LONIA AI / PALLAS

HECVAT-Full 4.1.6 Solution Provider Response

The Higher Education Community Vendor Assessment Toolkit, completed for Pallas by Lonia AI

A completed HECVAT-Full 4.1.6, the higher education sector's standard vendor security and privacy questionnaire. Every one of the 331 answerable questions carries a response drawn from the Pallas control inventory, and every gap is stated in the inventory's own disclosure wording rather than softened. Published as a PDF for reading and as a workbook in the official template for a reviewer's own tooling.

Version. 4.1.6. Published 2026-08-30 by Lonia AI.

Jurisdictions addressed. Used by higher education institutions in the United States, Canada, the United Kingdom, Ireland, Australia, and New Zealand. The questionnaire is sector-specific rather than jurisdiction-specific, and Pallas answers it identically for every institution.

Every control claim in this document is rendered from the Pallas control inventory at src/data/control-inventory.ts, with its status, its evidence basis, and its disclosure text unaltered. Appendix A lists every control cited.

This render is informational; signable version issued on request. Request one at support@lonia.ai, giving your legal entity name and the jurisdiction of your establishment.

Contents

1. What this document is

This is a completed HECVAT-Full, version 4.1.6. The HECVAT is the questionnaire higher education institutions send to a vendor before buying from it, and the reason it exists is that every institution used to send its own. A completed HECVAT means a reviewer reads the same questions in the same order with the same identifiers as every other vendor they are assessing, instead of reading whatever a vendor chose to volunteer.

Pallas by Lonia AI is the solution provider. Pallas is a hosted web accessibility testing and compliance reporting service: it evaluates web pages against the WCAG 2.2 success criteria using the axe-core rule engine, records findings per organisation, and generates accessibility reports and conformance documentation.

The questionnaire has fifteen worksheets. Seven of them ask the vendor questions, and those seven carry every response in this document: Organization, Product, Infrastructure, IT Accessibility, Case-Specific, AI, and Privacy, plus the START HERE worksheet that scopes which of the others apply. The remaining worksheets belong to the reviewing institution and are not ours to fill in.

2. Where the answers come from

Every answer in this document is generated from `src/data/control-inventory.ts` in the Pallas marketing repository. That file is the single source of truth for every control Pallas claims to a buyer, and the same file generates the security whitepaper, the Data Processing Agreement, the Data Protection Impact Assessment, the Transfer Impact Assessment, the Standard Contractual Clauses, and the institutional terms of service.

This matters for a reason that is worth stating plainly. A questionnaire answered by hand drifts: the person filling it in remembers a control being stronger than it is, or copies last year's answer, or rounds a partial control up to a yes because the form has no box for partial. Generating the answers from the inventory does not make them true, but it does make them consistent with every other document Pallas publishes, and it makes drift detectable. A build gate fails the release if this document no longer matches the inventory it was generated from.

Each response names the inventory rows it rests on. A reviewer who wants to know what is behind an answer can look the row up and find the migration, function, Worker, source file, test, build gate, or vendor attestation that supports it, together with an honest statement of how strong that evidence is.

3. How to read a No

Pallas is a small operation. A meaningful number of answers in this document are No, and they are not buried.

Where the answer is No, the detail says what is missing in the control inventory's own disclosure wording, unaltered. It does not offer a substitute control in place of the missing one and hope the reader does not notice the swap. Where a different control genuinely reduces the same risk, the detail says so and also says that it is not equivalent.

The largest concentrations of No are the ones a reviewer should expect from an operation this size, and they

are stated once here so they are not a surprise on page forty:

- **No independent assurance.** No SOC 2 report, no ISO 27001 certification, no independent penetration test, and no third-party accessibility audit. No date for an independent test is promised.
- **No formalised personnel programme.** No background screening, no security or privacy awareness training, no onboarding and offboarding policy.
- **No operated perimeter.** Pallas runs no firewall, no intrusion detection or prevention system, no host-based agent, and no 24 by 7 monitoring, because it operates no hosts and no network. Edge filtering and DDoS mitigation are Cloudflare functions.
- **No tested continuity plan.** No business continuity plan or disaster recovery plan that is owned and exercised annually, no published recovery time or recovery point objective, and no documented restore test.
- **No cyber liability certificate published.**

Every one of those is inventoried as a gap with its own row, and every one of them was already published on the Pallas trust page before this questionnaire was completed. Nothing here is a disclosure made only because a form asked.

