LumeTrax
Customer Security Pack

PROCUREMENT GRADE
CAIQ + SIG pre-completed

CUSTOMER SECURITY PACK

LumeTrax Security & Compliance

Architecture · Deployment · Identity · Data residency · Certifications · Incident response · CAIQ + SIG pre-completion · Data-neutrality policy

DOCUMENT	Customer Security Pack — v1
AUDIENCE	Customer security, procurement, and lender's IE teams
SCOPE	All LumeTrax-deployed assets and platform tenancies
VERSION CONTROL	Pinned to issuance date · superseded by re-issued packs
DISTRIBUTION	Confidential to named recipient — do not redistribute without LumeTrax authorisation
CONTACT	info@lumetrax.com · security@lumetrax.com (vuln. disclosure)

This pack is the source of truth for LumeTrax's security posture as of the issuance date. Where a certification is in progress, status is stated explicitly (**Current** / **In implementation** / **Planned** / **Future roadmap**) — we do not claim a certification we don't hold. Customer-specific questionnaires (CAIQ, SIG, custom) are pre-completed against this pack as a baseline; bespoke responses are produced by the LumeTrax Engineering team within five business days.

Issued 2026-05-08 · Document version: security-pack-v1 · Next review: 2026-08-08 (quarterly cadence)

Contents

§	Section	Page
1	Executive overview · how to use this pack	3
2	Platform architecture · OT/IT separation	4
3	Deployment shapes · cloud / private / on-prem / air-gapped	5
4	Identity, access, audit	6
5	Encryption + tenant isolation + data residency	7
6	Certification status · trust roadmap	8
7	Vulnerability management + patching cadence + incident response	9
8	Backup, recovery, business continuity (RPO/RTO)	10
9	Responsible disclosure	11
10	CAIQ pre-completion sample (CSA STAR Level 1 baseline)	12–14
11	Data-neutrality policy (the seven commitments)	15
12	Sub-processors · data-flow map	16
13	Customer security review process · contact	17
A	Appendix — methodology references and standards	18

1. Executive overview · how to use this pack

LumeTrax is a financial-grade energy operating platform for utility-scale and hybrid renewable assets. This pack documents the security posture of LumeTrax across architecture, deployment, identity, data, certifications, incident response, and business continuity. The intended readers are customer security and procurement teams, lender's IEs, and insurer technical reviewers.

How to use this pack:

• If you operate a CSA STAR / CAIQ-driven evaluation, jump to §10 — the most common 25 questions are pre-completed against the architecture and policy in §2–§9.

• If you operate a Shared Assessments / SIG-driven evaluation, the SIG-Lite mappings are referenced inline to the source sections in this pack.

• If you have a customer-specific questionnaire, the LumeTrax Engineering team produces a bespoke response within five business days. Send it to **info@lumetrax.com** with subject line *Security questionnaire*.

• For vulnerability disclosure, see §9. Reports go to **security@lumetrax.com**; we acknowledge within 2 business days, triage within 5.

Status legend used throughout this pack

Status	Meaning
CURRENT	In production today; evidence available on request
IN IMPLEMENTATION	Active build; expected GA inside the named window
PLANNED	Decision made, work scheduled, not yet started
SCHEDULED	On calendar (e.g. annual penetration test for a specific quarter)
FUTURE ROADMAP	Committed direction, not yet active
CONDITIONAL	Depends on prerequisite (e.g. NERC CIP applies only to bulk-electric-system assets)
AVAILABLE ON REQUEST	Engagement-specific deliverable; produced when scoped in the engagement

2. Platform architecture · OT/IT separation

LumeTrax is one unified multi-tenant platform with module-based feature activation. The architecture enforces a hard boundary between the deterministic OT layer (SCADA / PLC / RTU / on-site controller) and the shared platform services (analytics, workflow, optimization, assurance) above it.

