SECURITY

Aletheia Security Whitepaper

This whitepaper describes the security architecture of Aletheia by Lonia AI: how identity, data protection, isolation, audit logging, retention, and deletion are built into the product from the first release rather than added for institutional buyers. It is written for security reviewers, procurement teams, and accessibility offices who need concrete answers before deploying Aletheia across an institution.

Published: July 14, 2026. Product version: 1.0.0.

1. Overview

Aletheia is a user-side accessibility tool. It runs optical character recognition, generates image descriptions, restructures content, and labels forms, then exports the result as tagged PDF, plain text, or audio. Most of that work happens in the user's own browser, on the user's own device. The security posture follows from that architecture: the less data that leaves the device, the less there is to protect in transit or at rest, and the smaller the surface an attacker or an over-broad administrator can reach.

Where data does leave the device, it is limited to what an account needs to function: an identity from an OAuth provider, plan and billing status, and the usage counts needed to enforce plan limits. User documents are not stored on Lonia infrastructure. Authentication is OAuth single sign-on only, with no password anywhere in the system. Every database table is protected by row-level security so a user can reach only their own rows, and privileged institutional actions are recorded to an append-only audit log that cannot be edited or deleted.

Every control described in this document applies to every tier, including the permanent free tier. Security is treated as infrastructure, not as an upgrade. The

sections that follow describe each layer, the honest limits of Aletheia's current compliance posture, and how to report a security concern.

2. Identity and Access

Authentication is OAuth single sign-on only, through Google Workspace or Microsoft 365, on every tier including Free. There is no email-and-password login anywhere in the product: no password field, no password reset flow, and no password to store, leak, or phish. Sessions are managed by Supabase Auth. Because sign-in is delegated to the identity provider, Aletheia never holds a credential that can be reused elsewhere.

Institutional deployments separate administrator authority into distinct roles so that access follows least privilege:

- **Primary administrator:** full management of the institutional account, seats, and other administrators.
- **Secondary administrator:** day-to-day seat and license management without the ability to remove the primary administrator or change account-level settings.
- **Read-only administrator:** visibility into seat counts and aggregate usage for reporting, with no ability to change state.

FERPA-privileged access is a separate flag, not a role. It is not granted by default to any administrator, and it is the only path to individual student-scoped visibility. It is enforced at two gates, described in the Row-Level Security and Audit Logging sections below, and every use of it is written to the append-only institutional admin audit log.

3. Data Protection at Rest

Account data stored in Supabase PostgreSQL is encrypted at rest with AES-256, managed by the database platform. This covers the identity, plan, and usage records that make up an account, on every tier.

On the Professional tier, a user may connect their own AI provider key (bring your own key). That key is stored in the browser using a non-extractable key held in IndexedDB and encrypted at rest with AES-GCM-256. Non-extractable means the key material cannot be read back out of the browser's key store by page script; it can only be used to encrypt and decrypt locally. On Professional the provider key never leaves the device and is never transmitted to Lonia.

On the Enterprise tier the model is institution-managed and server-side. An institution administrator enrolls one organization API key with Lonia's Enterprise Worker over TLS. The Worker envelope-encrypts the key with a master key, the same wrapping pattern used by AWS KMS and HashiCorp Vault, and the wrapped key is stored encrypted at rest in Supabase (`aletheia_institutions.institution_byok_encrypted_key`). The Enterprise key material is never returned to any client: not to seat browsers, not to administrator browsers, and not to Lonia staff. User documents on both tiers are processed in the browser and saved to a local library on the device; they are not written to Lonia infrastructure at rest.

The Supabase primary data store is hosted in a single United States region. A future migration to an EU region is under consideration but not scheduled. The transfer analysis for institutional data at rest is set out in the Data Protection Impact Assessment and referenced in the Data Processing Agreement.

4. Data Protection in Transit

All network endpoints are served over TLS 1.3. Cloudflare terminates TLS at the edge in front of the static site (Cloudflare Pages) and the serverless functions (Cloudflare Workers), and connections onward to Supabase are likewise encrypted. HTTP Strict Transport Security is set with a two-year max-age and preload, so browsers refuse to connect over plaintext.