4. How to read a Yes that rests on a subprocessor

Pallas operates no data centre, no server, and no network. Every system that holds institutional data is operated by Supabase or Cloudflare.

That means a set of questions on the Infrastructure worksheet, particularly the sixteen about data centre staffing, cages, barriers, power, cooling, fire suppression, and carrier diversity, are answered Yes on the strength of a provider control rather than a Pallas control. Every one of those answers says so in its detail and names the provider.

The distinction is load-bearing and it is the single most consequential misreading available in this document. A Supabase or Cloudflare SOC 2 report covers that provider's infrastructure. It does not cover the Pallas application built on top of it, and Pallas holds no certification of its own. A reviewer who needs evidence of a physical control should read the provider's audit report; a Pallas assertion about a provider's facility is not evidence of anything.

5. Compensating controls, and why the workbook does not say so

HECVAT 4.1.6 permits three answers in its response dropdowns: Yes, No, and, for a minority of questions, N/A. Most questions permit only Yes and No. There is no Compensating Control option, and the workbook's scoring formulas compare the answer cell against those exact values.

Pallas therefore does not write "Compensating Control" into the workbook. Writing it would fail the template's own data validation and would break the scoring on the institution's evaluation worksheets, which is a worse outcome than the loss of nuance. Twenty-four responses in this document are classified internally as compensating controls, meaning the answer is honest but a different control is doing the work than the question assumes. In the workbook those appear as the Yes or No the template permits, with the full explanation in the Additional Information column beside them. In this PDF they are labelled explicitly.

6. Sections marked not applicable

Ninety-one of the 331 questions are not applicable to Pallas, and they are made so by the questionnaire's own mechanism rather than by our assertion. The START HERE worksheet carries eight scoping questions, and answering them scopes the rest of the document:

- **Consulting Services**, 9 questions. Not applicable: Pallas is a product, not a consulting engagement.
- **HIPAA**, 29 questions. Not applicable: Pallas processes no protected health information, is not a business associate, and will not execute a business associate agreement.
- **PCI**, 12 questions. Not applicable: no cardholder data reaches Pallas systems. Payment is handled by Stripe, which collects card details directly.
- **On-premises**, 10 questions. Not applicable: Pallas requires no appliance in the institution's environment and no inbound firewall exception.
- **AI**, 31 questions, the entire AI worksheet. Not applicable: Pallas performs no artificial intelligence or machine learning processing. Accessibility findings are produced by deterministic rule evaluation in axe-core, and no model runtime, inference client, or AI provider SDK is present in either Pallas repository.

In the workbook those answer cells are left blank, which is how the template itself expresses non-applicability: the guidance column populates automatically from the START HERE answer and states the reason. The Additional Information column beside each one carries the reason in full as well, so a reviewer reading a printed copy does not have to recalculate a spreadsheet to find out why a cell is empty.

The AI worksheet deserves a specific note because it is new in 4.1.6 and because a reviewer may be checking specifically for it. Pallas answers it not applicable rather than answering thirty-one questions with N/A, because the template forbids N/A on twenty-eight of them. The claim underneath is inventoried and is demonstrable by inspection of the dependency sets of both Pallas repositories, which is the strongest form the claim takes. It is a statement about what is installed, not a runtime proof that no request ever reaches a third-party model.

7. The version, and where the template came from

The reference workbook is HECVAT-Full 4.1.6, obtained from REN-ISAC, which hosts the HECVAT on behalf of the higher education community. The stored copy is src/data/procurement/reference/hecvat-4.1.6.xlsx, SHA-256 562995980e102f49d7777a0a02bc158194aba2f554d1119e55d5b5ef57c55fcb, and the generator refuses to run if that hash does not match the value recorded in the provenance note stored beside it. A build gate checks the same hash on every release, so the template cannot be swapped or edited under a published response without the release failing.

