

KOL Luminary

Client security & privacy packet

Version 1.2 | Updated October 5, 2026 | Public procurement overview

KOL Luminary helps agency and pharma teams research public professional information, assess project fit, build shortlists and prepare exports in a shared workspace. This packet describes the application controls and documented procedures reviewed in the repository. It is not an independent audit, a penetration-test report or a contractual service-level agreement.

Our commitment to your workspace

We will not use your workspace content to train or fine-tune AI models. Private collaboration fields - internal notes, ratings, relationship history and client feedback - are excluded from research-provider request schemas. Research briefs, clarification messages and public professional criteria are provider inputs; users must keep confidential project material out of those inputs.

No-training does not mean no-retention. Research providers process submitted inputs under their own terms. Our AI evidence provider excludes API content from model training by default. Luminary's resumable integration stores responses, so provider retention applies. The specialist discovery provider's published no-training terms include an aggregated de-identified data exception. Account-specific terms and settings need procurement verification.

Controls in the application

- Verified identities, workspace permissions and database-enforced tenant isolation.
- Private file storage and authenticated customer export downloads.
- Server-only privileged credentials, validated inputs and protected browser boundaries.
- Explicit research-provider schemas and separation of private collaboration data.
- Automated application, database and browser checks; audit histories for key changes.
- Documented export cleanup, owner-verified deletion and incident response.

Independent assurance: in progress

We are working towards ISO/IEC 27001 certification and SOC 2 Type II attestation, targeting the coming months. Neither has been achieved for KOL Luminary. The target depends on readiness, the observation period and independent assessment; an audit engagement, scope and completion date are not evidenced in this packet. Provider certifications do not certify Luminary.

Appropriate use

The service is for public professional information and authorized business data. Do not submit patient records or protected health information (PHI). Luminary does not claim HIPAA approval, GxP validation, customer-managed encryption keys or end-to-end encryption.

Security reviews and reports: support@kolluminary.com. Initial messages should contain no credentials or sensitive records. Current overview: kolluminary.com/security.

01 / Access & secure engineering

Identity and tenant isolation

Our managed authentication service verifies identities on the server. Protected actions check current workspace membership and the permission required for the operation. Database row-level security enforces organization boundaries; tenant-aware foreign keys prevent cross-organization parent/child relationships. Privileged database functions have restricted execution and controlled search paths.

Owners manage workspace access. Ownership protections prevent removal of the last active owner. Platform-owner administration has a separate current-access grant and requires an authenticated second factor. This is not a claim that MFA or enterprise SSO is enforced for every customer user. Privileged service credentials can bypass row-level security, so trusted server and worker paths must independently validate scope.

Frontend and request boundaries

- Production Content Security Policy uses per-request nonces. Frame restrictions, MIME protection, referrer/permissions policies and HTTPS/HSTS reduce browser attack exposure.
- Inputs are validated on the server, not only in the browser. Provider content is treated as untrusted text rather than executable HTML.
- Local redirect validation protects authentication callbacks; sensitive file responses use private, no-store cache headers.
- Database-backed rate limits protect authentication, research, retries and export actions. Rate-limit identifiers are hashed.

Secrets, workers and external sources

Privileged database, research, payment and worker credentials are server-side. Production and staging use separate configuration. Background research and export dispatch uses record identifiers; trusted workers load the required records and validate workflow state. This reduces queued payload content but does not mean worker infrastructure never processes workspace data.

Source and photo retrieval constrain destinations, redirects, response size and time to reduce server-side request forgery and resource abuse. Photo handling validates allowed formats, size and image content and strips metadata by re-encoding. General-purpose uploads and image-backed export templates remain disabled pending their separate security review.

Release and change controls

Automated release checks run application tests, lint/type checks, a production build, dependency auditing, database reset/isolation tests and browser/accessibility checks. Reviewed release procedures include commit-backed deployment, rollback and post-deploy verification. The dependency gate blocks critical production findings; it is not a guarantee that all dependencies are vulnerability-free or that branch protection enforces every gate. Audit history preserves key profile edits, corrections, merges and exports.

02 / Data flow, privacy & retention

What goes where

1. A user signs in and works within an authorized organization. Application hosting runs web/server requests; managed identity, database and private-storage services hold account and workspace records.
2. Research uses the submitted brief, clarification messages and public criteria. A specialist research provider supports discovery within our multi-stage workflow; enabled AI evidence workflows process selected public evidence and criteria. Schema checks exclude private collaboration fields, but cannot make confidential text entered in a research brief safe to share.
3. Background infrastructure executes trusted research, export and maintenance jobs. Results and audit records return to tenant-scoped storage. Public sources may receive research queries, identifiers or normal web-request metadata.
4. An authorized user requests an export. Private storage rechecks the caller's access on the byte request, with an additional access check before response delivery. Copying an application download URL alone does not grant access.