Architectural principles

Principle	How it is enforced
Mission-critical control stays in the deterministic OT layer	Supervisory commands, interlocks, safety-critical sequencing are bound to the on-site SCADA / PLC / RTU
Tenant data is segregated by architecture	Logical isolation in multi-tenant cloud (per-tenant DB schemas + row-level security); physical isolation in pr
Network segmentation is real, audited, and enforced	OT/IT boundary is enforced at the network layer in addition to the architecture layer. Explicit allow-lists for c
Vendor-agnostic ingestion	Platform connects to inverters, BESS, switchgear, trackers, met stations, and DG controllers over standard
Tenant hierarchy is the same on every screen and report	Client Organization → Portfolio → Plant → Subsystem → Asset → Tag/Point/Event. Hierarchy is enforced

Architectural reference standards

Internal SDLC aligned to **IEC 62443-4-1** (industrial cybersecurity for OT software suppliers). Ingestion topology and control-authority logic informed by **IEC 61400-26-1** (availability) and **IEC 61724-1** (PV system performance monitoring). Network segmentation and least-privilege principles aligned to **NIST SP 800-82 Rev. 3** (Guide to Operational Technology Security).

3. Deployment shapes

LumeTrax supports four deployment shapes. Same software, different topologies. Selection happens at engagement initiation through the Core questionnaire; subsequent shape changes are supported as commercial requirements evolve.

Shape	What it is	When to use	RPO target	RTO target
Cloud (multi-tenant)	Shared platform services on a managed cl[illegible]	[illegible]	[illegible]	[illegible]
Private cloud (single-te[illegible]	[illegible] cloud deployment per customer or[illegible]	[illegible]	[illegible]	[illegible]
On-prem	Customer-controlled deployment in custom[illegible]	[illegible] requiring [illegible]	[illegible]	[illegible] full)
Air-gapped	On-prem with no inbound or outbound pla[illegible]	[illegible]	[illegible]	[illegible] perimeter.

Cloud regions

Default cloud region(s): EU-West and MEA (specific provider region disclosed at engagement). Customer-requested regions are accommodated where the cloud provider supports them. Region pinning is contractual.

4. Identity, access, audit

Single sign-on

SAML 2.0 and OIDC supported. Customer's identity provider is the source of truth. Onboarding, offboarding, and group membership flow through the IdP. Most enterprise IdPs configure cleanly during standard onboarding (Okta, Azure AD / Entra, Google Workspace, Ping Identity, ADFS, Auth0).

Multi-factor authentication

Enforced by IdP policy where the IdP supports policy enforcement; enforced by LumeTrax otherwise. **No passwords-only access at any access tier.**

Role-based access control

Roles are scoped to plant, subsystem, function, and authority level. Granted access never exceeds the scope explicitly authorised by the customer. Third-party O&M; contractors are granted scoped access inside the customer's tenant — they see only the plants and functions the owner has authorised, with full audit trail per actor.

Role example	Default scope	Authority
Plant operator	Specific plant(s)	Read · supervisory control gated by authority matrix
Asset manager	Portfolio	Read · KPI export · report generation
Maintenance lead	Specific plant(s)	Read · ticket creation + assignment · spare-part transactions
Lender / IE viewer	Portfolio (read-only)	Read · evidence-pack export · audit log access
Third-party O&M contractor	Authorised plants only	Per contract — scoped read + write within work-order workflow
Security administrator (customer-side)	All resources in tenant	Audit log access · access-grant approval · revocation rights

Audit log

Every action — supervisory command, configuration change, data export, access grant, role assignment — is recorded with actor identity, timestamp, before/after state, and source IP. The audit log is exportable to customer SIEM via API or scheduled push (configurable per deployment). Retention is configurable per customer; default is 7 years.

5. Encryption · tenant isolation · data residency

Encryption in transit

TLS 1.3 minimum on all platform endpoints. Mutual TLS (mTLS) for edge-gateway-to-cloud sync where the deployment shape supports it. Certificate management is automated; customer certificate pinning is supported for high-security deployments.

Encryption at rest

AES-256 for historian storage, configuration database, document storage, and audit log. **Per-tenant encryption keys** with documented rotation cadence (quarterly default; customer-driven for private-cloud / on-prem deployments). Customer-managed keys (BYOK) supported on private-cloud and on-prem shapes.

Tenant isolation

Logical isolation in multi-tenant cloud — per-tenant DB schemas with row-level security policy enforcement. **Physical isolation** in private-cloud, on-prem, and air-gapped deployments. Cross-tenant data access is structurally blocked except where explicitly authorised by customer in writing.

