SECURECOMS • TRUST CENTER • ONE-PAGER • NOTEBOOKLM P2 BRIEFING

Threat model plain language

What we protect against, what we don’t, and how you verify it. securecoms.ai/security • 2026-08-10

WHAT WE PROTECT AGAINST

" Breached relay or DB attacker gets ciphertext, no plaintext.
" Rogue admin or bad dependency same: opaque bytes, no keys.
" Membership churn MLS re-keys on join/leave; old keys useless.
" Tampered history hash-chained, signed ledger; rewrite breaks chain.

WHAT WE DON’T COVER

" Compromised endpoint safety-number pairing is your defense.
" Lost recovery key you hold it; we never can. No recovery if lost.
" Routing metadata membership + timing visible; content never is.

CRYPTO CHOICES, PLAINLY

Group E2E
MLS RFC 9420 TreeKEM, forward secrecy, post-compromise recovery

Key exchange
X25519 • Signatures ed25519

Backup
Zero-knowledge sealed client-side under HKDF(seed); server holds ciphertext

Pairing
8-char safety number (Crockford blake2b of ephemeral X25519 pubkey)

THE BLIND RELAY THE LEDGER

Relay stores ciphertext, routes it. No plaintext, no search, no decrypt. Agent Connector does keys locally.

Humans verify devices with safety-number check.

```
// what the server stores
{ ciphertext: "bA9fX2N...9kLm4pQ==",  kid: "mls-epoch-42" }
```

Hash-chained, signed audit ledger exportable. Single rewritten block breaks verification.

Retention: Free 30d • Business 90d • Enterprise configurable

Exportable " Signed & hash-chained

BACKUP & DEVICE TRUST

Zero-knowledge backup
Blob sealed client-side; server holds ciphertext + recovery envelope. Only Clerk identity owner can touch.

Device pairing
8-char code from ephemeral X25519 pubkey. Substituting server -> mismatched code; human aborts.

Source: docs/gtm/GTM-LAUNCH-PLAN-2026-08-10.md §4 + /security copy + NotebookLM Pack P2 • Not legal advice; see /terms + /privacy.
MotiveFlow LLC • securecoms.ai/security • Questions? securecoms.ai/contact • Share this sheet with your security reviewer.
Generated from the P2 briefing doc download at securecoms.ai/files/securecoms-threat-model-one-pager.pdf