Encryption and sharing

Our managed database and storage provider documents AES-256 encryption at rest and TLS in transit. The application uses HTTPS, private storage and organization-specific paths. These are managed infrastructure controls, not customer-held keys: authorized application and infrastructure services process readable data to deliver the service.

Client-view exports exclude internal collaboration fields. Workspace-view content is permission-controlled. Once a user downloads or shares a file, their organization controls that copy; revoking access cannot recall it. Public sample exports and this security packet contain no private customer workspace data.

Retention and deletion

- Generated export artifacts and associated snapshots have a 30-day cleanup lifecycle, with a daily maintenance task and audit record. Cleanup failures need operational follow-up.
- Workspace records, private notes, provenance and audit history support the active account and correction obligations. Subscription access expiry is not an automatic data purge.
- An organization deletion request requires identity and owner verification, a retention review, cancellation of active jobs, removal of private objects, database deletion and completion checks. Any legally required exceptions must be explained. Backup expiry and provider deletion must be assessed separately; no universal deletion deadline is promised.
- Stored AI evidence responses have a standard application-state retention period of at least 30 days, subject to provider policy and account configuration. Abuse-monitoring retention is separate. Zero data retention is not asserted for this integration.

Telemetry

Optional product analytics requires explicit consent and excludes session recording, form values and profile content. It records normalized routes. Error reporting scrubs sensitive request data when enabled. The latest operational record does not establish completed alert delivery or continuous security monitoring.

03 / Provider roles & data handling

This public overview describes service roles. A named provider inventory, applicable terms and data-processing details are available privately for client reviews. We provide disclosures and change notices required by applicable law or customer agreements. Current contracts, regions, subprocessors and report access need account-specific review. Optional services are not assumed active; provider assurance does not certify Luminary.

Identity, database and private storage

Processes user identities, membership, professional records, collaboration data, files and audit records. Database row-level security and private object policies govern workspace access. Provider encryption and assurance evidence is available for review.

Application hosting

Processes web traffic, server requests, application code and deployment configuration. Environment-scoped secrets and application security headers support the boundary. Provider assurance reports are subject to access and confidentiality conditions.

AI evidence assessment, when enabled

Receives selected public professional identity, criteria, claims and source evidence. This provider does not use API content for training by default; Luminary does not use customer content for fine-tuning. Stored responses support interrupted-job recovery. Project settings and retention terms need review before agreeing additional restrictions.

Specialist research provider / discovery and professional research

Receives briefs, clarification messages, public criteria and selected professional profiles. Published terms prohibit training on Customer Data but exclude aggregated de-identified data from that restriction; free/trial offerings and order forms may have different protections. Applicable paid-service terms, retention and data-processing agreements need review before any blanket provider guarantee.

Background processing

Processes the workspace data required for research, exports and maintenance; dispatch payloads use record identifiers. Secrets and worker access remain privileged. Provider controls and operational settings are part of the review evidence.

Subscriptions and payments

A hosted checkout collects payment details. Luminary stores billing references, customer/subscription state and relevant billing metadata, not full card numbers or card security codes. Incoming billing notifications are signature-checked.

Other integrations

Transactional email services process recipient addresses, invitation/workspace details and notification links. Error reporting processes scrubbed errors when configured; product analytics handles consented usage. Development services hold source code and release records. Research retrieves public institutions, journals, registries and bibliographic sources. Live settings and applicable agreements belong in the review.

04 / Incident response & continuity

Report privately

Contact support@kolluminary.com with a short description, affected feature, approximate time and contact details. Do not include secrets, sensitive records or an exploit in a public issue. A secure follow-up channel can be arranged.

Our documented response process

1. **Contain and preserve.** Disable affected routes, providers or jobs; revoke exposed credentials; preserve relevant request/run identifiers and evidence. Limit evidence access and avoid sensitive payloads in general tickets.
2. **Assess scope.** Identify affected organizations, records, objects, time windows and ongoing exposure. Keep verified facts separate from hypotheses. Escalate to the responsible service owner and relevant vendors.
3. **Notify and update.** Assess legal and contractual notification requirements from the outset, alongside technical response. Communicate privately with affected customer contacts, describing confirmed scope, protective actions and next steps. Do not defer a required notification until the technical investigation is complete.
4. **Eradicate and recover.** Apply reviewed code or forward database fixes and rotate credentials that crossed the boundary. Run tenant-isolation, storage, browser and task checks before restoring affected operations.
5. **Review and track.** Document root cause, detection gaps, remediation owners and due dates. Track corrective actions and communicate relevant findings to affected customers.

The process is documented; this packet does not establish a completed tabletop exercise, dedicated 24/7 security operations coverage or a fixed incident-notification SLA. Any specific notification deadline must be agreed in the applicable contract and assessed against law.