Data residency

Cloud and private-cloud deployments are **region-pinned at engagement**. Default regions: EU-West, MEA. On-prem and air-gapped deployments don't leave the customer perimeter. Cross-border transfers (where applicable to cloud / private-cloud) governed by Standard Contractual Clauses (SCCs) for EU customers and equivalent legal mechanisms in other jurisdictions.

Sub-processors with operating-data access

Listed in §12. Customer notice provided ahead of additions, with the right to object built into the customer agreement. Any sub-processor change is communicated 30 days before activation.

6. Certification status · trust roadmap

Sequenced by what enterprise procurement actually asks for, not by badge collection. Status is updated as each phase progresses. **We do not claim a certification we don't hold.**

Item	Status	Window / Notes
Internal secure SDLC aligned to IEC 62443-4-1	IN IMPLEMENTATION	Phase 1 (0–9 months) · evidence available on request
ISO 27001 (ISMS)	PLANNED	Phase 1 (0–9 months) · preparation underway
ISO 9001 (QMS)	PLANNED	Phase 1 (0–9 months) · preparation underway
Third-party penetration testing	SCHEDULED	Phase 1 · annual cadence post-launch · most recent pen-
Customer security pack published	CURRENT	This document · quarterly review cadence
SOC 2 Type II	FUTURE ROADMAP	Phase 2 (6–15 months)
ISO 22301 (business continuity)	FUTURE ROADMAP	Phase 2 (6–15 months)
IEC 62443-4-1 certification	FUTURE ROADMAP	Phase 3 (9–18 months) · industrial cybersecurity for OT s
ISO 27017 / 27019 / 27701	FUTURE ROADMAP	Phase 3 · optional, per market demand
IEC 62443-4-2 / 3-3	CONDITIONAL	Phase 4 · only if shipping branded edge appliances
CE / UKCA / FCC / UL	CONDITIONAL	Phase 4 · for hardware shipping
NERC CIP regional readiness	AVAILABLE ON REQUEST	Engagement-specific for North American bulk-electric-sys
Project-specific DNV / TÜV / SGS assessments	AVAILABLE ON REQUEST	Per engagement

7. Vulnerability management · patching · incident response

Vulnerability management programme

Continuous dependency scanning (SCA), static application security testing (SAST), and infrastructure scanning are part of the SDLC. Severity-based remediation SLAs:

Severity	Remediation target (production)	Definition
Critical (CVSS 9.0+)	≤ 24 hours	Remote code execution · authentication bypass · data exfiltration with confirm
High (CVSS 7.0–8.9)	≤ 7 days	Privilege escalation · sensitive data exposure · DoS with confirmed exploit pa
Medium (CVSS 4.0–6.9)	≤ 30 days	Limited information disclosure · indirect attack vectors
Low (CVSS < 4.0)	Next quarterly release	Hardening recommendations · best-practice deviations

Patching cadence

Cloud and private-cloud: continuous deployment with automated regression testing. Critical patches deployed inside SLA. On-prem and air-gapped: signed patch bundles delivered to customer per cadence agreed at engagement (typical: monthly maintenance, with emergency out-of-band patches for critical CVEs).

Incident response

Phase	What happens	Timing
Detection	Automated alerts (SIEM, IDS, application monitoring) + manual reports	Continuous
Triage	Severity assessment, scope determination, customer impact analysis	Within 1 hour of detection
Notification (customer-affecting)	First customer notification with confirmed scope and customer impact	Within 24 hours of detection · contractual
Containment	Isolation, mitigation, evidence preservation	Per severity SLA
Eradication + recovery	Root-cause remediation, restoration to known-good state, validation	Per severity SLA
Post-incident review	Blameless postmortem, customer-facing incident report, methodology update	Within 14 days of resolution

8. Backup, recovery, business continuity

Targets are documented per deployment shape and stated contractually. Recovery point objective (RPO) and recovery time objective (RTO) below are default targets; tighter targets are available under Premium Support tier.

