PROCUREMENT

HECVAT 4.1.6 Response

This is Aletheia's pre-completed response to the Higher Education Community Vendor Assessment Toolkit (HECVAT). It answers all 332 questions in the current EDUCAUSE HECVAT 4.1.6 workbook honestly, so a procurement or security review can begin without waiting for a completed questionnaire. Read it in the browser, or download the tagged PDF or the XLSX for your vendor-tracking system.

Version: HECVAT 4.1.6. Completed: July 14, 2026. Solution: Aletheia by Lonia AI.

> **How to read this response.** The question text is taken verbatim from the official EDUCAUSE HECVAT 4.1.6 workbook, the current published version (4.1.6 supersedes 4.1.5), with punctuation normalized to plain text. Answers are Aletheia's own and are self-evaluated: Aletheia holds no SOC 2, ISO 27001, or HIPAA certification, and states this plainly where the workbook asks. Where Aletheia does not do exactly what a question asks but achieves the same objective another way, the answer is a compensating control rather than an unqualified "Yes." Where a control is planned but not yet in place, it is marked as roadmap. Honest answers are more useful to a reviewer than optimistic ones.

Response key

- **YES** Aletheia does this.
- **NO** Aletheia does not do this.
- **N/A** Not applicable to Aletheia's architecture, with the reason given.
- **COMPENSATING CONTROL** Aletheia achieves the same security objective a different way, described in the answer.
- **ROADMAP** Not currently in place; planned, with context in the answer.

Contents

1. Company Overview and Scoping (22 questions)

GNRL-01

Solution Provider Name

Response: Lonia AI

GNRL-02

Solution Name

Response: Aletheia

GNRL-03

Solution Description

Response: Aletheia is a user-side digital accessibility assistant. It converts inaccessible documents, images, and interfaces into accessible formats: structured text, described images, labeled forms, and readable reflowed content. Most processing runs in the user's own browser on their device.

Reference: Security Whitepaper

GNRL-04

Solution Provider Contact Name

Response: Lonia AI security contact

Provided to institutional buyers on request. Reached at security@lonia.ai.

GNRL-05

Solution Provider Contact Title

Response: Security contact

GNRL-06

Solution Provider Contact Email

Response: security@lonia.ai

GNRL-07

Solution Provider Contact Phone Number

Response: Available on request via security@lonia.ai

Aletheia support and procurement contact is handled by email; a direct line is provided to institutional buyers on request.

GNRL-08

Country of Company Headquarters

Response: United States

GNRL-09

Employee Work Locations (all)

Response: United States (remote workforce)

Lonia AI operates as a United States based remote team. Confirm exact staffing footprint with the vendor.

COMP-01 YES

Do you have a dedicated software and system development team(s) (e.g., customer support, implementation, product management, etc.)?*

Lonia AI maintains the engineering, product, and support functions for Aletheia.

COMP-02

Describe your organization's business background and ownership structure, including all parent and subsidiary relationships.

Response: Aletheia is developed and operated by Lonia AI, a United States based software company. Aletheia is its digital accessibility product. Ownership and corporate detail are provided to institutional buyers on request.

COMP-03 YES

Have you operated without unplanned disruptions to this solution in the past 12 months?

Aletheia has operated without unplanned service disruption. Hosting runs on Cloudflare (edge and compute) and Supabase (database), each with its own resilience posture. Confirm the exact operating window with the vendor.

Reference: Sub-processors

COMP-04 COMPENSATING CONTROL

Do you have a dedicated information security staff or office?

Aletheia does not maintain a separate information security office. Security ownership sits with Lonia engineering leadership, and security controls are built into the architecture from the first commit: OAuth-only identity, row-level security on every table, WORM audit logging, and encryption at rest and in transit.

Reference: Security Whitepaper

COMP-05

Use this area to share information about your environment that will assist those who are assessing your company's data security program.

Response: Aletheia minimizes what leaves the device. Only account identity, plan and billing status, and usage counts are processed by Lonia; user documents are processed in-browser and stored on-device. Identity is OAuth-only with no stored passwords, every database table enforces row-level security, and privileged institutional actions write to append-only (WORM) audit logs.

Reference: Security Whitepaper

REQU-01 YES

Are you offering a cloud-based product?

Aletheia is a browser-based web application hosted on Cloudflare (Pages and Workers) with a Supabase (US region) PostgreSQL database. User documents are processed in the user's browser and stored in a local on-device library; they are not stored on Lonia infrastructure.

Reference: Security Whitepaper

REQU-02 YES

Does your product or service have an interface?

Aletheia has a web application user interface, built to WCAG 2.2 AA.

Reference: VPAT

REQU-03 NO

Are you providing consulting services?

Aletheia is a software product, not a consulting engagement. The Consulting (CONS) section therefore does not apply.

REQU-04 YES

Does your solution have AI features, or are there plans to implement AI features in the next 12 months?

Aletheia uses AI for accessibility conversion: an on-device vision-language model on the base tier; on Professional, the customer's own commercial AI provider via browser-direct bring-your-own-key (BYOK); and on Enterprise, an institution-managed BYOK key held server-side by Lonia's Enterprise Worker and used to call the provider on the institution's behalf. See the AI section.

Reference: Security Whitepaper

REQU-05 NO

Does your solution process protected health information (PHI) or any data covered by the Health Insurance Portability and Accountability Act (HIPAA)?

Aletheia is not designed to process protected health information and is not a HIPAA-covered processing platform. It includes architectural PII detection to help users avoid inadvertently sharing sensitive content, but that is a feature, not a HIPAA certification. User documents are processed on-device. A Business Associate Agreement can be provided on request for a healthcare Enterprise deployment.

Reference: Privacy Policy

REQU-06 NO

Is the solution designed to process, store, or transmit credit card information?

Aletheia does not store, process, or transmit cardholder data. All payment processing is handled by Stripe; Lonia never receives full card or bank account numbers.

Reference: Sub-processors

REQU-07 NO

Does operating your solution require the institution to operate a physical or virtual appliance in their own environment or to provide inbound firewall exceptions to allow your employees to remotely administer systems in the institution's environment?

Aletheia requires no on-premises or virtual appliance and no inbound firewall exceptions. It is a browser-based web application.

REQU-08 YES

Does your solution have access to personal or institutional data?

Aletheia processes limited account identity (name and email from OAuth), plan and billing status, usage counts, and, for institutions, admin and audit records. User document content is processed on-device and is not stored on Lonia infrastructure.

Reference: Privacy Policy

2. Organization: Documentation, Third Parties, Change, Policies (43 questions)

DOCU-01 COMPENSATING CONTROL

Do you have a well-documented business continuity plan (BCP), with a clear owner, that is tested annually?*

Aletheia does not maintain a separately documented, annually tested business continuity plan of its own. Continuity rests on the resilience of its managed providers (Cloudflare global edge, Supabase managed database) and on a stateless static-site plus serverless architecture that can be redeployed from version control. Formalizing and testing a written BCP is on the roadmap.

Reference: Sub-processors

DOCU-02 COMPENSATING CONTROL

Do you have a well-documented disaster recovery plan (DRP), with a clear owner, that is tested annually?*

Recovery relies on managed-provider durability (Supabase point-in-time backups within the US region, Cloudflare redeploy) and infrastructure-as-code redeploy from version control. A formally documented, annually tested disaster recovery plan is on the roadmap.

Reference: Sub-processors

DOCU-03 NO

Have you undergone a SSAE 18/SOC 2 audit?

Aletheia has not undergone a SOC 2 / SSAE 18 audit and claims no SOC 2 attestation. Its infrastructure providers (Supabase, Cloudflare, and the AWS platform underlying Supabase) maintain their own SOC 2 reports. Aletheia's own posture is self-evaluated.

Reference: Security Whitepaper

DOCU-04 COMPENSATING CONTROL

Do you conform with a specific industry standard security framework (e.g., NIST Cybersecurity Framework, CIS Controls, ISO 27001, etc.)?

Aletheia holds no ISO 27001 or equivalent security certification. Its architecture is built to widely recognized control practices: least privilege, encryption at rest and in transit, row-level tenant isolation, append-only audit logging, and OAuth-only identity. Conformance is self-evaluated, not third-party certified.

Reference: Security Whitepaper

DOCU-05 YES

Can you provide overall system and/or application architecture diagrams, including a full description of the data flow for all components of the system?

The Security Whitepaper includes an architecture and data-flow description, including both bring-your-own-key paths: the Professional browser-direct path that bypasses Lonia, and the Enterprise institution-managed path that runs through Lonia's Enterprise Worker to the provider.

Reference: Security Whitepaper

DOCU-06 YES

Does your organization have a data privacy policy?

Aletheia publishes a privacy policy.

Reference: Privacy Policy

DOCU-07 COMPENSATING CONTROL

Do you have a documented, and currently implemented, employee onboarding and offboarding policy?

Access is OAuth-based and least-privilege, so joiner/leaver changes are enforced through the institution's identity provider and Lonia's access model rather than local credentials. A formally documented onboarding/offboarding policy is maturing; confirm status with the vendor.

THRD-01 YES

Do you perform security assessments of third-party companies with which you share data (e.g., hosting providers, cloud services, PaaS, IaaS, SaaS)?*

Sub-processors are limited to established providers (Supabase, Cloudflare, Google, Microsoft, Stripe), each selected and reviewed for their security posture. See the authoritative Sub-processor list.

Reference: Sub-processors

THRD-02 YES

Do you have contractual language in place with third parties governing access to institutional data?*

Data protection addendums and, where applicable, Standard Contractual Clauses govern each sub-processor's access to personal data.

Reference: Sub-processors

THRD-03 YES

Do the contracts in place with these third parties address liability in the event of a data breach?*

Sub-processor contracts (DPAs) address security and breach obligations. Liability terms with institutional customers are set in the Principal Agreement and DPA.

Reference: DPA

THRD-04 YES

Do you have an implemented third-party management strategy?*

Aletheia maintains an authoritative, versioned Sub-processor list with an update-on-change and advance-notification policy.

Reference: Sub-processors

THRD-05 COMPENSATING CONTROL

Do you have a process and implemented procedures for managing your hardware supply chain (e.g., telecommunications equipment, export licensing, computing devices)?

Aletheia operates no hardware supply chain of its own; it runs entirely on managed cloud providers (Cloudflare, Supabase on AWS), which manage their own hardware supply chains.

Reference: Sub-processors

CHNG-01 YES

Will the institution be notified of major changes to your environment that could impact the institution's security posture?*

Institutions are notified of material changes that could affect their security posture, including sub-processor changes under the Sub-processor update policy.