Continuity and rollback

Application rollback uses the last known-good production-context deployment; worker recovery uses an appropriate prior version. Database repair follows reviewed forward migrations or controlled transactions, preserving an audit trail. Public boundary checks and an authenticated read-only check are required before reopening writes after rollback.

Managed database backup capabilities depend on the vendor plan and settings. This review has not established current backup retention, point-in-time recovery enablement, separate storage-object backups or a successful end-to-end restore exercise. No recovery time objective (RTO) or recovery point objective (RPO) is promised without a verified, agreed service arrangement.

Shared responsibilities

Customer owners should keep membership current, remove departed users, protect credentials, use appropriate export visibility and limit downloaded copies. They should supply an incident contact and agree restricted-data requirements before uploading or entering such information.

05 / Assurance status & procurement

Implemented application safeguards

The reviewed code contains tenant isolation, server-side authorization, protected downloads, provider-input boundaries, secret separation, browser hardening, rate limits, restricted image handling and audit histories. Automated tests exercise these boundaries. These are meaningful safeguards, but code and test results alone do not prove an operating compliance program.

Documented operating procedures

The repository defines release gates, rollback, export cleanup, owner-verified deletion and incident response. The latest operations record identifies monitoring work still open. Completed exercises, signed agreements and current deployment settings need their own evidence.

Work to complete or verify

- **ISO 27001 and SOC 2 Type II:** establish audit scope, accountable owners, auditor engagement, policy/evidence readiness and the observation period. Target: coming months; no completed Luminary certificate or report.
- **Independent testing:** commission and track an external penetration test, remediation and retesting. An independent report is not evidenced by this packet.
- **Monitoring and incident readiness:** finish alert routing, prove receipt, establish escalation contacts and exercise the incident runbook. Do not infer 24/7 response coverage.
- **Recovery:** confirm database and object backup scope, retention and restoration permissions; complete a restore exercise before making RTO/RPO commitments.
- **Vendor and privacy evidence:** verify applicable agreements, DPAs, subprocessors, regions, retention/deletion and AI data-sharing settings. Published policies alone do not prove signed contractual protection. Customer privacy-policy/DPA terms require completion and legal review.
- **Access assurance:** tenant-wide customer MFA and enterprise SSO are not claimed. Leaked-password screening is a documented disabled setting and accepted risk requiring owner review. The platform-owner MFA gate is a separate implemented control.

Common procurement questions

Do you train on our data? No. Luminary will not use workspace content to train or fine-tune AI models. Provider-specific conditions and retention are described in this packet; a blanket zero-retention or no-derived-data-use claim is not made.

Can we receive your SOC 2 report? Luminary does not yet have one. We can discuss current controls and roadmap. Vendor reports are subject to vendor access and confidentiality conditions.

Can you sign our security questionnaire or DPA? Send your requirements for review. Responses must reflect verified controls and any agreed exceptions; this packet does not itself execute a contract or approve restricted data.

Where is our data hosted? Personal information may be transferred, processed or stored outside your country, including outside Canada, and may be subject to lawful access by authorities there. Deployment and provider regions must be confirmed for your review; this packet does not promise single-country or EU-only processing.

06 / Evidence & review references

How this packet was prepared

Reviewed against the application's security policy, security model, operations runbook, billing-retention design and current implementation on October 1, 2026. Newer authenticated export routes take precedence over older documentation describing five-minute signed download links. Live configuration, external attestations and contractual coverage are separate evidence categories.

The implementation review covered identity and owner MFA, provider request schemas, AI response storage, private export byte delivery, analytics consent, release checks and cleanup procedures. It did not constitute a new external penetration test or an audit of every production vendor setting.

Evidence available for client review

- Named provider inventory, service roles and data categories handled.
- Applicable provider privacy, security and data-use policies.
- Available assurance reports and their scope and access conditions.
- Account-specific agreements, processing locations and retention settings, with unverified items identified.
- Application controls, operational procedures and outstanding assurance work.

Provider policies may change; report access can depend on contract or plan. We do not reproduce restricted audit reports in this public packet. Required privacy and contractual disclosures are provided through the applicable customer process, including provider-change notices where required.

For a client-specific review

Send your questionnaire, intended data categories, required jurisdictions, vendor restrictions, retention requirements and security contact to support@kolluminary.com. Do not send confidential project files in the initial request. We can share the named provider inventory and applicable terms, agree the scope of a private review and identify available evidence, gaps and contractual requirements. A request or confidentiality agreement is not a prerequisite for disclosures you are legally entitled to receive.

Document maintenance

This packet and the public security page should be reviewed when architecture, providers, controls or assurance status change. The version and date identify this snapshot; they are not a promise that all operating evidence has been independently verified. The editable source and evidence register are maintained with the application repository.

KOL Luminary | kolluminary.com/security | Version 1.2