Deployment	Backup cadence	RPO target	RTO target	Off-site replication
Cloud (multi-tenant)	Continuous historian replication + daily full + weekly off-site	≤ 15 min historian · ≤ 1 h workflow	≤ 4 h full platform recovery	Yes — secondary region
Private cloud (single-tenant)	Continuous historian replication + daily full + weekly off-site	≤ 15 min	≤ 1 h	≤ 4 h	Yes — secondary region
On-prem	Customer-configured (default: hourly historian + daily full + weekly off-site customer storage)	Customer-set	Per runbook	Customer-configured
Air-gapped	On-prem only — no off-site replication possible by design	Per runbook (no off-site)	Per runbook	No (by design)

Disaster recovery testing

DR testing runs **quarterly for cloud and private-cloud** deployments (full failover simulation, with documented evidence). On-prem DR testing is customer-driven; LumeTrax provides runbooks and supports customer-led tests on request. Test results are summarised in the next-quarterly customer security review.

Business continuity

Edge gateway operates in local-fallback mode while cloud / private-cloud platform recovers — plant safety is unaffected because mission-critical control stays inside the deterministic OT layer. The plant continues to operate against locally-configured logic during platform recovery.

9. Responsible disclosure

If you've identified a security vulnerability in LumeTrax, we want to hear about it. Reports are received at **security@lumetrax.com**. We acknowledge within **2 business days**, triage within **5 business days**, and target a remediation timeline proportionate to severity (per §7). Coordinated disclosure is preferred.

Safe harbour

Researchers acting in good faith — not violating customer data, not interfering with production assets, not extracting more data than necessary to demonstrate the issue — will not be threatened with legal action. Public disclosure timing should align with remediation; we coordinate fix windows with the reporter.

Acknowledgement

Reporters are credited in published security advisories at the reporter's option. A formal bug-bounty programme is on the roadmap; pre-launch reporters can request acknowledgement in published advisories.

What to include in a disclosure

- A brief technical description of the vulnerability and its impact
- Reproducible steps (proof-of-concept code if applicable)
- Affected component(s) and version(s) where known
- Suggested mitigations or patches if you have them
- Your preferred disclosure timeline

10. CAIQ pre-completion sample (CSA STAR Level 1 baseline)

The Cloud Security Alliance's Consensus Assessments Initiative Questionnaire (CAIQ) is one of the most-requested security questionnaires in enterprise procurement. Below is a representative sample of pre-completed answers — covering the major CAIQ domains — that LumeTrax customers can use as a baseline. The full pre-completion (~250 questions) is delivered with the engagement; bespoke customer-specific questionnaire variations are produced within five business days.

Format: **ID** · **Domain** · **Question** · **Yes/No/NA/Partial** · **Notes / source-section reference**