Reference: Sub-processors

CHNG-02 YES

Does the system support client customizations from one release to another?*

Per-institution configuration (retention window, roles, institution type) is preserved across releases.

CHNG-03 COMPENSATING CONTROL

Do you have an implemented system configuration management process (e.g., secure "gold" images, etc.)?*

Configuration is managed as infrastructure-as-code with reproducible builds and managed runtimes (Cloudflare Pages, Supabase), rather than hand-configured servers.

CHNG-04 YES

Do you have a documented change management process?

Changes are version-controlled and flow through a preview-to-production pipeline with a manual smoke test before production.

CHNG-05 YES

Does your change management process minimally include authorization, impact analysis, testing, and validation before moving changes to production?

The change process includes authorization, impact analysis, testing, and validation before production.

CHNG-06 YES

Does your change management process verify that all required third-party libraries and dependencies are still supported with each major change?

Third-party libraries and dependencies are reviewed for continued support as part of each significant change.

CHNG-07 COMPENSATING CONTROL

Do you have policy and procedure, currently implemented, managing how critical patches are applied to all systems and applications?

Managed runtimes (Cloudflare Workers, Supabase) are patched by the providers; application dependencies are updated promptly through the change pipeline. A formally documented patch policy is maturing.

CHNG-08 COMPENSATING CONTROL

Have you implemented policies and procedures that guide how security risks are mitigated until patches can be applied?

Where a fix cannot ship immediately, exposure is reduced through edge controls (Cloudflare WAF), least privilege, and the minimal data footprint. A documented interim-mitigation procedure is maturing.

CHNG-09 NO

Do clients have the option to not participate in or postpone an upgrade to a new release?

Aletheia is a continuously delivered SaaS; all customers run the current version so that security fixes reach everyone. Institutions are notified of material changes.

CHNG-10 COMPENSATING CONTROL

Do you have a fully implemented solution support strategy that defines how many concurrent versions you support?

A single current version is supported, which keeps every customer on patched code and minimizes exposure from unsupported versions.

CHNG-11 YES

Do you have a release schedule for product updates?

Aletheia is continuously delivered; material changes are announced to institutional customers.

CHNG-12 COMPENSATING CONTROL

Do you have a technology roadmap, for at least the next two years, for enhancements and bug fixes for the solution being assessed?

A product roadmap is maintained and shared with institutional buyers on request. A formally published two-year roadmap is maturing.

CHNG-13 YES

Can solution updates be completed without institutional involvement (i.e., technically or organizationally)?

Updates are deployed by Lonia without requiring institutional involvement.

CHNG-14 YES

Are upgrades or system changes installed during off-peak hours or in a manner that does not impact the customer?

Static-site and serverless deploys are effectively zero-downtime and do not require a maintenance window that affects users.

CHNG-15 YES

Do procedures exist to provide that emergency changes are documented and authorized (including after-the-fact approval)?

Emergency changes are documented and authorized, including after-the-fact approval where speed is required.

CHNG-16 COMPENSATING CONTROL

Do you have a systems management and configuration strategy that encompasses servers, appliances, cloud services, applications, and mobile devices (company and employee owned)?

Aletheia's footprint is managed and serverless (Cloudflare, Supabase) rather than a fleet of servers and appliances; endpoint posture is managed for a small remote team.

PPPR-01 COMPENSATING CONTROL

Do you have a documented patch management process?*

Managed runtimes are patched by the providers; application dependencies are updated through the change pipeline. A formally documented patch-management policy is maturing.

PPPR-02 YES

Can your organization comply with institutional policies on privacy and data protection with regard to users of institutional systems, if required?*

Aletheia can comply with institutional privacy and data-protection policies for users of institutional systems.

Reference: Privacy Policy

PPPR-03 YES

Is your company subject to the institution's geographic region's laws and regulations?*

Aletheia is subject to the applicable laws of the institution's region for the services it provides, and offers a DPA with SCCs where relevant.

Reference: DPA

PPPR-04 YES

Can you accommodate encryption requirements using open standards?

Encryption uses open standards (TLS 1.3, AES-256, AES-GCM-256, WebCrypto).

Reference: Security Whitepaper

PPPR-05 COMPENSATING CONTROL

Do you have a documented systems development life cycle (SDLC)?

Development follows a defined, version-controlled process with review and a preview-to-production pipeline. A formally documented SDLC is maturing.

PPPR-06 ROADMAP

Do you perform background screenings or multi-state background checks on all employees prior to their first day of work?

Formal pre-employment background screening is being established as the team grows; confirm current practice with the vendor.

PPPR-07 COMPENSATING CONTROL

Do you require new employees to fill out agreements and review policies?

Confidentiality and acceptable-use expectations apply to team members; formal signed onboarding agreements and policy attestations are maturing.

PPPR-08 COMPENSATING CONTROL

Do you have a documented information security policy?

Security controls are documented in the Security Whitepaper. A formal internal information-security policy document is maturing.

Reference: Security Whitepaper

PPPR-09 YES

Are information security principles designed into the product lifecycle?

Security is designed into the product lifecycle from the first commit under the Three Pillars.

Reference: Security Whitepaper

PPPR-10 YES

Will you comply with applicable breach notification laws?

Aletheia commits to applicable breach-notification laws, including the 72-hour notification in the DPA.

Reference: DPA

PPPR-11 ROADMAP

Do you have an information security awareness program?

A formal, tracked security-awareness program is being established as the team grows.

PPPR-12 ROADMAP

Is security awareness training mandatory for all employees?

Mandatory, tracked security training is being formalized; confirm current status with the vendor.

PPPR-13 COMPENSATING CONTROL

Do you have process and procedure(s) documented, and currently followed, that require a review and update of the access list(s) for privileged accounts?

Privileged access is minimal and least-privilege by design; access is reviewed periodically. A formally documented review cadence is maturing.

PPPR-14 COMPENSATING CONTROL

Do you have documented, and currently implemented, internal audit processes and procedures?

Self-review against the Three Pillars is built into the development process. A formal internal-audit program is maturing.

PPPR-15 COMPENSATING CONTROL

Does your organization have physical security controls and policies in place?

Aletheia holds no institutional data in physical offices or its own data centers (cloud-hosted, remote team). Physical security of infrastructure is provided by the cloud providers.

Reference: Sub-processors

3. Product: Authentication and Data (41 questions)

AAAI-01 YES

Does your solution support single sign-on (SSO) protocols for user and administrator authentication?*

Aletheia is OAuth SSO only on every tier, including Free: Google Workspace and Microsoft 365 via OIDC. Sessions are managed by Supabase Auth.

Reference: Security Whitepaper

AAAI-02 NO

For customers not using SSO, does your solution support local authentication protocols for user and administrator authentication?*

By design there is no local password authentication on any tier. Aletheia is OAuth-only and stores zero passwords. This is a deliberate security posture, not a gap.

Reference: Security Whitepaper

AAAI-03 N/A

For customers not using SSO, can you enforce password/passphrase complexity requirements (provided by the institution)?*

There is no local password authentication, so password complexity enforcement does not apply. Complexity and MFA are enforced by the institution's identity provider.

Reference: Security Whitepaper

AAAI-04 N/A

For customers not using SSO, does the system have password complexity or length limitations and/or restrictions?*

No passwords exist in the system, so password length/complexity limitations do not apply.

Reference: Security Whitepaper

AAAI-05 N/A

For customers not using SSO, do you have documented password/passphrase reset procedures that are currently implemented in the system and/or customer support?*

There are no passwords and therefore no password reset flow. Account recovery is handled by the institution's identity provider.

Reference: Security Whitepaper

AAAI-06 ROADMAP

Does your organization participate in InCommon or another eduGAIN-affiliated trust federation?*

SSO is offered through Google Workspace and Microsoft 365 (the institution's identity provider). Direct InCommon / eduGAIN federation is not currently offered and is on the roadmap if institutions require it.

AAAI-07 NO

Are there any passwords/passphrases hard-coded into your systems or solutions?*

No passwords or passphrases are hard-coded into Aletheia's systems.

AAAI-08 NO

Are you storing any passwords in plaintext?*

Aletheia stores no passwords at all, in plaintext or otherwise.

Reference: Security Whitepaper

AAAI-09 COMPENSATING CONTROL

Are audit logs available that include AT LEAST all of the following: login, logout, actions performed, and source IP address?*

User and administrator actions are recorded in append-only (WORM) audit logs. Authentication events (login/logout, including source IP) are handled and logged by the institution's OAuth identity provider, since Aletheia performs no local authentication.

Reference: Security Whitepaper

AAAI-10

Describe or provide a reference to the (a) system capability to log security/authorization changes, as well as user and administrator security events (i.e., physical or electronic), such as login failures, access denied, changes accepted; and (b) all requirements necessary to implement logging and monitoring on the system. Include (c) information about SIEM/log collector usage.*

Response: Aletheia writes user actions to aletheia_audit_log and institutional admin actions to aletheia_institutional_admin_audit_log; both are append-only (insert and read policies only, no UPDATE or DELETE). Privileged operations emit their audit records through server-side RPCs. Authentication events are logged by the institution's identity provider (Google Workspace / Microsoft 365).

Reference: Security Whitepaper

AAAI-11 YES

Can you provide the institution documentation regarding the retention period for those logs, how logs are protected, and whether they are accessible to the customer (and if so, how)?*

Audit records are append-only and protected by row-level security. Institutional administrators can view the institutional admin audit trail. Retention is documented in the Security Whitepaper.

Reference: Security Whitepaper

AAAI-12 N/A

For customers not using SSO, does your application support integration with other authentication and authorization systems?

Aletheia authenticates only through Google Workspace and Microsoft 365 SSO; there is no separate non-SSO authentication path to integrate.

Reference: Security Whitepaper

AAAI-13 ROADMAP

Do you allow the customer to specify attribute mappings for any needed information beyond a user identifier? (e.g., Reference eduPerson, ePPA/ePPN/ePE)

Standard OIDC identity claims are consumed today. Custom attribute mapping (for example eduPerson / ePPN) is on the roadmap for institutions that require it.

AAAI-14 N/A

For customers not using SSO, does your application support directory integration for user accounts?

User accounts are provisioned through the institution's OAuth identity provider; there is no separate directory-integration path for a non-SSO mode, which does not exist.

Reference: Security Whitepaper

AAAI-15 YES

Does your solution support any of the following web SSO standards: SAML2 (with redirect flow), OIDC, CAS, or other?

Aletheia uses OIDC through Google Workspace and Microsoft 365.

Reference: Security Whitepaper

AAAI-16 YES

Do you support differentiation between email address and user identifier?

Aletheia distinguishes the account identifier from the email address as asserted by the identity provider.

