

POLOSYS CLIENT PORTAL & MOBILE APP - PRIVACY POLICY

User Privacy, Mobile Data Protection & Telemetry Standards

Polosys Technologies | Client Portal & Mobile App Policies | October 2026

1. Scope & Application

This Privacy Policy governs the collection, processing, and safeguarding of user data within the Polosys Client Portal and Mobile Application ('Client App', 'Portal'), operated by Polosys Technologies for enterprise clients, store managers, and authenticated subscribers.

2. Personal & Device Information Processed

User Credentials: Username, email, telephone number, and secure password hashes used for multi-factor authentication.

Mobile Device Telemetry: Device model, operating system version, push notification tokens, and biometric authorization tokens stored on-device.

Business Operations: Order histories, payments, real-time sync transactions, and invoice receipts accessed via the Client Portal.

3. Mobile Permissions & Usage

The Client Mobile App may request hardware permissions such as Biometrics (Fingerprint/FaceID for instant authentication), Push Notifications (order updates, billing alerts), and Network Access. Permissions are requested dynamically and can be toggled by the user at any time.

4. Data Security & Storage Controls

All mobile communications enforce HTTPS with TLS 1.3 encryption and API certificate validation. Authentication tokens are stored securely in hardware-backed keystores on Android/iOS, ensuring zero access by third-party apps.

5. User Privacy Rights & Data Retention

Users may review, update, or request the deletion of their portal profile at any time through their account settings. Account data is retained only as long as the Client organization maintains an active subscription with Polosys.