ID	Domain	Question (abridged)	Answer	Source
AAC-01	Audit Assurance & Compliance	Are audit logs of system events maintained?	YES	§4 Audit log
AAC-02	Audit Assurance & Compliance	Are audit logs reviewed?	YES	§7 Incident response, continuous monitoring
AAC-03	Audit Assurance & Compliance	Are independent third-party audits performed?	PARTIAL	§6 Pen-test annual; SOC 2 Type II in roadmap
AIS-01	Application & Interface Security	Is application security testing part of the SDLC?	YES	§7 SCA + SAST + scanning
AIS-02	Application & Interface Security	Are APIs secured against common attack vectors (OWASP API Top 10)?	YES	§3 TLS 1.3 + auth · §4 RBAC
BCR-01	Business Continuity & Disaster Recovery	Are backup processes documented and tested?	YES	§8 BCP table + DR testing
BCR-02	Business Continuity & Disaster Recovery	Are RPO and RTO defined per deployment?	YES	§8 RPO ≤ 15 min · RTO ≤ 4 h (cloud)
CCC-01	Change Control & Configuration	Are infrastructure-as-code and change-management processes documented?	YES	Change requests via internal CI/CD with peer review
CCC-02	Change Control & Configuration	Are configuration baselines maintained?	YES	Per-deployment runbooks; drift detection in cloud
CEK-01	Cryptography, Encryption & Key Management	Is data encrypted in transit?	YES	§5 TLS 1.3 minimum
CEK-02	Cryptography, Encryption & Key Management	Is data encrypted at rest?	YES	§5 AES-256 with per-tenant keys
CEK-03	Cryptography, Encryption & Key Management	Are encryption keys managed by customer (BYOK)?	PARTIAL	§5 BYOK on private-cloud and on-prem; standard KMS
DCS-01	Datacenter Security	Is physical security at the datacenter validated?	YES	Cloud provider attestations (AWS / Azure / GCP) refere
DSI-01	Data Security & Information Lifecycle	Is customer data classified, segregated, and minimised?	YES	§5 tenant isolation · §11 data-neutrality policy
DSI-02	Data Security & Information Lifecycle	Is data lifecycle (creation → deletion) documented?	YES	Default retention 7 yr; deletion on customer request per
EKM-01	Encryption Key Management	Is key rotation enforced on a documented cadence?	YES	§5 quarterly default; customer-driven for BYOK
GRC-01	Governance, Risk & Compliance	Is a security governance framework documented?	YES	§2 IEC 62443-4-1 alignment; §6 trust roadmap
HRS-01	Human Resources Security	Are employees screened, trained, and bound by NDAs?	YES	Pre-employment screening, annual security training, ND
IAM-01	Identity & Access Management	Is SSO / SAML supported?	YES	§4 SAML 2.0 + OIDC
IAM-02	Identity & Access Management	Is MFA enforced?	YES	§4 IdP-enforced or LumeTrax-enforced; passwords-only
IPY-01	Interoperability & Portability	Is customer data exportable in standard formats?	YES	Historian + tenant data exportable throughout tenancy a
IVS-01	Infrastructure & Virtualisation Security	Is network segmentation enforced?	YES	§2 OT/IT boundary at network + architecture layers
LOG-01	Logging & Monitoring	Are security-relevant events logged?	YES	§4 audit log · §7 SIEM-exportable
RPM-01	Risk & Patch Management	Are vulnerabilities tracked and patched per documented SLA?	YES	§7 SLA table by severity
SEF-01	Security Incident Mgmt, E-Discovery & Cloud Forensics	Is an incident response plan documented and tested?	YES	§7 IR phases · postmortem within 14 days
STA-01	Supply Chain Mgmt, Transparency & Accountability	Are sub-processors disclosed and managed?	YES	§12 sub-processors list + 30-day notice rule
TVM-01	Threat & Vulnerability Management	Are dependency / SCA scans run continuously?	YES	§7 continuous scanning

UEM-01	Universal Endpoint Management	Are administrative endpoints (laptops, VPNs) hardened?	YES	MDM-enforced; least-privilege; full-disk encryption man

Sample shown: 27 of ~250 CAIQ questions across the 19 CSA control domains. Full pre-completion is delivered with the engagement. SIG-Lite mappings are inline (each CAIQ question maps to one or more SIG-Lite controls); SIG-Core variants are produced bespoke within 5 business days.

11. Data-neutrality policy — the seven commitments

The seven commitments below are **published policy on the public site AND verbatim contractual clauses in the customer DPA / MSA.** They are not aspirational; they are how LumeTrax operates. If procurement asks how independence holds in practice, this is the answer.

1. Customer data belongs to the customer.

Plant operating data, configurations, alarm records, work orders, and historian content are customer property. LumeTrax holds it in trust to deliver contracted services.

2. Tenant data is segregated by architecture.

Logical isolation in multi-tenant cloud (per-tenant DB schemas + row-level security); physical isolation in private-cloud, on-prem, and air-gapped deployments. Cross-tenant access structurally blocked.

3. LumeTrax does not share plant-level data with OEMs, EPCs, O&M; contractors, lenders, or affiliates unless explicitly authorised by the customer in writing.

Authorisation is per-purpose, time-bounded, and audit-logged. Tacit consent does not exist in this policy.

4. Cross-portfolio benchmarking is opt-in and anonymised.

Customers who opt in receive industry-anonymised aggregates; their plants do not become identifiable to any third party. Customers who opt out are excluded entirely.

5. Commercial teams do not access customer operating data except for contracted support, audit, or advisory scope.

Sales, marketing, and partnership teams do not read customer plant data. Engineering and support access is logged and scoped.

