UnitTrack -- Security One-Pager

UnitTrack — Security & Privacy at a Glance

A one-page summary for procurement and security reviewers. Every control here is implemented today unless explicitly marked roadmap. Full detail, mapped control-by-control to the standards below, is in our Security & PII document and Methods & Formulas document.

What UnitTrack is. A platform for utilities to analyze metered energy/water data and publish it safely — statistical disclosure control, mapped to accepted standards, with PII protected end to end.

What we protect, and how

Area	Control (implemented today)
Encryption at rest	Field-level AES-256-GCM for PII; uploaded source files stored as ciphertext. Encryption key held outside the database.
Access control	Role-based, least-privilege, separation of duties. Reading raw PII is a distinct capability held only by a gated PII Steward — not even an Org Owner by default.
Authentication	Two-factor required for every user (NIST SP 800-63B, AAL2). Access is application-mediated, never direct database access.
Disclosure control	Every published aggregate passes k-anonymity + (n,k)-dominance + complementary suppression, with a residual re-identification risk score. Safe-by-default at the utility 15/15 standard; loosening a control warns.
Verification	Every disclosure-control rule and analysis has been independently, adversarially verified — formulas re-derived against the code + tests, and each citation checked against the primary literature; findings remediated and locked with regression tests. Backed by 300+ automated tests and dependency scanning in CI. Formulas + citations published in Methods & Formulas.
Tenant isolation	All data is organization-scoped; cross-tenant access blocked at the query layer and adversarially reviewed.
Audit	Append-only log of authentication, PII access, exports, and config changes — actor, timestamp, client IP, user agent — scoped per organization.

Area	Control (implemented today)
Resilience	Automated backups plus independent encrypted off-site copies; restore procedure tested, including recovery of encrypted PII.
Transport & app	HTTPS/HSTS, Content Security Policy, per-IP rate limiting, per-account brute-force throttling, secure cookies, CSV formula-injection defenses.
Payments	Billing (when enabled) via Stripe hosted checkout; card data never touches our servers — PCI DSS SAQ-A.

Standards we map to

NIST SP 800-53 (SC-28, AC-3/5/6, AU-2/3, PT), SP 800-122 (PII), SP 800-188 / NISTIR 8053 (de-identification), SP 800-63B (AAL2); ESSnet/Eurostat SDC Handbook; regulatory alignment with CA CPUC D.14-05-016 (“15/15”) and IL 220 ILCS 33.

Candid about the roadmap

We don’t overstate. A few controls are designed and planned, not yet live, and are called out as such in the full document: tokenized identity separation (keyed-HMAC pseudonyms in a separate identity store, per SP 800-122 §4.2.3; today PII is protected by the field- and file-level encryption above), KMS/HSM custody of the master key with a FIPS 140-3 validated module (per-org envelope encryption — each organization’s data under its own key — is already live; what remains is hosting the key-encryption key in hardware), and third-party attestation (SOC 2 Type II / external penetration test — internal adversarial reviews are complete). Differential privacy is available as an exploratory method; suppression is the production default.

Learn more: the full Security & PII and Methods & Formulas documents are at /trust. Security contact: support@polishcloversolutions.com.