AAAI-17 COMPENSATING CONTROL

For customers not using SSO, does your application and/or user frontend/portal support multifactor authentication (e.g., Duo, Google Authenticator, OTP, etc.)?

Because authentication is SSO-only, multi-factor authentication is enforced by the institution's identity provider (Google Workspace / Microsoft 365) and inherited by Aletheia for every user.

Reference: Security Whitepaper

AAAI-18 YES

Does your application automatically lock the session or log out an account after a period of inactivity?

Sessions expire and re-authentication is required after inactivity, governed by Supabase Auth session management and the identity provider's session policy.

DATA-01 NO

Will the institution's data be stored on any devices (database servers, file servers, SAN, NAS, etc.) configured with non-RFC 1918/4193 (i.e., publicly routable) IP addresses?*

Databases are not exposed on publicly routable addresses; Supabase PostgreSQL is reached through managed, authenticated endpoints.

DATA-02 YES

Is the transport of sensitive data encrypted using security protocols/algorithms (e.g., system-to-client)?*

All transport is encrypted with TLS 1.3, terminated at the Cloudflare edge and encrypted onward to Supabase.

Reference: Security Whitepaper

DATA-03 YES

Is the storage of sensitive data encrypted using security protocols/algorithms (e.g., disk encryption, at-rest, files, and within a running database)?*

Account data is encrypted at rest with Supabase-managed AES-256. On Professional BYOK, the user's API key is stored on-device with a non-extractable AES-GCM-256 key. On Enterprise BYOK, the institution's key is envelope-encrypted with a master key and stored encrypted at rest, decrypted by Lonia's Enterprise Worker only in memory at request time.

Reference: Security Whitepaper

DATA-04 COMPENSATING CONTROL

Do all cryptographic modules in use in your solution conform to the Federal Information Processing Standards (FIPS PUB 140-2 or 140-3)?*

Aletheia relies on platform cryptography (Cloudflare TLS, AWS/Supabase at-rest encryption, and the browser WebCrypto API). FIPS 140-2/3 validated modules are used where the underlying provider offers them; Aletheia does not independently FIPS-certify its own modules.

Reference: Security Whitepaper

DATA-05 YES

Will the institution's data be available within the system for a period of time at the completion of this contract?*

Account data can be exported, and a wind-down period at contract completion allows the institution to retrieve data before deletion.

Reference: DPA

DATA-06 YES

Are ownership rights to all data, inputs, outputs, and metadata retained even through a provider acquisition or bankruptcy event?*

The institution retains ownership of its data, inputs, outputs, and metadata, including through an acquisition or bankruptcy event (90-day migration commitment in the DPA).

Reference: DPA

DATA-07 NO

Do backups containing the institution's data ever leave the institution's data zone either physically or via network routing?*

Backups remain within the US region; they do not leave the data zone.

Reference: Sub-processors

DATA-08 COMPENSATING CONTROL

Is media used for long-term retention of business data and archival purposes stored in a secure, environmentally protected area?*

Aletheia stores no physical media. Backups are managed by Supabase (encrypted, US region) with the provider's environmental and physical controls.

Reference: Sub-processors

DATA-09 YES

At the completion of this contract, will data be returned to the institution and/or deleted from all your systems and archives?

At contract completion, account data is returned (export) and/or deleted, with append-only audit records retained only where legally required.

Reference: DPA

DATA-10 YES

Can the institution extract a full or partial backup of data?

Institutions can export account data, and end users can export their on-device document library at any time.

Reference: DPA

DATA-11 COMPENSATING CONTROL

Do current backups include all operating system software, utilities, security software, application software, and data files necessary for recovery?

Supabase managed backups plus infrastructure-as-code redeploy cover recovery of the service and account data. User documents live on the device, so they are recovered from the user's own library rather than a server backup.

DATA-12 COMPENSATING CONTROL

Are you performing off-site backups (i.e., digitally moved off site)?

Supabase performs managed, geographically durable backups within the US region.

Reference: Sub-processors

DATA-13 N/A

Are physical backups taken off-site (i.e., physically moved off site)?

No physical backup media exists; backups are cloud-managed by Supabase.

Reference: Sub-processors

DATA-14 YES

Are data backups encrypted?

Backups are encrypted by the managed database provider.

Reference: Sub-processors

DATA-15 COMPENSATING CONTROL

Do you have a media handling process that is documented and currently implemented that meets established business needs and regulatory requirements, including end-of-life, repurposing, and data-sanitization procedures?

Aletheia handles no physical media. Media lifecycle, end-of-life, and sanitization are handled by AWS, Supabase, and Cloudflare under their own programs.

Reference: Sub-processors

DATA-16 COMPENSATING CONTROL

Does the process described in DATA-15 adhere to DoD 5220.22-M and/or NIST SP 800-88 standards?

Media sanitization to NIST SP 800-88 is inherited from the underlying cloud providers (AWS via Supabase, Cloudflare).

Reference: Sub-processors

DATA-17 NO

Does your staff (or third party) have access to institutional data (e.g., financial, PHI, or other sensitive information) through any means?

Staff do not access user documents (they are processed and stored on-device). Access to limited account data is least-privilege and audit-logged.

Reference: Security Whitepaper

DATA-18 COMPENSATING CONTROL

Do you have a documented and currently implemented strategy for securing employee workstations when they work remotely (i.e., not in a trusted computing environment)?

The remote team uses least-privilege, OAuth-authenticated access; user documents are never stored on staff workstations because they live on the end user's device. A formally documented remote-workstation standard is maturing.

DATA-19 YES

Does the environment provide for dedicated single-tenant capabilities? If not, describe how your solution or environment separates data from different customers (e.g., logically, physically, single tenancy, multi-tenancy).

Aletheia is multi-tenant with row-level security enforcing per-user and per-institution isolation on every table; student-scoped tables carry institution_id from creation.

Reference: Security Whitepaper

DATA-20 YES

Are ownership rights to all data, inputs, outputs, and metadata retained by the institution?

The institution retains ownership rights to all its data, inputs, outputs, and metadata.

Reference: DPA

DATA-21 YES

In the event of imminent bankruptcy, closing of business, or retirement of service, will you provide 90 days for customers to get their data out of the system and migrate applications?

The DPA commits to a 90-day window for customers to retrieve data and migrate in a bankruptcy or service-retirement event.

Reference: DPA

DATA-22 COMPENSATING CONTROL

Are involatile backup copies made according to predefined schedules and securely stored and protected?

Backups are made on the managed provider's schedule and stored encrypted within the US region.

Reference: Sub-processors

DATA-23 COMPENSATING CONTROL

Do you have a cryptographic key management process (generation, exchange, storage, safeguards, use, vetting, and replacement) that is documented and currently implemented, for all system components (e.g., database, system, web, etc.)?

At-rest keys are managed by Supabase / AWS KMS; TLS keys are managed by Cloudflare; BYOK keys are generated and held non-extractably on the user's device and never reach Lonia. Key handling is described in the Security Whitepaper.

Reference: Security Whitepaper

4. Infrastructure: Application, Hosting, Network, Incident, Vulnerability (51 questions)

APPL-01 YES

Are access controls for institutional accounts based on structured rules, such as role-based access control (RBAC), attribute-based access control (ABAC), or policy-based access control (PBAC)?*

Institutional access is role-based: Primary (full), Secondary (day-to-day seat/license management), and Read-only (reporting). A separate FERPA-privileged flag, off by default, is the only path to individual student-scoped visibility and is two-gate enforced and audit-logged.

Reference: Security Whitepaper

APPL-02 COMPENSATING CONTROL

Are you using a web application firewall (WAF)?*

Cloudflare provides a web application firewall, DDoS protection, and bot management (Turnstile) at the edge in front of the application.

Reference: Sub-processors

APPL-03 YES

Are only currently supported operating system(s), software, and libraries leveraged by the system(s)/application(s) that will have access to institution's data?*

The application runs on managed, currently supported runtimes (Cloudflare Workers, Supabase); dependencies are kept current.

APPL-04 NO

Does your application require access to location or GPS data?*

Aletheia does not require or request location or GPS data.

APPL-05 YES

Does your application provide separation of duties between security administration, system administration, and standard user functions?*

Administrative, system, and standard-user functions are separated through least-privilege roles and scoped service roles.

Reference: Security Whitepaper

APPL-06 COMPENSATING CONTROL

Do you subject your code to static code analysis and/or static application security testing prior to release?*

Code is reviewed before release and dependencies are scanned automatically. A formal static application security testing (SAST) tool is being adopted; confirm current tooling with the vendor.

APPL-07 YES

Do you have software testing processes (dynamic or static) that are established and followed?*

Changes flow through a Cloudflare Pages preview-to-production pipeline with a manual smoke test before production deploys.

APPL-08 YES

Are access controls for staff within your organization based on structured rules, such as RBAC, ABAC, or PBAC?

Staff access follows least-privilege, role-based rules; sensitive operations run through scoped service roles.

Reference: Security Whitepaper

APPL-09 YES

Does the system provide data input validation and error messages?

User inputs are validated and sanitized, and the application returns controlled error messages without leaking sensitive detail.

APPL-10 COMPENSATING CONTROL

Do you have a process and implemented procedures for managing your software supply chain (e.g., libraries, repositories, frameworks, etc.)?

Dependencies are pinned and updated through the change pipeline with automated vulnerability scanning. A formal software bill of materials (SBOM) process is maturing.

APPL-11 COMPENSATING CONTROL

Have your developers been trained in secure coding techniques?

The team builds to secure-by-default patterns (OAuth-only, RLS, encryption, input validation). Formal, tracked secure-coding training is maturing; confirm status with the vendor.

Reference: Security Whitepaper

APPL-12 YES

Was your application developed using secure coding techniques?

The application was built to the Three Pillars (accessibility, compliance, security) from the first commit, including input validation, output encoding, and a content security policy.

Reference: Security Whitepaper

APPL-13 N/A

If mobile, is the application available from a trusted source (e.g., App Store, Google Play Store)?

Aletheia is delivered as a responsive web application, not a native mobile app distributed through an app store.

APPL-14 YES

Do you have a fully implemented policy or procedure that details how your employees obtain administrator access to institutional instance of the application?

Administrator access to an institutional instance is granted through OAuth-based roles under least privilege; the model is documented in the Security Whitepaper.

Reference: Security Whitepaper

DCTR-01

Select your hosting option.

Response: Cloud hosted (Supabase on AWS for the database; Cloudflare for edge and compute). Aletheia operates no data centers of its own.

Reference: Sub-processors

DCTR-02 COMPENSATING CONTROL

Is a SOC 2 Type 2 report available for the hosting environment?

The hosting providers (AWS underlying Supabase, and Cloudflare) maintain SOC 2 Type 2 reports for their environments. Aletheia itself is not SOC 2 audited.