On the Professional tier, the bring-your-own-key path is deliberately architected so that the user's provider key and the content they choose to describe travel **browser-direct** to the AI provider (Anthropic, OpenAI, or OpenRouter). The request goes from the user's browser straight to the provider the user configured. It does not transit

Lonia infrastructure, Lonia does not proxy or intermediate it, and Lonia never sees the key or the content. This is shown as the Professional (browser-direct) path in the data flow diagram below.

On the Enterprise tier the path is **Lonia-mediated**. An Enhanced AI request runs from the seat's browser to Lonia's Enterprise Worker (a Cloudflare Worker) over TLS 1.3; the Worker decrypts the institution's enrolled key in memory for the lifetime of that request only, calls the AI provider on the institution's behalf, and returns the description. The institution's request content therefore transits Lonia infrastructure to the provider on this tier. The Worker does not persist the image beyond the synchronous request and response, and never returns the key material to any client. This is shown as the Enterprise (via Cloudflare Worker) path in the data flow diagram below.

The Personal and Family tier Enhanced AI path is different: it is Lonia-mediated, routing the single image a user chooses through a Lonia Cloudflare Worker to OpenRouter (United States hosted) over TLS 1.3, with no image content logged in the Worker and no image persisted server-side beyond the synchronous request and response. That cross-border transfer is covered by the scoped Standard Contractual Clauses and evaluated in the Transfer Impact Assessment.

5. Row-Level Security

Row-level security (RLS) is enabled on every table in the Supabase database, with no exceptions. A signed-in user can read and write only the rows that belong to them; there is no query path that returns another user's rows. Institutional data is scoped by an `institution_id` so that an administrator's reach is bounded to their own institution, and student-scoped tables carry that foreign key from creation.

Individual student-scoped visibility is gated twice. A server-side remote procedure enforces the FERPA-privileged condition in the database before any student-scoped row is returned, and a matching client-side flag governs whether the interface exposes the request at all. Neither gate alone is sufficient; both must be satisfied, and the server-side gate is authoritative. The default for every institutional administrator is aggregate-only visibility.

6. Audit Logging (WORM)

Significant user actions and every institutional administrator action are written to append-only audit logs: `aletheia_audit_log` for user-level actions and `aletheia_institutional_admin_audit_log` for administrator actions. These tables are write-once, read-many (WORM): their row-level security policies permit inserts and reads but define no UPDATE and no DELETE policy, so an existing audit record cannot be altered or removed, including by an administrator. Privileged operations emit their audit records through server-side remote procedures, so the act of performing the operation and the act of recording it are bound together rather than left to the caller. Any use of the FERPA-privileged flag is recorded here.

7. Data Retention

Retention for institutional deployments is configurable per institution, with a default of 365 days, stored as `retention_days` on the institution record. A Cloudflare Worker runs on a daily schedule at 03:00 UTC and deletes student-scoped data that has passed the institution's retention window. Retention is enforced by that scheduled job, not merely recorded as a preference: when the window elapses, the data is removed.

8. Sub-processors

The following third parties process data on Lonia's behalf to operate Aletheia. Each is limited to the purpose listed.

Sub-processors, their region, and their purpose.

Sub-processor	Region	Purpose
Supabase	United States	Managed PostgreSQL database, authentication, and account storage.

Sub-processor	Region	Purpose
Cloudflare	Global edge network, United States account	Static site hosting (Pages), serverless compute (Workers), and bot protection (Turnstile).
Google	United States	OAuth sign-in. Identity assertion only; no password is exchanged or stored.
Microsoft	United States	OAuth sign-in. Identity assertion only; no password is exchanged or stored.
Stripe	United States	Payment processing and subscription billing. Card data is handled by Stripe; Lonia never receives full card numbers.
OpenRouter (Enhanced AI on Personal and Family tiers)	United States	AI model routing for the opt-in Enhanced AI image description path on the Personal and Family consumer tiers only. Lonia operates its own OpenRouter account and mediates the request on the user's behalf; the image is discarded once the description is returned and is not logged, retained, or used for training. Covered by the scoped Standard Contractual Clauses at /legal/sccs.