6. LumeTrax does not resell or license customer operating data to any third party.

Customer operating data is not a LumeTrax product. Future benchmark-dataset products (if developed) operate strictly under commitment 4 — opt-in and anonymised — with explicit customer authorisation.

7. Where LumeTrax software is installed, Audit & Assurance reports distinguish measured data, calculated outputs, assumptions, and reviewer judgment.

Sources are not blended in any deliverable. Disagreements between counterparties typically resolve at the assumption-or-judgement layer, where they belong.

12. Sub-processors · data-flow map

LumeTrax engages a small number of sub-processors with operating-data access. Customer notice is provided **30 days before any addition**; the right to object is contractual. The list below is illustrative for the cloud / private-cloud deployment shapes; on-prem and air-gapped deployments engage no LumeTrax sub-processors with operating-data access by design.

Sub-processor category	Purpose	Data scope	Region(s)
Cloud infrastructure (IaaS)	Compute, storage, networking	All operating data (encrypted at rest)	EU-West / MEA per engagement
Email delivery (transactional)	Demo / contact / security disclosure delivery	Submitter email + form-input metadata only	EU
Error monitoring (application observability)	Stack-trace and error context for engineering response	Application errors only — no customer operating data	EU
Web analytics (privacy-respecting, aggregated)	Marketing-site usage trends	Marketing-site visit metadata only — never platform data	EU
Identity provider (where customer does not bring own IdP)	SSO + MFA for LumeTrax staff	User identity, MFA tokens — no operating data	EU

Specific provider names per category are disclosed in the engagement letter and updated per change. The 30-day customer-notice obligation applies to any addition or substitution.

13. Customer security review process · contact

Customers running their own security review of LumeTrax can use this pack as the procurement-grade baseline. Standard process:

Step	What happens	Owner	Timing
1. Pack review	Customer reviews this pack and identifies sections requiring deeper documentation	Customer procurement	Self-paced
2. Questionnaire scoping	If a customer-specific questionnaire (CAIQ extended / SIG-Core / custom) is required, customer sends template to LumeTrax	Customer	—
3. Bespoke completion	LumeTrax Engineering completes the questionnaire against this pack as the source of truth	LumeTrax Engineering	5–10 business days
4. Clarifying questions	Customer reviews response; LumeTrax Engineering handles incremental clarifications	Both	1–2 business days per round
5. Architecture deep-dive (optional)	Live walkthrough of architecture, deployment, identity, or any specific control area on customer request	Both	Scheduled — typically 60–90 min
6. Sign-off	Customer issues sign-off; LumeTrax archives the response in the engagement record	Customer	—

Contact

Purpose	Path
General security questions	info@lumetrax.com (subject: Security question)
Customer security questionnaire / pre-completion request	info@lumetrax.com (subject: Security questionnaire)
Vulnerability disclosure	security@lumetrax.com
Incident reporting (customer-affecting)	security@lumetrax.com
Architecture / deployment deep-dive	info@lumetrax.com (subject: Architecture question)

Appendix A — Methodology references and standards

LumeTrax security posture aligns to the standards below. Where alignment is partial, this is stated explicitly in §6.

Standard	Application	LumeTrax position
IEC 62443-4-1	Industrial cybersecurity for OT software suppliers	Internal SDLC aligned · certification on Phase 3 roadmap
IEC 61400-26-1	Availability definitions for renewable energy plants	Adopted for capacity-weighted availability calculation
IEC 61724-1	PV system performance monitoring	Adopted for PR computation and weather normalisation
ISO/IEC 27001	Information Security Management System	Phase 1 · preparation underway
ISO 9001	Quality Management System	Phase 1 · preparation underway
SOC 2 Type II	Service organisation control attestation	Phase 2 · future roadmap
ISO 22301	Business continuity management	Phase 2 · future roadmap
NIST SP 800-82 Rev. 3	Guide to OT security	Network segmentation, least-privilege principles aligned
CSA STAR (CAIQ)	Cloud-services security questionnaire	Pre-completed at Level 1 baseline; full response per engagement
Shared Assessments SIG	Standardised security questionnaire	SIG-Lite pre-completed; SIG-Core bespoke per engagement
NERC CIP	Critical Infrastructure Protection (North America)	Regional readiness on request; engagement-specific scope

End of pack.