Reference: Sub-processors

DCTR-03 COMPENSATING CONTROL

Are you generally able to accommodate storing each institution's data within its geographic region?

Data is currently stored in a single US region. Broader per-region placement follows the provider's available regions; confirm requirements with the vendor.

Reference: Sub-processors

DCTR-04 COMPENSATING CONTROL

Are the data centers staffed 24 hours a day, seven days a week (i.e., 24 x 7 x 365)?

Aletheia operates no data centers of its own. Hosting is Supabase (on AWS) and Cloudflare, whose certified data centers provide this control. See the Sub-processor list.

Reference: Sub-processors

DCTR-05 COMPENSATING CONTROL

Are your servers separated from other companies via a physical barrier, such as a cage or hard walls?

Aletheia operates no data centers of its own. Hosting is Supabase (on AWS) and Cloudflare, whose certified data centers provide this control. See the Sub-processor list.

Reference: Sub-processors

DCTR-06 COMPENSATING CONTROL

Does a physical barrier fully enclose the physical space, preventing unauthorized physical contact with any of your devices?*

Aletheia operates no data centers of its own. Hosting is Supabase (on AWS) and Cloudflare, whose certified data centers provide this control. See the Sub-processor list.

Reference: Sub-processors

DCTR-07 COMPENSATING CONTROL

Are your primary and secondary data centers geographically diverse?

Geographic diversity and redundancy are provided by the underlying cloud platforms (AWS, Cloudflare). Aletheia operates no data centers of its own. Hosting is Supabase (on AWS) and Cloudflare, whose certified data centers provide this control. See the Sub-processor list.

Reference: Sub-processors

DCTR-08 COMPENSATING CONTROL

Is the service hosted in a high-availability environment?

High availability is provided by the Cloudflare edge and Supabase managed platform. Aletheia operates no data centers of its own. Hosting is Supabase (on AWS) and Cloudflare, whose certified data centers provide this control. See the Sub-processor list.

Reference: Sub-processors

DCTR-09 COMPENSATING CONTROL

Is redundant power available for all data centers where institutional data will reside?

Aletheia operates no data centers of its own. Hosting is Supabase (on AWS) and Cloudflare, whose certified data centers provide this control. See the Sub-processor list.

Reference: Sub-processors

DCTR-10 COMPENSATING CONTROL

Are redundant power strategies tested?*

Aletheia operates no data centers of its own. Hosting is Supabase (on AWS) and Cloudflare, whose certified data centers provide this control. See the Sub-processor list.

Reference: Sub-processors

DCTR-11 COMPENSATING CONTROL

Does the center where the data will reside have cooling and fire-suppression systems that are active and regularly tested?

Aletheia operates no data centers of its own. Hosting is Supabase (on AWS) and Cloudflare, whose certified data centers provide this control. See the Sub-processor list.

Reference: Sub-processors

DCTR-12 COMPENSATING CONTROL

Do you have Internet Service Provider (ISP) redundancy?

Aletheia operates no data centers of its own. Hosting is Supabase (on AWS) and Cloudflare, whose certified data centers provide this control. See the Sub-processor list.

Reference: Sub-processors

DCTR-13 COMPENSATING CONTROL

Does every data center where the institution's data will reside have multiple telephone company or network provider entrances to the facility?

Aletheia operates no data centers of its own. Hosting is Supabase (on AWS) and Cloudflare, whose certified data centers provide this control. See the Sub-processor list.

Reference: Sub-processors

DCTR-14 YES

Do you require multifactor authentication for all administrative accounts in your environment?

Administrative access requires multi-factor authentication, enforced through the OAuth identity provider (Google Workspace / Microsoft 365).

Reference: Security Whitepaper

DCTR-15 YES

Are you using your cloud provider's available hardening tools or pre-hardened images?

Aletheia uses managed, hardened runtimes and enables the cloud providers' available security features.

DCTR-16 COMPENSATING CONTROL

Does your cloud solution provider have access to your encryption keys?

Database at-rest encryption keys are managed by the platform provider (Supabase / AWS KMS), which is standard for managed hosting. On Professional BYOK, the key protecting the user's AI credentials is non-extractable and never leaves the user's device, so no cloud provider, and not Lonia, can access it. On Enterprise BYOK, the institution's key is envelope-encrypted with a master key and stored encrypted at rest; only Lonia's Enterprise Worker decrypts it, in memory at request time, and the key material is never returned to any client.

Reference: Security Whitepaper

FIDP-01 COMPENSATING CONTROL

Are you utilizing a stateful packet inspection (SPI) firewall?*

Aletheia runs on managed serverless infrastructure with no self-managed network devices. Network firewalling, intrusion detection and prevention, DDoS mitigation, and monitoring are provided by Cloudflare (edge) and AWS/Supabase.

Reference: Sub-processors

FIDP-02 COMPENSATING CONTROL

Do you have a documented policy for firewall change requests?*

Edge firewall and WAF rules are managed through Aletheia's change process on Cloudflare; underlying network firewalling is provider-managed.

Reference: Sub-processors

FIDP-03 COMPENSATING CONTROL

Have you implemented an intrusion detection system (network-based)?*

Aletheia runs on managed serverless infrastructure with no self-managed network devices. Network firewalling, intrusion detection and prevention, DDoS mitigation, and monitoring are provided by Cloudflare (edge) and AWS/Supabase.

Reference: Sub-processors

FIDP-04 COMPENSATING CONTROL

Do you employ host-based intrusion detection?*

There are no self-managed hosts; the serverless platform is monitored by the providers.

Reference: Sub-processors

FIDP-05 COMPENSATING CONTROL

Are audit logs available for all changes to the network, firewall, IDS, and IPS systems?*

Changes to edge/network controls are logged by Cloudflare and Supabase.

Reference: Sub-processors

FIDP-06 COMPENSATING CONTROL

Is authority for firewall change approval documented? Please list approver names or titles in Additional Info.

Edge/WAF change approval sits with Lonia engineering leadership; underlying network change control is provider-managed.

Reference: Sub-processors

FIDP-07 COMPENSATING CONTROL

Have you implemented an intrusion prevention system (network-based)?

Cloudflare provides WAF and DDoS/intrusion prevention at the edge.

Reference: Sub-processors

FIDP-08 COMPENSATING CONTROL

Do you employ host-based intrusion prevention?

No self-managed hosts exist; prevention is handled at the managed-platform layer.

Reference: Sub-processors

FIDP-09 COMPENSATING CONTROL

Are you employing any next-generation persistent threat (NGPT) monitoring?

Advanced threat monitoring is provided by the cloud platforms (Cloudflare, AWS).

Reference: Sub-processors

FIDP-10

Is intrusion monitoring performed internally or by a third-party service?

Response: Intrusion monitoring is provided by the hosting providers (Cloudflare and AWS/Supabase) as part of their managed platforms.

Reference: Sub-processors

FIDP-11 COMPENSATING CONTROL

Do you monitor for intrusions on a 24 x 7 x 365 basis?

The cloud providers monitor their platforms on a 24x7 basis. Aletheia does not staff an internal 24x7 security operations center.

Reference: Sub-processors

HFIH-01 YES

Do you have a formal incident response plan?

Aletheia has a documented incident-response process: reports go to security@lonia.ai, acknowledgment is targeted within 24 hours, and where institutional personal data is affected, notification follows the DPA timeline (72 hours, GDPR Art. 33). Formalization of the written plan continues.

Reference: Security Whitepaper

HFIH-02 COMPENSATING CONTROL

Do you either have an internal incident response team or retain an external team?

Incident response is handled by Lonia engineering leadership, with external counsel and forensic support engaged as needed. A standing external retainer is under consideration.

HFIH-03 COMPENSATING CONTROL

Do you have the capability to respond to incidents on a 24 x 7 x 365 basis?

The cloud platforms provide 24x7 monitoring and alerting. Aletheia does not staff an internal 24x7 security operations center but commits to a 24-hour acknowledgment target.

HFIH-04 ROADMAP

Do you carry cyber-risk insurance to protect against unforeseen service outages, data that is lost or stolen, and security incidents?

Cyber-risk insurance is being evaluated as the business scales; confirm current coverage with the vendor.

VULN-01 COMPENSATING CONTROL

Are your systems and applications scanned with an authenticated user account for vulnerabilities (that are remediated) prior to new releases?*

Dependencies are scanned automatically and code is reviewed before release. Authenticated dynamic scanning is being adopted.

VULN-02 COMPENSATING CONTROL

Will you provide results of application and system vulnerability scans to the institution?*

Available scan and assessment results can be shared with an institution on request, under NDA where appropriate.

VULN-03 YES

Will you allow the institution to perform its own vulnerability testing and/or scanning of your systems and/or application, provided that testing is performed at a mutually agreed upon time and date?*

An institution may perform its own vulnerability testing or scanning of the service at a mutually agreed time.

VULN-04 NO

Have your systems and applications had a third-party security assessment completed in the last year?

A third-party security assessment (penetration test) has not been conducted in the past year; the posture is self-evaluated. A third-party assessment is on the roadmap.

Reference: Security Whitepaper

VULN-05 COMPENSATING CONTROL

Do you regularly scan for common web application security vulnerabilities (e.g., SQL injection, XSS, XSRF, etc.)?

Common web vulnerabilities are mitigated by design: parameterized queries and RLS (SQL injection), output encoding and a content security policy (XSS), and framework CSRF protections. Dependency scanning is automated; formal DAST is maturing.

Reference: Security Whitepaper

VULN-06 COMPENSATING CONTROL

Are your systems and applications regularly scanned externally for vulnerabilities?

The Cloudflare edge provides external protection and monitoring; scheduled external vulnerability scanning is being formalized.

5. IT Accessibility (18 questions)

ITAC-01

Solution Provider Accessibility Contact Name

Response: Lonia AI accessibility contact

Reached at accessibility@lonia.ai.

Reference: VPAT

ITAC-02

Solution Provider Accessibility Contact Title

Response: Accessibility contact

ITAC-03

Solution Provider Accessibility Contact Email

Response: accessibility@lonia.ai

ITAC-04

Solution Provider Accessibility Contact Phone Number

Response: Available on request via accessibility@lonia.ai

ITAC-05

Web Link to Accessibility Statement or VPAT

Response: https://aletheia.lonia.ai/accessibility/vpat

VPAT / Accessibility Conformance Report, with a tagged PDF at /accessibility/vpat-aletheia.pdf.

Reference: VPAT

ITAC-06 YES

Has a VPAT or ACR been created or updated for the solution and version under consideration within the past 12 months?*

The VPAT / ACR was published for the current version in 2026 and is reviewed at least annually or on material change.