Sub-processor	Region	Purpose
AI provider for Enterprise bring-your-own-key (institution-selected: Anthropic, OpenAI, or OpenRouter)	User-selectable per institutional enrollment	On the Enterprise tier only, the institution-selected AI provider receives Enhanced AI request payloads (a single image and a short instruction) relayed by Lonia's Enterprise Worker using the institution's own enrolled key, decrypted at request time. The image is not persisted server-side beyond the synchronous request and response. The transit runs through Lonia's Cloudflare and Supabase infrastructure, covered by the Standard Contractual Clauses referenced in the DPA at /legal/dpa; the provider is engaged as a Lonia sub-processor for this path and is disclosed under the update-on-change policy at /legal/subprocessors.

Bring-your-own-key AI providers are treated per tier. On the Professional tier the user's browser calls the provider the user configured directly, under the user's own account and terms, so no user key or content passes through Lonia to that provider, and the provider is **not** a Lonia sub-processor. On the Enterprise tier the institution's key is enrolled with Lonia's Enterprise Worker, which relays Enhanced AI request payloads to the institution-selected provider on the institution's behalf; for that path the provider receives content via Lonia infrastructure and **is** engaged as a Lonia sub-processor, listed in the table above. OpenRouter can therefore hold up to three roles depending on the path: a Lonia sub-processor on the Lonia-mediated Enhanced AI path for Personal and Family; a Lonia sub-processor on the Enterprise institution-managed bring-your-own-key path when an institution selects it; and a user-invoked provider that is not a Lonia sub-processor on the Professional browser-direct bring-your-own-key path. The authoritative, versioned list, with the update-on-change and advance-notification policy, is published at the Sub-processor List.

9. Data Deletion

When an account is terminated, the account-level data Lonia holds is deleted by cascade: the identity, plan, billing status, and usage records associated with the account are removed. Because user documents live in the local library on the user's device and were never stored on Lonia infrastructure, there is nothing on the document side for Lonia to delete. Append-only audit records are preserved as required for compliance and retained per the applicable retention policy; they record that actions occurred without retaining the underlying documents.

10. Compliance Posture

Aletheia's compliance posture is stated plainly, including what it does not hold.

- **Accessibility:** WCAG 2.2 Level AA is the conformance target, with Section 508 alignment. Aletheia publishes a VPAT accessibility report, a European Accessibility Act conformance statement, and an EN 301 549 conformance mapping. Accessibility status is self-evaluated; a formal third-party accessibility audit is planned but has not yet been conducted.
- **FERPA:** the data-segmentation architecture described above (institution scoping, per-institution retention, two-gate privileged access, and append-only audit logging) is built in and available for education deployments.
- **SOC 2:** Aletheia is **not** SOC 2 audited and claims no SOC 2 attestation.
- **ISO 27001:** Aletheia holds **no** ISO 27001 certification.
- **HIPAA:** Aletheia claims **no** HIPAA compliance certification. For healthcare Enterprise deployments the product includes architectural detection of personally identifiable information; detection is an architectural feature, not a certification, and no HIPAA compliance is claimed.

All security and compliance statements in this whitepaper are based on self-evaluation. No third-party security audit has been performed.

11. Incident Response

Suspected vulnerabilities and security concerns can be reported to security@lonia.ai. Aletheia aims to acknowledge security reports within 24 hours of receipt and to keep the reporter informed as the report is triaged and addressed. Where a security incident affects personal data processed for an institutional customer, notification follows the timeline in the applicable Data Processing Agreement, which reflects the 72-hour notification expectation of GDPR Article 33.

12. Data Flow Diagram

The diagram below shows the standard request path from the browser through Cloudflare to Supabase, and the two bring-your-own-key paths: the Professional path, in which the browser calls the AI provider directly and bypasses Lonia infrastructure, and the Enterprise path, in which the request runs from the browser through Lonia's Cloudflare Worker to the AI provider. A text description follows the diagram.