HECVAT 4 merged what were previously separate Full, Lite, and On-Premise questionnaires into a single instrument, with the scoping questions on the START HERE worksheet doing the work the separate versions used to do. A reviewer who asks for a HECVAT Lite should be given this document: there is no longer a separate Lite questionnaire to complete.

The workbook published alongside this PDF is the official template with the Pallas answers filled in. Question

text, question identifiers, sheet names, column layout, formulas, data validation, and the institution's own evaluation worksheets are untouched. They are not reconstructed faithfully; they are the bytes REN-ISAC published, copied through unchanged, with only the answer and Additional Information cells on the vendor worksheets written to.

8. What this document is not

It is not an audit. Nothing in it has been reviewed by an auditor, an assessor, or counsel. Every answer is the operator's, generated from the operator's own record of the operator's own controls.

It is not a certification. Pallas holds none. Certifications named anywhere in this document belong to Supabase, Cloudflare, Stripe, or Resend, and cover their infrastructure.

It is not a contract. Where an answer describes a commitment rather than an implemented control, it says so. Commitments become binding when they are written into an agreement, and the institutional terms of service, Data Processing Agreement, and Standard Contractual Clauses are published for that purpose.

Questions about anything in this document go to support@lonia.ai.

9. Responses

The responses follow, worksheet by worksheet, in the order the workbook presents them. Each carries its question identifier, the question exactly as the template words it, the response written into the workbook, the classification Pallas assigns it, the detail written into the Additional Information column, and the control inventory rows the answer rests on.

START HERE (22 questions)

GNRL-01

Solution Provider Name

Response: Lonia AI. Classification: Informational.

Lonia AI is the operating identity for all Pallas commitments. The registered legal entity name and jurisdiction are supplied directly to a buyer's procurement team on request and appear in the party block of any executed agreement.

Control inventory: none. This is an identity or contact field and asserts no control.

GNRL-02

Solution Name

Response: Pallas. Classification: Informational.

Pallas by Lonia AI.

Control inventory: none. This is an identity or contact field and asserts no control.

GNRL-03

Solution Description

Response: Pallas is a hosted web accessibility testing and compliance reporting service. It evaluates web pages against the WCAG 2.2 success criteria using the axe-core rule engine, records findings per organisation, and generates accessibility reports and conformance documentation.. Classification: Informational.

Scanning is deterministic rule evaluation over a single page of static HTML. Automated detection covers approximately 17 of the WCAG 2.2 success criteria; the rest require human review and are reported as such rather than silently passed.

Control inventory: scan-single-page-static-only, scan-wcag-coverage.

GNRL-04

Solution Provider Contact Name

Response: Pallas Support. Classification: Informational.

Pallas is supported by a role mailbox rather than a named individual, so that a procurement contact does not go stale when staffing changes.

Control inventory: none. This is an identity or contact field and asserts no control.

GNRL-05

Solution Provider Contact Title

Response: Support and Security Contact. Classification: Informational.

Security and data protection correspondence are both handled at support@lonia.ai.

Control inventory: none. This is an identity or contact field and asserts no control.

GNRL-06

Solution Provider Contact Email

Response: support@lonia.ai. Classification: Informational.

support@lonia.ai for security reports, vulnerability disclosure, data protection, and subprocessor correspondence.

Control inventory: none. This is an identity or contact field and asserts no control.

GNRL-07

Solution Provider Contact Phone Number

Response: Not published. Pallas is supported by email at support@lonia.ai.. Classification: Informational.

No telephone support line is published. The published support response window is 2 to 3 business days, and telephone contact is arranged during Enterprise onboarding where a buyer requires it.

Control inventory: none. This is an identity or contact field and asserts no control.

GNRL-08

Country of Company Headquarters

Response: United States. Classification: Informational.

The default processing location is also the United States: Supabase hosts the database and Storage in us-east-1.

Control inventory: data-location-default-us.