Reference: VPAT

ITAC-07 YES

Will your company agree to meet your stated accessibility standard or WCAG 2.1 AA as part of your contractual agreement for the solution?*

Aletheia commits contractually to WCAG 2.2 AA, which supersets WCAG 2.1 AA.

Reference: VPAT

ITAC-08 YES

Does the solution substantially conform to WCAG 2.1 AA?*

Aletheia targets WCAG 2.2 AA, which exceeds WCAG 2.1 AA. The published VPAT documents criterion-level conformance, including a small number of criteria still under manual verification.

Reference: VPAT

ITAC-09 YES

Do you have a documented and implemented process for reporting and tracking accessibility issues?*

Accessibility issues can be reported to accessibility@lonia.ai and are tracked to resolution.

Reference: VPAT

ITAC-10 YES

Do you have documentation to support the accessibility features of your solution?

Accessibility documentation includes the VPAT, the EAA conformance statement, and the EN 301 549 mapping.

Reference: VPAT

ITAC-11 NO

Has a third-party expert conducted an audit of the most recent version of your solution?

A formal third-party accessibility audit has not yet been conducted; conformance is currently self-evaluated against WCAG 2.2 AA. A third-party audit is planned.

Reference: VPAT

ITAC-12 YES

Do you have a documented and implemented process for verifying accessibility conformance?

Conformance is verified through a documented internal process combining automated checks, keyboard and screen-reader testing, and criterion-level review recorded in the VPAT.

Reference: VPAT

ITAC-13 YES

Have you adopted a technical or legal standard of conformance for the solution?

Aletheia has adopted WCAG 2.2 AA and Revised Section 508 as its standard of conformance, and aligns with EN 301 549 for the EU.

Reference: EN 301 549 Mapping

ITAC-14 YES

Can you provide a current, detailed accessibility roadmap with delivery timelines?

A criterion-level VPAT records current conformance, and the accessibility roadmap covers the criteria under manual verification. Timelines are provided to buyers on request.

Reference: VPAT

ITAC-15 YES

Do you expect your staff to maintain a current skill set in IT accessibility?

Accessibility is a first-principle of the product, and the team maintains current accessibility skills as part of the development lifecycle.

ITAC-16 YES

Do you have documented processes and procedures for implementing accessibility into your development lifecycle?

Accessibility is built in from the first commit: semantic HTML, keyboard operability, focus-visible outlines, and contrast are architectural requirements, not later fixes.

Reference: VPAT

ITAC-17 YES

Can all functions of the application or service be performed using only the keyboard?

Every function is operable using only the keyboard (Tab / Enter / Escape); full keyboard navigation is an architectural requirement.

Reference: VPAT

ITAC-18 NO

Does your product rely on activating a special "accessibility mode," a "lite version," or using an alternate interface (including "overlay" or AI-based alternates) for accessibility purposes?

Aletheia's own interface is natively accessible and does not rely on a special "accessibility mode," a "lite version," or an overlay for its own conformance. Aletheia is a user-side assistive tool that makes other content accessible; its own UI conforms to WCAG 2.2 AA directly.

Reference: VPAT

6. Case-Specific: Consulting, HIPAA, PCI, Operations (60 questions)

CONS-01 N/A

Will the consultant require access to the institution's network resources?*

Aletheia is a software product, not a consulting engagement (see REQU-03). No consultant accesses the institution's networks, hardware, accounts, or data.

CONS-02 N/A

Has the consultant received training on (sensitive, HIPAA, PCI, etc.) data handling?*

Aletheia is a software product, not a consulting engagement (see REQU-03). No consultant accesses the institution's networks, hardware, accounts, or data.

CONS-03 N/A

Is the data encrypted (at rest) while in the consultant's possession?*

Aletheia is a software product, not a consulting engagement (see REQU-03). No consultant accesses the institution's networks, hardware, accounts, or data.

CONS-04 N/A

Can access be restricted based on source IP address?*

Aletheia is a software product, not a consulting engagement (see REQU-03). No consultant accesses the institution's networks, hardware, accounts, or data.

CONS-05 N/A

Will the consulting take place on-premises?

Aletheia is a software product, not a consulting engagement (see REQU-03). No consultant accesses the institution's networks, hardware, accounts, or data.

CONS-06 N/A

Will the consultant require access to hardware in the institution's data centers?

Aletheia is a software product, not a consulting engagement (see REQU-03). No consultant accesses the institution's networks, hardware, accounts, or data.

CONS-07 N/A

Will the consultant require an account within the institution's domain (@*.edu)?

Aletheia is a software product, not a consulting engagement (see REQU-03). No consultant accesses the institution's networks, hardware, accounts, or data.

CONS-08 N/A

Will any data be transferred to the consultant's possession?

Aletheia is a software product, not a consulting engagement (see REQU-03). No consultant accesses the institution's networks, hardware, accounts, or data.

CONS-09 N/A

Will the consultant need remote access to the institution's network or systems?

Aletheia is a software product, not a consulting engagement (see REQU-03). No consultant accesses the institution's networks, hardware, accounts, or data.

HIPA-01 N/A

Do your workforce members receive regular training related to the Health Insurance Portability and Accountability Act (HIPAA) Privacy and Security Rules and the HITECH Act?*

Aletheia is not designed to process protected health information and is not a HIPAA-covered platform (see REQU-05); user documents are processed on-device. This question does not apply to a standard deployment.

Reference: Privacy Policy

HIPA-02 N/A

Have you identified areas of risk?*

Aletheia is not designed to process protected health information and is not a HIPAA-covered platform (see REQU-05); user documents are processed on-device. This question does not apply to a standard deployment.

Reference: Privacy Policy

HIPA-03 N/A

Have the relevant policies/plans been tested?*

Aletheia is not designed to process protected health information and is not a HIPAA-covered platform (see REQU-05); user documents are processed on-device. This question does not apply to a standard deployment.

Reference: Privacy Policy

HIPA-04 N/A

Have you entered into a Business Associate Agreements with all subcontractors who may have access to protected health information (PHI)?*

Aletheia is not designed to process protected health information and is not a HIPAA-covered platform (see REQU-05); user documents are processed on-device. This question does not apply to a standard deployment.

Reference: Privacy Policy

HIPA-05 N/A

Do you monitor or receive information regarding changes in HIPAA regulations?

Aletheia is not designed to process protected health information and is not a HIPAA-covered platform (see REQU-05); user documents are processed on-device. This question does not apply to a standard deployment.

Reference: Privacy Policy

HIPA-06 N/A

Has your organization designated HIPAA Privacy and Security officers as required by the rules?

Aletheia is not designed to process protected health information and is not a HIPAA-covered platform (see REQU-05); user documents are processed on-device. This question does not apply to a standard deployment.

Reference: Privacy Policy

HIPA-07 N/A

Do you comply with the requirements of the Health Information Technology for Economic and Clinical Health Act (HITECH)?

Aletheia is not designed to process protected health information and is not a HIPAA-covered platform (see REQU-05); user documents are processed on-device. This question does not apply to a standard deployment.

Reference: Privacy Policy

HIPA-08 N/A

Have you conducted a risk analysis as required under the HIPAA Security Rule?

Aletheia is not designed to process protected health information and is not a HIPAA-covered platform (see REQU-05); user documents are processed on-device. This question does not apply to a standard deployment.

Reference: Privacy Policy

HIPA-09 N/A

Have you taken actions to mitigate the identified risks?

Aletheia is not designed to process protected health information and is not a HIPAA-covered platform (see REQU-05); user documents are processed on-device. This question does not apply to a standard deployment.

Reference: Privacy Policy

HIPA-10 N/A

Does your application require user and system administrator password changes at a frequency no greater than 90 days?

Aletheia is not designed to process protected health information and is not a HIPAA-covered platform (see REQU-05); user documents are processed on-device. This question does not apply to a standard deployment.

Reference: Privacy Policy

HIPA-11 N/A

Does your application require users to set their own password after an administrator reset or on first use of the account?

Aletheia is not designed to process protected health information and is not a HIPAA-covered platform (see REQU-05); user documents are processed on-device. This question does not apply to a standard deployment.

Reference: Privacy Policy

HIPA-12 N/A

Does your application lock out an account after a number of failed login attempts?

Aletheia is not designed to process protected health information and is not a HIPAA-covered platform (see REQU-05); user documents are processed on-device. This question does not apply to a standard deployment.

Reference: Privacy Policy

HIPA-13 N/A

Does your application automatically lock or log-out an account after a period of inactivity?

Aletheia is not designed to process protected health information and is not a HIPAA-covered platform (see REQU-05); user documents are processed on-device. This question does not apply to a standard deployment.

Reference: Privacy Policy

HIPA-14 NO

Are passwords visible in plain text, whether when stored or entered, including service level accounts (i.e., database accounts, etc.)?

Aletheia stores no passwords in plaintext (or at all); authentication is OAuth-only.

Reference: Security Whitepaper

HIPA-15 N/A

If the application is institution-hosted, can all service level and administrative account passwords be changed by the institution?

Aletheia is not designed to process protected health information and is not a HIPAA-covered platform (see REQU-05); user documents are processed on-device. This question does not apply to a standard deployment.

Reference: Privacy Policy

HIPA-16 N/A

Does your application provide the ability to define user access levels?

Aletheia is not designed to process protected health information and is not a HIPAA-covered platform (see REQU-05); user documents are processed on-device. This question does not apply to a standard deployment.

Reference: Privacy Policy

HIPA-17 N/A

Does your application support varying levels of access to administrative tasks defined individually per user?

Aletheia is not designed to process protected health information and is not a HIPAA-covered platform (see REQU-05); user documents are processed on-device. This question does not apply to a standard deployment.

Reference: Privacy Policy

HIPA-18 N/A

Does your application support varying levels of access to records based on user ID?

Aletheia is not designed to process protected health information and is not a HIPAA-covered platform (see REQU-05); user documents are processed on-device. This question does not apply to a standard deployment.

Reference: Privacy Policy

HIPA-19 N/A

Is there a limit to the number of groups to which a user can be assigned?

Aletheia is not designed to process protected health information and is not a HIPAA-covered platform (see REQU-05); user documents are processed on-device. This question does not apply to a standard deployment.

Reference: Privacy Policy

HIPA-20 N/A

Do accounts used for solution provider-supplied remote support abide by the same authentication policies and access logging as the rest of the system?

Aletheia is not designed to process protected health information and is not a HIPAA-covered platform (see REQU-05); user documents are processed on-device. This question does not apply to a standard deployment.

Reference: Privacy Policy

HIPA-21 N/A

Does the application log record access including specific user, date/time of access, and originating IP or device?