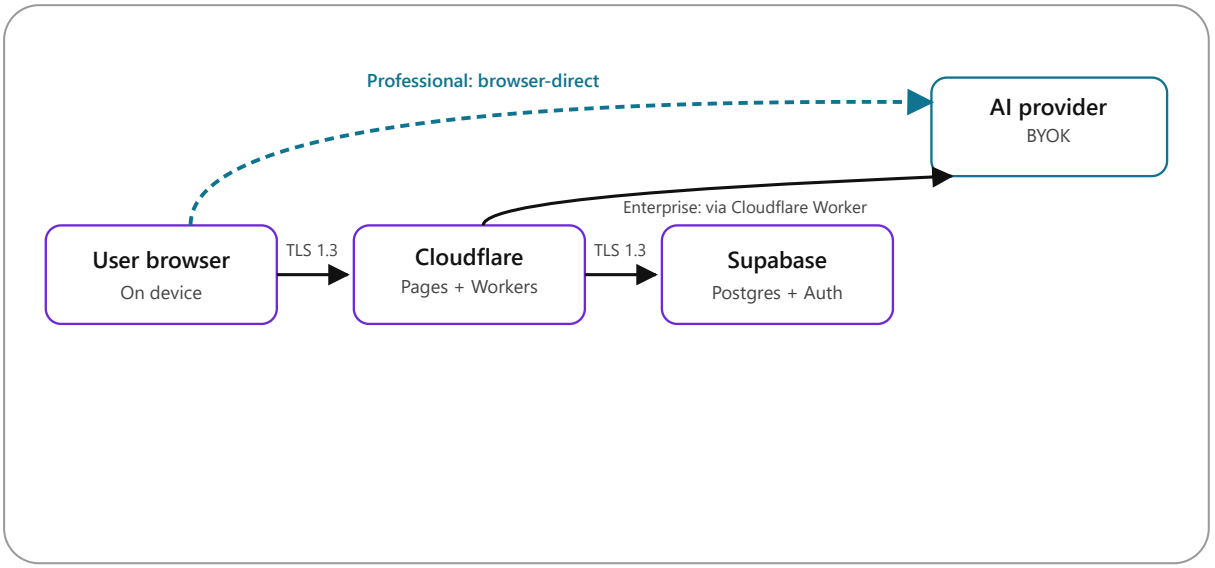

Figure 1. Standard requests flow browser to Cloudflare to Supabase over TLS 1.3. The Professional bring-your-own-key path runs browser-direct to the AI provider and never touches Lonia infrastructure. The Enterprise bring-your-own-key path runs from the browser through Lonia's Cloudflare Worker to the AI provider.

In words, the flow is:

The user's browser processes documents on the device and, for account and billing operations, connects over TLS 1.3 to Cloudflare.
Cloudflare Pages serves the static site and Cloudflare Workers run the serverless functions; Workers connect over TLS to Supabase.
Supabase holds the PostgreSQL database (with row-level security on every table) and manages authentication.
On the Professional bring-your-own-key tier, when the user chooses to use their own provider key, the browser calls the AI provider directly. That request bypasses Cloudflare and Supabase and never reaches Lonia infrastructure, so Lonia never sees the key or the content.
On the Enterprise bring-your-own-key tier, the institution's key is enrolled once with Lonia's Enterprise Worker and stored envelope-encrypted at rest. When a seat makes an Enhanced AI request, it runs from the browser to the Enterprise Worker, which decrypts the key in memory for that request only and calls the AI provider on the institution's behalf. The key material is never returned to any client.

13. Change History and Review Cadence

This whitepaper was published on July 14, 2026 for Aletheia version 1.0.0. Last review date: July 14, 2026. Next review: annually, or on material change, whichever comes first. Material changes include an architecture change, a sub-processor change, and a relevant regulatory change. The review is owned by legal@lonia.ai, in coordination with security@lonia.ai, and on each review this page and the tagged PDF are regenerated together from the same source.

Related documents

- Security whitepaper (tagged PDF)
- HECVAT 4.1.6 response (pre-completed higher-education vendor assessment)
- Data Processing Agreement (DPA) template
- Data Protection Impact Assessment (DPIA)
- Scoped Standard Contractual Clauses (SCCs)
- Transfer Impact Assessment (TIA)

- Privacy policy
- VPAT accessibility report
- European Accessibility Act (EAA) conformance statement
- EN 301 549 conformance mapping