GNRL-09

Employee Work Locations (all)

Response: United States. Classification: Informational.

All personnel work in the United States. There is no offshore development, support, or administration.

Control inventory: data-location-default-us.

COMP-01

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

Response: No. Classification: Gap, disclosed.

Pallas is operated by a small team and does not maintain separate dedicated teams for development, customer support, implementation, or product management. Deployment to Cloudflare Pages and to every Worker is a deliberate manual operator step rather than an automatic consequence of a merge.

Control inventory: personnel-no-formal-screening-program, vuln-deploys-are-manual.

COMP-02

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

Response: Pallas is a product of Lonia AI. Lonia AI is privately held and independently operated, with no outside investors, no parent company exercising control beyond the operator, and no subsidiaries. Lonia AI is the trade name under which the operating company does business; the registered legal entity name and its jurisdiction of formation are provided directly to a buyer's procurement or security team on request, and appear in the party block of any executed agreement.. Classification: Informational.

There is no offshoring and no multinational arrangement. All personnel and all corporate operations are in the United States.

Control inventory: none. This is an identity or contact field and asserts no control.

COMP-03

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

Response: Yes. Classification: Compensating control.

No unplanned disruption to the service has been recorded or disclosed in the past 12 months. This is an operator statement rather than a measured figure: Pallas operates no public status page and publishes no measured availability history, so the statement cannot be independently verified from either repository. The published operating target is 99.9 percent monthly availability, offered on commercially reasonable efforts and not as a contractual service credit.

Control inventory: incident-detection-monitoring.

COMP-04

Do you have a dedicated information security staff or office?

Response: No. Classification: Gap, disclosed.

There is no dedicated information security staff or office. Pallas is operated by a small team, and security work is performed by the operator rather than by a separate function.

Control inventory: personnel-no-formal-screening-program.

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: Pallas runs entirely on managed infrastructure: Supabase for PostgreSQL, Auth, and Storage, and Cloudflare for the edge, Workers, and Pages. It operates no servers, no network, and no physical facility. Authentication is Google and Microsoft OAuth only, with no password storage and no password reset flow anywhere in the product. Row-Level Security is enabled on every application table. Administrative actions append to a SHA-256 hash chain that is append-only at the database level and carries a seven-year retention floor enforced by a CHECK constraint. A single release command runs a type check, the unit suite over the security and validation code, an automated accessibility scan against the built artifact, and a freshness gate that fails closed if any published procurement document has drifted from the control inventory.. Classification: Informational.

The controls above are inventoried individually in src/data/control-inventory.ts, which separates what this repository can demonstrate from what is a statement about the sibling application repository and from what is a subprocessor's assertion. A reviewer should read that distinction as load-bearing.

Control inventory: auth-oauth-only, tenant-rls-every-table, audit-sha256-ledger, audit-seven-year-floor, appsec-release-gate-fails-closed, encryption-in-transit.

REQU-01

Are you offering a cloud-based product?

Response: Yes. Classification: Informational.

Pallas is a cloud-hosted multi-tenant service. Default processing is in the United States.

Control inventory: data-location-default-us.

REQU-02

Does your product or service have an interface?

Response: Yes. Classification: Informational.

Pallas has a browser-based application interface for end users and organisation administrators at app.pallas.lonia.ai.

Control inventory: auth-oauth-only.

REQU-03

Are you providing consulting services?

Response: No. Classification: Informational.

Pallas is a product, not a consulting engagement. This answer marks the entire Consulting Services section of the Case-Specific worksheet not applicable.

Control inventory: data-classes-enumerated.

REQU-04

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

Response: No. Classification: Informational.

Pallas performs no artificial intelligence or machine learning processing, and none is planned within the next 12 months. Accessibility findings are produced by deterministic rule evaluation in axe-core. This answer marks the entire AI worksheet not applicable.

Control inventory: ai-no-model-processing.

REQU-05

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

Response: No. Classification: Informational.