Aletheia is not designed to process protected health information and is not a HIPAA-covered platform (see REQU-05); user documents are processed on-device. This question does not apply to a standard deployment.

Reference: Privacy Policy

HIPA-22 N/A

Does the application log administrative activity, such as user account access changes and password changes, including specific user, date/time of changes, and originating IP or device?

Aletheia is not designed to process protected health information and is not a HIPAA-covered platform (see REQU-05); user documents are processed on-device. This question does not apply to a standard deployment.

Reference: Privacy Policy

HIPA-23 N/A

Do you retain logs for at least as long as required by HIPAA regulations?

Aletheia is not designed to process protected health information and is not a HIPAA-covered platform (see REQU-05); user documents are processed on-device. This question does not apply to a standard deployment.

Reference: Privacy Policy

HIPA-24 N/A

Can the application logs be archived?

Aletheia is not designed to process protected health information and is not a HIPAA-covered platform (see REQU-05); user documents are processed on-device. This question does not apply to a standard deployment.

Reference: Privacy Policy

HIPA-25 N/A

Can the application logs be saved externally?

Aletheia is not designed to process protected health information and is not a HIPAA-covered platform (see REQU-05); user documents are processed on-device. This question does not apply to a standard deployment.

Reference: Privacy Policy

HIPA-26 N/A

Do you have a disaster recovery plan and emergency mode operation plan?

Aletheia is not designed to process protected health information and is not a HIPAA-covered platform (see REQU-05); user documents are processed on-device. This question does not apply to a standard deployment.

Reference: Privacy Policy

HIPA-27 NO

Can you provide a HIPAA compliance attestation document?

Aletheia does not provide a HIPAA compliance attestation and is not HIPAA certified.

Reference: Privacy Policy

HIPA-28 ROADMAP

Are you willing to enter into a Business Associate Agreement (BAA)?

A Business Associate Agreement can be provided on request for a healthcare Enterprise deployment (template prepared on demand). Aletheia is not HIPAA certified and does not claim HIPAA compliance.

Reference: Privacy Policy

HIPA-29 N/A

Do your data backup and retention policies and practices meet HIPAA requirements?

Aletheia is not designed to process protected health information and is not a HIPAA-covered platform (see REQU-05); user documents are processed on-device. This question does not apply to a standard deployment.

Reference: Privacy Policy

PCID-01 N/A

Do you have a current, executed within the past year, Attestation of Compliance (AoC) or Report on Compliance (RoC)?*

Aletheia is out of PCI DSS scope because it never handles cardholder data; Stripe (a PCI DSS Level 1 service provider) processes all payments and maintains its own AoC.

Reference: Sub-processors

PCID-02 N/A

Is the application listed as an approved Payment Application Data Security Standard (PA-DSS) application?*

Aletheia is not a payment application; card data is handled entirely by Stripe.

Reference: Sub-processors

PCID-03 YES

Does the system or solutions use a third party to collect, store, process, or transmit cardholder (payment/credit/debt card) data?*

Stripe, a PCI DSS Level 1 service provider, collects, stores, processes, and transmits all payment card and ACH data. Lonia never receives full card or bank account numbers.

Reference: Sub-processors

PCID-04 NO

Do your systems or solutions store, process, or transmit cardholder (payment/credit/debt card) data?

Aletheia's own systems do not store, process, or transmit cardholder data.

Reference: Sub-processors

PCID-05 COMPENSATING CONTROL

Are you compliant with the Payment Card Industry Data Security Standard (PCI DSS)?

Aletheia is SAQ-A eligible: it never touches cardholder data, and Stripe maintains PCI DSS compliance for payment processing.

Reference: Sub-processors

PCID-06 N/A

Are you classified as a service provider?

Aletheia is not a payment service provider; it is a merchant using Stripe.

Reference: Sub-processors

PCID-07 N/A

Are you on the list of Visa approved service providers?

Aletheia is not a payment service provider and is not on Visa's service-provider list; Stripe is the payment processor.

Reference: Sub-processors

PCID-08 COMPENSATING CONTROL

Are you classified as a merchant? If so, what level (1, 2, 3, 4)?

Lonia is a merchant using Stripe with card data fully outsourced, making it SAQ-A eligible.

Reference: Sub-processors

PCID-09

Describe the architecture employed by the system to verify and authorize credit card transactions.

Response: Payment authorization is handled entirely by Stripe (Checkout / Elements). Card data is submitted by the user's browser directly to Stripe and never transits Lonia systems.

Reference: Sub-processors

PCID-10

What payment processors/gateways does the system support?

Response: Stripe.

Reference: Sub-processors

PCID-11 N/A

Can the application be installed in a PCI DSS-compliant manner?

Aletheia is a SaaS with no institution-side installation; PCI scope is limited to Stripe.

Reference: Sub-processors

PCID-12

Include documentation describing the system's abilities to comply with the PCI DSS and any features or capabilities of the system that must be added or changed in order to operate in compliance with the standards.

Response: Aletheia stays out of PCI DSS scope by fully outsourcing payment handling to Stripe (SAQ-A). No configuration change is needed for an institution to remain out of cardholder-data scope.

Reference: Sub-processors

OPEM-01 YES

Do you support role-based access control (RBAC) for system administrators?

Role-based access control governs administrator access; roles are least-privilege.

Reference: Security Whitepaper

OPEM-02 NO

Can your employees access customer systems remotely?

Lonia employees do not have remote access into customer systems; Aletheia is a browser-based SaaS.

OPEM-03 YES

Can you provide overall system and/or application architecture diagrams including a full description of the data communications architecture for all components of the system?

Architecture and data-flow are described in the Security Whitepaper.

Reference: Security Whitepaper

OPEM-04 NO

Do you require remote management of the system?

Aletheia requires no remote management of any institution-side system; there is none.

OPEM-05 N/A

If you answered "yes" to OPEM-04, are your remote actions and changes logged or otherwise visible to the campus?

Not applicable: Aletheia performs no remote management of institution systems.

OPEM-06 N/A

If you maintain remote access to the system, will you handle data in a FERPA-compliant manner?

Aletheia has no remote access to institution systems. FERPA data segmentation applies to the platform itself (per-institution scoping, two-gate audited access to individual student data).

Reference: Security Whitepaper

OPEM-07 N/A

Do you support campus status monitoring through SNMPv3 or other means?

There is no on-premises appliance to monitor via SNMP; Aletheia is a browser-based SaaS.

OPEM-08

Describe or provide a reference to any other safeguards used to monitor for malicious activity.

Response: Malicious-activity monitoring is provided by Cloudflare and Supabase at the platform layer, complemented by Aletheia's append-only (WORM) audit logs for privileged actions.

Reference: Security Whitepaper

OPEM-09

Describe how long your organization has conducted business in this area.

Response: Provided on request

Lonia AI operates Aletheia in active production. Company operating history is provided to institutional buyers on request.

OPEM-10

Do you have existing higher education customers?

Response: See details

Aletheia is newly available to higher-education institutions. Contact enterprise@lonia.ai to discuss a pilot deployment.

7. Artificial Intelligence (32 questions)

AIQU-01 YES

Does your solution leverage machine learning (ML) or do you plan to do so in the next 12 months?

Aletheia uses machine learning for accessibility: an on-device vision-language model (base tier) generates image descriptions locally on the user's device.

Reference: Security Whitepaper

AIQU-02 YES

Does your solution leverage a large language model (LLM) or do you plan to do so in the next 12 months?

Aletheia can call a large language model through the customer's own commercial provider via bring-your-own-key. On Professional the call is browser-direct; on Enterprise the institution's key is held server-side by Lonia's Enterprise Worker, which calls the provider on the institution's behalf.

Reference: Security Whitepaper

AIGN-01 COMPENSATING CONTROL

Does your solution have an AI risk model when developing or implementing your solution's AI model?*

AI design follows practices aligned with the NIST AI Risk Management Framework: on-device processing by default, no training on user data, human-in-the-loop output, and per-user opt-out. Formal AI-risk documentation is maturing, and an EU AI Act Article 50 transparency statement is planned (deadline 2 December 2026).

Reference: Security Whitepaper

AIGN-02 YES

Can your solution's AI features be disabled by tenant and/or user?*

AI features can be disabled per user: the base tier can run without any cloud AI, and cloud AI is inactive unless the user supplies their own BYOK key.

Reference: Security Whitepaper

AIGN-03 ROADMAP

Have your staff completed responsible AI training?*

Formal, tracked responsible-AI training is being established as the team grows; the AI design principles (no training on user data, human-in-the-loop) are already applied.

AIGN-04

Please describe the capabilities of your solution's AI features.

Response: Aletheia's AI generates image descriptions and alternative text, restructures documents for readability, labels forms, and simplifies content for accessibility. The base tier uses an on-device vision-language model; Professional and Enterprise can use the customer's own commercial LLM via BYOK (browser-direct on Professional, institution-managed server-side via Lonia's Enterprise Worker on Enterprise). AI output is always presented to the user for review; Aletheia takes no autonomous actions.

Reference: Security Whitepaper

AIGN-05 YES

Does your solution support business rules to protect sensitive data from being ingested by the AI model?

On-device processing keeps content local by default, and architectural PII detection warns the user before sensitive content is sent to a cloud provider. On BYOK, only what the user chooses is sent: browser-direct to the user's own provider on Professional, or via Lonia's Enterprise Worker to the institution-selected provider on Enterprise.

Reference: Privacy Policy

AIPL-01 ROADMAP

Are your AI developer's policies, processes, procedures, and practices across the organization related to the mapping, measuring, and managing of AI risks conspicuously posted, unambiguous, and implemented effectively?*

A public AI transparency statement (aligned with EU AI Act Article 50, planned by 2 December 2026) will document AI practices. Current practices (on-device default, no training on user data, human-in-the-loop) are applied today.

AIPL-02 COMPENSATING CONTROL

Have you identified and measured AI risks?*

Key AI risks are addressed by design decisions: on-device default, no training on or retention of user data, and mandatory human review of output. Formal, documented risk measurement is maturing.

Reference: Security Whitepaper

AIPL-03 YES

In the event of an incident, can your solution's AI features be disabled in a timely manner?*

AI features can be disabled quickly: the on-device path can be turned off, and BYOK cloud AI is user-controlled and can be disconnected immediately.

AIPL-04 YES

If disabled because of an incident, can your solution's AI features be re-enabled in a timely manner?*

AI features can be re-enabled promptly once an incident is resolved.

AIPL-05 COMPENSATING CONTROL

Do you have documented technical and procedural processes to address potential negative impacts of AI as described by the AI Risk Management Framework (RMF)?

