incoming messages or calls.

6. Music and Audio, allows the T5 Secure to record audio through your microphone and access audio files (under your control) for sending and sharing.
7. Phone, allows the T5 Secure to access your phone's state to manage and enhance in bound T5 secure call functionality.

5. How We Use Information

We use the limited information described above for the following purposes only:

- Authentication: To verify your identity and provide access to the Application.
- Notification delivery: To route push notifications for incoming messages and calls to your device via Apple Push Notification Service (APNs), Google Mobile Services (GMS) and Huawei Mobile Services (HMS). In these cases, your name and identity are not shared with the provider, only a token identity and provided by the respective operating system.
- Security and integrity: To maintain the security of encrypted communications and protect the Application from unauthorised access.
- Technical diagnostics: To diagnose faults and maintain the stability and performance of the Application.

We do not use personal information for advertising, behavioural profiling, or any purpose other than those listed above. We do not sell personal data.

6. Data Sharing and Third Parties

We do not sell, rent, or share your personal information with third parties.

Controlled information may be shared in the following limited circumstances:

- Your organisation: The Application connects to your organisation's self-hosted server. Your organisation is an independent data controller for all data processed on its own infrastructure.
- Apple Push Notification Service (APNs): Push notification tokens are shared with Apple solely for the purpose of delivering notifications to your device. Apple's privacy policy is available at <https://www.apple.com/legal/privacy/>
- Google Mobile Service (GMS): Push notification tokens are shared with Google solely for the purpose of delivering notifications to your device. Google's privacy policy is available at <https://policies.google.com/privacy/>
- Huawei Mobile Service (HMS): Push notification tokens are shared with Huawei solely for the purpose of delivering notifications to your device. Huawei's privacy policy is available at <https://consumer.huawei.com/en/privacy/privacy-statement-huawei/>
- Firebase: Etion Create receives a crash report that contains no user or location information. The Firebase Crashlytics is governed by specific terms from Google/Firebase available at <https://firebase.google.com/terms/crashlytics>
- Legal obligations: Your organisation may disclose information where required by law, court order, or regulatory authority, or where necessary to protect the legal rights of your organisation or its clients.

7. Data Retention

Because T5 Secure uses a self-hosted architecture, the retention of message content, call logs, and communication data is governed by your organisation's own data retention policies, not by Etion Create.

Where Etion Create processes data incidental to the operation of the Application (such as push notification tokens or transient network metadata), such data is retained only for as long as is necessary for the purpose for which it was collected. It is then securely deleted. Token data is deleted immediately when a user is removed from the system.

8. Security

T5 Secure is designed with security as its primary architectural principle:

- All messages and voice/video calls are end-to-end encrypted. Only the communicating parties can access the content of communications.
- All data in transit is protected using industry-standard encrypted transport protocols.
- No message content is stored on Etion Create's infrastructure at any point.
- Access to the Application requires valid credentials provisioned by your licensed client organisation.
- Credentials are not stored in plaintext on the device or transmitted to Etion Create.

While we implement robust technical and organisational security measures, no system of electronic communication is entirely free from risk. We encourage users to use strong, unique credentials and to report any suspected security issues to thorax@etioncreate.co.za.

9. International Data Transfers

T5 Secure is used by clients and users globally. Because the Application uses a self-hosted architecture, the geographic location of communication data processing is determined by where your organisation has deployed its server infrastructure — not by Etion Create.

To the extent that your organisation processes any personal data in connection with operating the Application (for example, push notification tokens or transient network metadata), such processing may involve transfers of data across international borders depending on the location of your organisation's infrastructure and any third-party service providers. Where such transfers occur, Etion Create takes appropriate steps to ensure that personal data is protected in accordance with applicable law.

10. Your Rights

Depending on your jurisdiction, you may have rights in relation to your personal data. These commonly include the right to:

- Access the personal data we hold about you.
- Request correction of inaccurate or incomplete data.
- Request deletion of your personal data, subject to applicable legal obligations and retention requirements.
- Object to or restrict certain processing of your data.
- Receive your data in a portable format (where technically feasible and applicable).
- Withdraw consent where processing is based on consent.

To exercise any of these rights, please contact us at thorax@etioncreate.co.za. Where a request relates to data held on your organisation's own server, we will direct you to your

organisation as the relevant data controller. We aim to respond to all legitimate requests within 30 days.

11. Account Deletion

Accounts in Thorax T5 Secure are provisioned by your licensed client organisation. The Application does not provide self-service account creation and therefore does not provide a self-service account deletion feature within the app. To request account deletion or deactivation, contact your organisation's administrator directly.

You may also contact your organisation's administrator to request deletion of any personal data held by your organisation in connection with your account. Data stored on your organisation's self-hosted server is subject to your organisation's own deletion policies.

12. Changes to This Privacy Policy

We may update this Privacy Policy from time to time to reflect changes in our data practices, technology, legal requirements, or other factors. We will notify licensed client organisations of any material changes in advance. The updated policy will be made available at <https://www.etioncreate.co.za> with a revised effective date.

Continued use of the Application following notification of material changes constitutes acknowledgement of the updated policy.

13. Contact Us

For any questions, concerns, or requests relating to this Privacy Policy or our data practices, please contact:

Etion Create

Email: thorax@etioncreate.co.za

Website: <https://www.etioncreate.co.za>