Pallas holds account identity, organisation records, scan findings, generated reports, and transiently uploaded source files. It does not process protected health information or any data covered by HIPAA. This answer marks the entire HIPAA section of the Case-Specific worksheet not applicable.

Control inventory: data-classes-enumerated.

REQU-06

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

Response: No. Classification: Informational.

Pallas neither processes, stores, nor transmits cardholder data. Payment is handled by Stripe, which collects card details directly; no card number, expiry, or verification value reaches Pallas systems. This answer marks the entire PCI section of the Case-Specific worksheet not applicable.

Control inventory: data-classes-enumerated, subprocessors-published-list.

REQU-07

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?

Response: No. Classification: Informational.

Pallas requires no physical or virtual appliance in the institution's environment and requires no inbound firewall exception. It is reached over the public web. This answer marks the entire on-premises section of the Case-Specific worksheet not applicable.

Control inventory: network-perimeter-subprocessor-operated.

REQU-08

Does your solution have access to personal or institutional data?

Response: Yes. Classification: Informational.

Pallas holds account identity for institutional users, organisation records, accessibility findings about institutional web properties, generated reports, and source files uploaded for scanning. The full enumeration is inventoried rather than summarised.

Control inventory: data-classes-enumerated.

Organization (43 questions)

DOCU-01

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

Response: No. Classification: Gap, disclosed.

There is no business continuity plan that is documented, assigned to a named owner, and exercised annually. Continuity rests on the managed platform underneath: Supabase provider backups with point-in-time recovery, and Cloudflare for edge and Pages hosting. A buyer for whom a tested plan is a control requirement should treat this as an open item.

Control inventory: continuity-no-tested-bcp-drp.

DOCU-02

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

Response: No. Classification: Gap, disclosed.

There is no disaster recovery plan that is documented, owned, and exercised annually, and no restore test has been performed. Recoverability of the provider backups is therefore a provider assertion rather than a demonstrated property.

Control inventory: continuity-no-tested-bcp-drp, backup-no-restore-test, backup-no-published-rto-rpo.

DOCU-03

Have you undergone a SSAE 18/SOC 2 audit?

Response: No. Classification: Gap, disclosed.

Pallas has not undergone an SSAE 18 or SOC 2 audit and holds no SOC 2 report. Certifications named on the Pallas subprocessor list belong to those providers and cover their infrastructure, not the Pallas application built on top of it.

Control inventory: vuln-no-independent-certification, subprocessors-certifications-are-theirs.

DOCU-04

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

Response: No. Classification: Gap, disclosed.

Pallas asserts no conformance to NIST CSF, CIS Controls, ISO 27001, or an equivalent security framework, and holds no independent certification against any of them. WCAG 2.2 AA is adopted as a product accessibility floor, which is a different kind of standard and is not offered as a security framework conformance claim.

Control inventory: vuln-no-independent-certification.

DOCU-05

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

Response: Yes. Classification: Implemented.

The published security whitepaper describes system components and the data flow between them, and the published subprocessor list names each provider with its purpose, data categories, and processing location. Both are generated from the control inventory and gated against drift on every release. A written architecture description, component by component (the product repository's ARCHITECTURE.md), is provided to a buyer's security team on request; there is no diagram.

Control inventory: procurement-documentation-published, subprocessors-published-list, data-classes-enumerated.

DOCU-06

Does your organization have a data privacy policy?

Response: Yes. Classification: Implemented.

A privacy notice is published at pallas.lonia.ai/privacy, alongside a Data Processing Agreement, a Data Protection Impact Assessment, a Transfer Impact Assessment, and the EU Standard Contractual Clauses. The schema distinguishes the two controller roles rather than only the policy text doing so.

Control inventory: procurement-documentation-published, gdpr-controller-split-documented.

DOCU-07

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

Response: No. Classification: Gap, disclosed.

There is no documented employee onboarding and offboarding policy. What limits operator access instead is technical: OAuth-only sign-in with no password to share or transfer, least-privilege service roles, and a tamper-evident audit trail over administrative actions.

Control inventory: personnel-no-formal-screening-program, auth-oauth-only, tenant-service-role-bypass-disclosed.