Documented technical safeguards (on-device default, human-in-the-loop, opt-out, no training on user data) address the negative-impact concerns in the NIST AI RMF. Formal procedural documentation is maturing.

Reference: Security Whitepaper

AISC-01 COMPENSATING CONTROL

If sensitive data is introduced to your solution's AI model, can the data be removed from the AI model by request?*

No user data is incorporated into any Aletheia model, so there is nothing embedded to remove. On-device inference is transient; BYOK content is governed by the user's own provider contract.

Reference: Security Whitepaper

AISC-02 NO

Is user input data used to influence your solution's AI model?*

User input is not used to train or influence Aletheia's models. The on-device model is pre-trained and static; BYOK calls go to the user's provider under the user's own terms.

Reference: Security Whitepaper

AISC-03 COMPENSATING CONTROL

Do you provide logging for your solution's AI feature(s) that includes user, date, and action taken?*

On-device AI runs locally and is not transmitted or server-logged by design (data minimization). Privileged institutional actions are recorded in the append-only audit log.

Reference: Security Whitepaper

AISC-04

Please describe how you validate user inputs.

Response: User inputs are validated and sanitized client-side before processing. Base-tier inference runs on-device, and BYOK content is not executed on Lonia infrastructure: on Professional the call is browser-direct to the user's provider, and on Enterprise the request is relayed by Lonia's Enterprise Worker to the provider without executing untrusted content.

AISC-05 COMPENSATING CONTROL

Do you plan for and mitigate supply-chain risk related to your AI features?

AI supply-chain risk is limited by using a vetted on-device model and, for cloud AI, established commercial providers reached under the user's own contract. Dependencies are managed through the change pipeline.

Reference: Sub-processors

AIML-01 N/A

Do you separate ML training data from your ML solution data?*

Aletheia does not train, fine-tune, or maintain ML training data. The base-tier vision-language model is a pre-trained model run on-device; Professional/Enterprise use the customer's own commercial provider via BYOK.

Reference: Security Whitepaper

AIML-02 N/A

Do you authenticate and verify your ML model's feedback?*

Aletheia runs no training loop, so there is no model feedback to authenticate.

Reference: Security Whitepaper

AIML-03 N/A

Is your ML training data vetted, validated, and verified before training the solution's AI model?

Aletheia maintains no ML training data to vet; it consumes a pre-trained model and, on BYOK, the customer's commercial provider.

Reference: Security Whitepaper

AIML-04 N/A

Is your ML training data monitored and audited?

Aletheia maintains no ML training data to monitor or audit.

Reference: Security Whitepaper

AIML-05 N/A

Have you limited access to your ML training data to only staff with an explicit business need?

Aletheia holds no ML training data, so training-data access controls do not apply.

Reference: Security Whitepaper

AIML-06 N/A

Have you implemented adversarial training or other model defense mechanisms to protect your ML-related features?

Aletheia trains no model, so adversarial training and model-defense of a trained model are the responsibility of the upstream model provider.

Reference: Security Whitepaper

AIML-07 COMPENSATING CONTROL

Do you make your ML model transparent through documentation and log inputs and outputs?

Aletheia trains no model, but the model provenance and behavior are documented. On-device inference is not logged, by design, to preserve privacy.

Reference: Security Whitepaper

AIML-08 N/A

Do you watermark your ML training data?

Aletheia maintains no ML training data to watermark.

Reference: Security Whitepaper

AILM-01 YES

Do you limit your solution's LLM privileges by default?*

The LLM has no autonomous privileges. It returns text and descriptions that are presented to the user; it cannot take actions, call tools, or reach institutional systems.

Reference: Security Whitepaper

AILM-02 N/A

Is your LLM training data vetted, validated, and verified before training the solution's AI model?*

Aletheia does not train or fine-tune an LLM; BYOK uses the customer's commercial provider under the customer's own terms.

Reference: Security Whitepaper

AILM-03 YES

Do any actions taken by your solution's LLM features or plugins require human intervention?*

All AI output is presented to the user for review; the LLM performs no autonomous actions. This is a core design principle.

Reference: Security Whitepaper

AILM-04 COMPENSATING CONTROL

Do you limit multiple LLM model plugins being called as part of a single input?*

Aletheia uses no LLM plugins, tools, or agent chaining, so multiple plugins cannot be invoked from a single input.

Reference: Security Whitepaper

AILM-05 COMPENSATING CONTROL

Do you limit your solution's LLM resource use per request, per step, and per action?

Requests are single-shot and bounded; plan-limit usage counts constrain overall use.

AILM-06 N/A

Do you leverage LLM model tuning or other model validation mechanisms?

Aletheia performs no model tuning; it consumes a pre-trained on-device model and, on BYOK, the customer's provider models.

Reference: Security Whitepaper

AILM-07 N/A

Do you perform taint tracing or tracking on all plugin content related to the LLM?

Aletheia uses no LLM plugins, so plugin-content taint tracing does not apply.

Reference: Security Whitepaper

8. Privacy (65 questions)

PRGN-01 YES

Does your solution process FERPA-related data?

On the Campus tier, Aletheia processes limited student-associated account data. FERPA data segmentation is built in: per-institution scoping (institution_id), a K-12/higher-ed discriminator, per-institution retention, and two-gate, audit-logged access for any individual student visibility.

Reference: Security Whitepaper

PRGN-02 YES

Does your solution process GDPR-related or PIPL-related data?

EU institutions may use Aletheia. A Data Processing Agreement with Standard Contractual Clauses is available. Data is stored in the US region (not the EEA); see INTL.

Reference: DPA

PRGN-03 YES

Does your solution process personal data regulated by state law(s) (e.g., CCPA)?

Aletheia processes personal data subject to US state laws such as the CCPA; the privacy policy covers these rights.

Reference: Privacy Policy

PRGN-04 YES

Does your solution process user-provided data that may contain regulated information?

User-submitted documents may contain regulated information. Aletheia processes them on-device, includes PII detection to warn users, and does not store documents on Lonia infrastructure.

Reference: Privacy Policy

PRGN-05

Web Link to Product/Service Privacy Notice

Response: https://aletheia.lonia.ai/privacy

Aletheia privacy policy.

Reference: Privacy Policy

PCOM-01 NO

Have you had a personal data breach in the past three years that involved reporting to a governmental agency, notice to individuals (including voluntary notice), or notice to another organization or institution?*

Aletheia has had no reportable personal-data breach in the past three years.

PCOM-02

Use this area to share information about your privacy practices that will assist those who are assessing your company data privacy program.*

Response: Aletheia's privacy program centers on data minimization: documents are processed on-device, only account identity, plan/billing status, and usage counts leave the device, there are no third-party trackers, user data is not sold, and user data is not used to train Aletheia's AI models.

Reference: Privacy Policy

PCOM-03 NO

Have you had any violations of your internal privacy policies or violations of applicable privacy law in the past 36 months?

Aletheia has had no known violations of its privacy policy or applicable privacy law in the past 36 months.

PCOM-04 COMPENSATING CONTROL

Do you have a dedicated data privacy staff or office?

Privacy is owned by a designated privacy contact (privacy@lonia.ai, with legal@lonia.ai for legal matters) rather than a separate privacy office, and privacy-by-design is built into the architecture.

Reference: Privacy Policy

PDOC-01 N/A

If you have completed a SOC 2 audit, does it include the Privacy Trust Service Principle?

Aletheia has not completed a SOC 2 audit, so the Privacy Trust Services Principle does not apply.

PDOC-02 COMPENSATING CONTROL

Do you conform with a specific industry-standard privacy framework (e.g., NIST Privacy Framework, GDPR, ISO 27701)?

Aletheia applies privacy-by-design and is GDPR-aligned (DPA with SCCs available). It holds no ISO 27701 or equivalent privacy certification.

Reference: DPA

PDOC-03 COMPENSATING CONTROL

Does your employee onboarding and offboarding policy include training of employees on information security and data privacy?

Security and privacy responsibilities are communicated to team members; a formally documented training component within onboarding/offboarding is maturing.

PTHP-01 YES

Do you have contractual agreements with third parties that require them to maintain standards and to comply with all regulatory requirements?*

Sub-processor contracts (DPAs, with SCCs where relevant) require them to maintain appropriate standards and meet regulatory requirements.

Reference: Sub-processors

PTHP-02 COMPENSATING CONTROL

Do you perform privacy impact assessments of third parties that collect, process, or have access to personal data to ensure they meet industry and regulatory standards and to mitigate harmful, unethical, or discriminatory impacts on data subjects?

Sub-processors are established providers with published security and privacy programs and executed DPAs. A formally documented third-party privacy impact assessment process is maturing.

Reference: Sub-processors

PCHG-01 COMPENSATING CONTROL

Does your change management process include privacy review and approval?

Changes affecting personal data are reviewed against privacy-by-design before release; a formally documented privacy sign-off step is maturing.

PCHG-02 COMPENSATING CONTROL

Do you have policy and procedure, currently implemented, guiding how privacy risks are mitigated until they can be resolved?

Where a privacy risk cannot be resolved immediately, exposure is reduced through the minimal data footprint and on-device processing. A documented interim-mitigation procedure is maturing.

PDAT-01 NO

Do you collect, process, or store demographic information?*

Aletheia does not collect, process, or store demographic information.

Reference: Privacy Policy

PDAT-02 NO

Do you capture or create genetic, biometric, or behaviometric information (e.g., facial recognition or fingerprints)?*

Aletheia does not capture or create genetic, biometric, or behaviometric information. There is no facial recognition or fingerprinting. (The on-device model describes images the user chooses to submit; that is user content processed locally, not biometric capture by Aletheia.)

Reference: Privacy Policy

PDAT-03 NO

Do you combine institutional data (including "de-identified," "anonymized," or otherwise masked data) with personal data from any other sources?*

Aletheia does not combine institutional data with personal data from other sources.

Reference: Privacy Policy

PDAT-04 NO

Is institutional data coming into or going out of the United States at any point during collection, processing, storage, or archiving?

Institutional account data is stored in the US region and is not routed outside the United States by Aletheia. (On BYOK, the user's own provider call goes wherever the user's chosen provider operates, under the user's own contract.)

Reference: Sub-processors

PDAT-05 COMPENSATING CONTROL

Do you capture device information (e.g., IP address, MAC address)?

Network-level IP is processed transiently at the Cloudflare edge for routing and abuse prevention. Aletheia does not capture MAC addresses or build device fingerprints, and uses no third-party trackers.

Reference: Cookies

PDAT-06 NO

Does any part of this service/project involve a web/app tracking component (e.g., use of web-tracking pixels, cookies)?

Aletheia uses no third-party analytics, tracking pixels, session replay, or advertising cookies.

