

POLOSYS CLIENT PORTAL - SECURITY & AUTHENTICATION POLICY

Mobile Security Architecture, Cryptography & Session Protection

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

1. Mobile Architecture & Hardening

The Polosys Client Mobile Application is built with defense-in-depth principles, incorporating secure storage wrappers, root/jailbreak detection, and tamper-resistant API communication channels.

2. Tokenized Authentication & Session Security

JWT Authentication: Secure short-lived JSON Web Tokens (JWT) with automatic background refresh tokens.

Biometric Authorization: Seamless biometric integration using system-level biometric prompts without transmitting biometric data over the wire.

Automatic Timeout: Inactive sessions automatically lock to prevent unauthorized physical device access.

3. In-Transit Encryption & SSL Pinning

All traffic between the Client Mobile App and the Polosys CRM Cloud Gateway is encrypted using TLS 1.3 with strict modern cipher suites, eliminating man-in-the-middle (MITM) vulnerabilities.

4. Payment Data Protection

Card numbers and sensitive banking credentials are never stored on the mobile device or local databases. All transactions are securely routed through PCI-DSS certified payment gateways and tokenized endpoints.

5. Compliance & Vulnerability Management

The Client Portal undergoes continuous static code analysis and dependency auditing to adhere to OWASP Mobile Top 10 security standards.