THRD-01

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

Response: No. Classification: Gap, disclosed.

Pallas does not perform its own security assessments of Supabase, Cloudflare, Stripe, or Resend. It relies on the certifications each provider publishes. Those certifications belong to the provider and cover that provider's infrastructure only.

Control inventory: subprocessors-certifications-are-theirs.

THRD-02

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

Response: Yes. Classification: Implemented.

Each subprocessor is engaged under that provider's data processing terms, which govern access to and handling of customer data. The full list with purpose, data categories, and processing location is published rather than supplied on request.

Control inventory: subprocessors-published-list, subprocessors-change-notice.

THRD-03

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

Response: No. Classification: Gap, disclosed.

Pallas accepts each provider's standard published data processing terms and has not negotiated bespoke breach-liability provisions with any subprocessor. Liability allocation between Pallas and the institution is addressed in the institutional terms of service rather than upstream.

Control inventory: subprocessors-published-list, procurement-documentation-published.

THRD-04

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

Response: Yes. Classification: Compensating control.

The strategy is publication and notice rather than assessment: the subprocessor list is published with purpose, data categories, processing location, and published certifications for each provider, and a new subprocessor is published with 30 days advance notice before it processes any customer data. It does not include independent assessment of those providers, which is answered no at THRD-01.

Control inventory: subprocessors-published-list, subprocessors-change-notice, subprocessors-certifications-are-theirs.

THRD-05

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

Response: No. Classification: Not applicable.

Pallas procures and operates no hardware. All compute, storage, and network capacity is provider-managed, so there is no hardware supply chain to govern. The software supply chain is managed and is answered at APPL-10.

Control inventory: network-perimeter-subprocessor-operated, physical-security-subprocessor-operated.

CHNG-01

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

Response: Yes. Classification: Implemented.

A new subprocessor is published with 30 days advance notice before it processes any customer data. Material changes affecting security posture are communicated to institutional customers.

Control inventory: subprocessors-change-notice.

CHNG-02

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

Response: N/A. Classification: Not applicable.

N/A - not applicable to Pallas because it is a single-version multi-tenant service with no per-customer code customisation. Per-plan feature differences are enforced server side in Row-Level Security policies rather than delivered as customer-specific builds.

Control inventory: plan-feature-flags-server-enforced.

CHNG-03

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

Response: N/A. Classification: Not applicable.

N/A - not applicable to Pallas because it deploys no virtual machines, server images, or operating system instances. Compute is Cloudflare Workers and Supabase managed services, so there is no gold image to manage.

Control inventory: network-perimeter-subprocessor-operated.

CHNG-04

Do you have a documented change management process?

Response: Yes. Classification: Implemented.

Every change reaches production through version control, and deployment to Cloudflare Pages and to every Worker is a deliberate manual operator step rather than an automatic consequence of a merge.

Control inventory: vuln-version-control-and-review, vuln-deploys-are-manual.

CHNG-05

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

Response: Yes. Classification: Implemented.

A single release command runs a type check, the unit test suite over the security and validation code, the build, an automated accessibility scan against the built artifact, and a Turnstile configuration check. The chain fails closed rather than degrading, so an unvalidated change cannot reach production through it.

Control inventory: appsec-release-gate-fails-closed, vuln-version-control-and-review.

CHNG-06

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

Response: Yes. Classification: Implemented.

Dependency advisories are monitored through the package registry audit feed and platform security alerts, and are triaged by whether a request path actually reaches the affected code. The triage record covers every open advisory with the specific reason it is or is not reachable in the current build.

Control inventory: vuln-advisory-triage-artifact.

CHNG-07

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

Response: Yes. Classification: Compensating control.

Patching is governed by the advisory triage record rather than by a numeric remediation window. No numeric remediation window is published, and one will not be quoted before it can be held. Platform-level patching for the database, edge network, and runtime is performed by Supabase and Cloudflare on their own schedules.

Control inventory: vuln-advisory-triage-artifact, network-perimeter-subprocessor-operated.

CHNG-08

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

Response: Yes. Classification: Implemented.