Reference: Cookies

PDAT-07 NO

Does your staff (or a third party) have access to institutional data (e.g., financial, PHI, or other sensitive information) through any means?

Staff do not access institutional user documents (processed on-device). Access to limited account data is least-privilege and audit-logged.

Reference: Security Whitepaper

PDAT-08 YES

Will you handle personal data in a manner compliant with all relevant laws, regulations, and applicable institution policies?

Aletheia commits to handling personal data in compliance with applicable laws, regulations, and institutional policies.

Reference: Privacy Policy

PRPO-01 YES

Do you have a documented privacy management process?

Privacy commitments are documented in the privacy policy and the DPA, and privacy-by-design governs the architecture.

Reference: Privacy Policy

PRPO-02 YES

Are privacy principles designed into the product lifecycle (i.e., privacy-by-design)?

Privacy-by-design is core: on-device processing, data minimization, and no third-party trackers.

Reference: Privacy Policy

PRPO-03 YES

Will you comply with applicable breach notification laws?

Aletheia commits to applicable breach-notification laws (DPA, 72 hours).

Reference: DPA

PRPO-04 YES

Will you comply with the institution's policies regarding user privacy and data protection?

Aletheia complies with the institution's user-privacy and data-protection policies.

Reference: Privacy Policy

PRPO-05 YES

Is your company subject to the laws and regulations of the institution's geographic region?

Aletheia is subject to the applicable laws and regulations of the institution's region for the services it provides.

Reference: DPA

PRPO-06 ROADMAP

Do you have a privacy awareness/training program?*

A formal, tracked privacy-awareness program is being established; privacy-by-design principles are applied today.

PRPO-07 ROADMAP

Is privacy awareness training mandatory for all employees?

Mandatory, tracked privacy training is being formalized as the team grows.

PRPO-08 ROADMAP

Is AI privacy and ethics awareness/training required for all employees who work with AI?

Dedicated AI privacy-and-ethics training for AI staff is being formalized; the applied AI principles (no training on user data, human-in-the-loop) already reflect these values.

PRPO-09 NO

Do you have any decision-making processes that are completely automated (i.e., there is no human involvement)?

Aletheia makes no fully automated decisions about individuals. AI output is always presented to the user for review.

Reference: Security Whitepaper

PRPO-10 COMPENSATING CONTROL

Do you have a documented process for managing automated processing, including validations, monitoring, and data subject requests?

AI is assistive, not decisional, so automated-decision governance is limited in scope; the privacy policy and DPA cover data-subject requests. Documentation is maturing alongside the AI transparency statement.

Reference: DPA

PRPO-11 COMPENSATING CONTROL

Do you have a documented policy for sharing information with law enforcement?

Aletheia holds minimal data and discloses only under valid legal process. A formally documented law-enforcement request policy is maturing.

Reference: Privacy Policy

PRPO-12 NO

Do you share any institutional data with law enforcement without a valid warrant or subpoena?*

Aletheia does not share institutional data with law enforcement without a valid warrant or subpoena.

Reference: Privacy Policy

PRPO-13 COMPENSATING CONTROL

Does your incident response team include a privacy analyst/officer?

The designated privacy contact participates in incident handling. A separately staffed privacy-analyst role is planned as the team grows.

INTL-01 NO

Will data be collected from or processed in or stored in the European Economic Area (EEA)?

Data is collected, processed, and stored in a single US region, not the EEA.

Reference: Sub-processors

INTL-02 COMPENSATING CONTROL

Do you have a data protection officer (DPO)?

Privacy is owned by a designated privacy contact (privacy@lonia.ai). A formally appointed GDPR Article 37 Data Protection Officer is not currently mandated at Aletheia's scale; one will be appointed if the criteria are triggered.

Reference: Privacy Policy

INTL-03 YES

Will you sign appropriate GDPR Standard Contractual Clauses (SCCs) with the institution?

Aletheia will sign GDPR Standard Contractual Clauses; they are incorporated in the DPA (Annex D).

Reference: DPA

INTL-04 NO

Will data be collected from or processed in or stored in China?

Data is not collected, processed, or stored in China.

Reference: Sub-processors

INTL-05 N/A

Do you comply with PIPL security, privacy, and data localization requirements?

Aletheia does not target China or store data there, so PIPL localization requirements do not apply. This would be reassessed if a China deployment were contemplated.

DRPV-01 COMPENSATING CONTROL

Have you performed a Data Privacy Impact Assessment for the solution/project?

Privacy-by-design and a minimal data footprint reduce privacy risk; the DPA documents processing details. A formally documented Data Privacy Impact Assessment is maturing and available to institutions on request.

Reference: DPA

DRPV-02 YES

Do you provide an end-user privacy notice about privacy policies and procedures that identify the purpose(s) for which personal information is collected, used, retained, and disclosed?

Aletheia provides an end-user privacy notice describing why personal information is collected, used, retained, and disclosed.

Reference: Privacy Policy

DRPV-03 YES

Do you describe the choices available to the individual and obtain implicit or explicit consent with respect to the collection, use, and disclosure of personal information?

The privacy policy describes user choices and the consent basis for collection, use, and disclosure.

Reference: Privacy Policy

DRPV-04 YES

Do you collect personal information only for the purpose(s) identified in the agreement with an institution or, if there is none, the purpose(s) identified in the privacy notice?

Personal information is collected only for the purposes identified in the agreement or the privacy notice.

Reference: Privacy Policy

DRPV-05 YES

Do you have a documented list of personal data your service maintains?

Data categories are enumerated in the privacy policy, the Sub-processor list, and DPA Annex A.

Reference: Privacy Policy

DRPV-06 YES

Do you retain personal information for only as long as necessary to fulfill the stated purpose(s) or as required by law or regulation and thereafter appropriately dispose of such information?

Personal information is retained only as long as necessary; per-institution retention defaults to 365 days with scheduled deletion.

Reference: Security Whitepaper

DRPV-07 YES

Do you provide individuals with access to their personal information for review and update (i.e., data subject rights)?

Individuals can access and update their personal information; data-subject rights are supported through the DPA and privacy policy.

Reference: DPA

DRPV-08 YES

Do you disclose personal information to third parties only for the purpose(s) identified in the privacy notice or with the implicit or explicit consent of the individual?

Personal information is disclosed to third parties only for the purposes in the privacy notice or with consent.

Reference: Privacy Policy

DRPV-09 YES

Do you protect personal information against unauthorized access (both physical and logical)?

Personal information is protected against unauthorized access through OAuth-only identity, RLS on every table, and encryption at rest and in transit.

Reference: Security Whitepaper

DRPV-10 YES

Do you maintain accurate, complete, and relevant personal information for the purposes identified in the privacy notice?

Account identity is refreshed from the institution's identity provider, keeping it accurate and current.

DRPV-11 YES

Do you have procedures to address privacy-related noncompliance complaints and disputes?

Privacy complaints and disputes can be raised with privacy@lonia.ai and are handled through a documented response path.

Reference: Privacy Policy

DRPV-12 YES

Do you "anonymize," "de-identify," or otherwise mask personal data?

Institutional reporting is aggregate-only by default; individual student visibility requires the two-gate, audit-logged FERPA-privileged path.

Reference: Security Whitepaper

DRPV-13 NO

Do you or your subprocessors use or disclose "anonymized," "de-identified," or otherwise masked data for any purpose other than those identified in the agreement with an institution (e.g., sharing with ad networks or data brokers, marketing, creation of profiles, analytics unrelated to services provided to institution)?

Aletheia does not use or disclose de-identified or masked data for advertising, data brokerage, marketing, profiling, or unrelated analytics. User data is not sold.

Reference: Privacy Policy

DRPV-14 YES

Do you certify stop-processing requests, including any data that is processed by a third party on your behalf?

Stop-processing requests are honored, including for data processed by sub-processors on Aletheia's behalf.

Reference: DPA

DRPV-15 COMPENSATING CONTROL

Do you have a process to review code for ethical considerations?

Code review considers accessibility and privacy impact as part of the development process; a separately documented ethics-review checklist is maturing.

DPAI-01 NO

Does your service use AI for the processing of institutional data?

Aletheia does not apply AI to institutional account data. AI processes the user's own document content that the user submits, on-device or via the user's BYOK provider; it does not process institutional records, rosters, or admin data.

Reference: Security Whitepaper

DPAI-02 NO

Is any institutional data retained in AI processing?*

No institutional data is retained in AI processing. On-device inference is transient and local; BYOK calls are governed by the user's provider contract and are not retained by Lonia.

Reference: Security Whitepaper

DPAI-03 YES

Do you have agreements in place with third parties or subprocessors regarding the protection of customer data and use of AI?*

Data-flow sub-processors are covered by DPAs. On Professional BYOK, the AI provider is reached under the user's own contract and is not a Lonia sub-processor. On Enterprise BYOK, the institution-selected provider is invoked by Lonia's Enterprise Worker and is engaged as a Lonia sub-processor for that path; see /legal/subprocessors.

Reference: Sub-processors

DPAI-04 NO

Will institutional data be processed through a third party or subprocessor that also uses AI?

Institutional data is not processed through a sub-processor that applies AI to it.

Reference: Sub-processors

DPAI-05 YES

Is AI processing limited to fully licensed commercial enterprise AI services?

Cloud AI is limited to licensed commercial providers reached via the user's BYOK key; the base tier uses a licensed on-device model.

Reference: Security Whitepaper

DPAI-06 NO

Will institutional data be used or processed by any shared AI services?

Institutional data is not used or processed by shared AI services.

Reference: Security Whitepaper

DPAI-07 YES

Do you have safeguards in place to protect institutional data and data privacy from unintended AI queries or processing?

On-device processing by default, PII detection, and user control over what is sent protect institutional data from unintended AI processing.

Reference: Privacy Policy

DPAI-08 YES

Do you provide choice to the user to opt out of AI use?

Users can opt out of cloud AI: the base tier runs on-device without any cloud AI, and BYOK cloud AI is inactive unless the user connects a key.

Reference: Security Whitepaper

Review cadence

Last review date: July 17, 2026. Next review: Annually or on material change, whichever comes first. This response is regenerated from a single source of truth, so the online page, the PDF, and the XLSX are always in step.

Question text is from the official EDUCAUSE HECVAT 4.1.6 workbook (hecvat416.xlsx), the current published version, downloaded from educause.edu. Punctuation normalized to ASCII; wording unchanged.

Related documents

- Security whitepaper (tagged PDF)
- Data Processing Agreement (DPA) template (tagged PDF)
- Sub-processor list
- VPAT accessibility report (tagged PDF)
- European Accessibility Act (EAA) conformance statement
- EN 301 549 conformance mapping
- Privacy policy
- Cookies and tracking statement