The triage record states, for each open advisory, whether a request path reaches the affected code. An advisory in a build-time tool that never runs in front of a visitor is treated differently from one in shipped code, and the reasoning is written down rather than asserted.

Control inventory: vuln-advisory-triage-artifact.

CHNG-09

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

Response: No. Classification: Not applicable.

Pallas is a single-version multi-tenant service. Customers cannot postpone or decline an update, because only one version is in production at any time. This is a property of the delivery model rather than a control gap, but it is answered no because the capability genuinely does not exist.

Control inventory: plan-feature-flags-server-enforced.

CHNG-10

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

Response: N/A. Classification: Not applicable.

N/A - not applicable to Pallas because exactly one version is in production at any time, so there is no concurrent-version support policy to define.

Control inventory: plan-feature-flags-server-enforced.

CHNG-11

Do you have a release schedule for product updates?

Response: No. Classification: Gap, disclosed.

No release schedule is published. Deployment is a deliberate manual operator step taken when a change has passed the release chain, rather than on a published cadence.

Control inventory: vuln-deploys-are-manual.

CHNG-12

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

Response: No. Classification: Gap, disclosed.

No two-year technology roadmap with enhancement and bug-fix timelines is published. A buyer who needs committed delivery dates should raise it during Enterprise contracting.

Control inventory: vuln-deploys-are-manual.

CHNG-13

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

Response: Yes. Classification: Implemented.

Updates are deployed to the hosted service and require no technical or organisational action by the institution.

Control inventory: vuln-deploys-are-manual.

CHNG-14

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

Response: Yes. Classification: Implemented.

Maintenance windows are announced at least 48 hours in advance and are scheduled outside 08:00 to 18:00 US Eastern on business days wherever possible. Because deployment is a deliberate manual step rather than an automatic consequence of a merge, timing is controlled rather than incidental.

Control inventory: vuln-deploys-are-manual.

CHNG-15

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

Response: Yes. Classification: Implemented.

Every change, including an emergency change, reaches production through version control and through the same release chain, so it is recorded and attributable after the fact even when the decision to ship was urgent.

Control inventory: vuln-version-control-and-review, vuln-deploys-are-manual, appsec-release-gate-fails-closed.

CHNG-16

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

Response: No. Classification: Gap, disclosed.

Pallas operates no server fleet, no appliances, and no managed device estate, so there is no systems management strategy covering them. There is also no mobile device management programme covering operator workstations, which is a genuine gap rather than an inapplicable question.

Control inventory: network-perimeter-subprocessor-operated, personnel-no-formal-screening-program.

PPPR-01

Do you have a documented patch management process?*

Response: Yes. Classification: Compensating control.

Patch management operates through the dependency advisory triage record, which covers every open advisory with the reason it is or is not reachable in the current build, and carries a review date. No numeric remediation window is published.

Control inventory: vuln-advisory-triage-artifact.

PPPR-02

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

Response: Yes. Classification: Implemented.

Pallas distinguishes the two controller roles in its schema, not only in its policy text: Lonia AI is controller for user account data, and the institution is controller for the data it brings. An organisation administrator can export the full organisation data set for a subject access request.

Control inventory: gdpr-controller-split-documented, gdpr-org-dsar-export.

PPPR-03

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

Response: Yes. Classification: Implemented.

Pallas accepts the obligations of the institution's jurisdiction as set out in the published Data Processing Agreement and Transfer Impact Assessment. Authority notification follows the jurisdiction: Ireland DPC, UK ICO, and EU supervisory authorities within 72 hours, with equivalent routes for Canadian and Australian regulators.

Control inventory: incident-authority-notification, procurement-documentation-published.

PPPR-04

Can you accommodate encryption requirements using open standards?

Response: Yes. Classification: Implemented.

All connections are TLS 1.3, enforced by Cloudflare and Supabase, and data at rest is encrypted with AES-256 through Supabase-managed infrastructure. Both are open, published standards rather than proprietary schemes.

Control inventory: encryption-in-transit, encryption-at-rest.

PPPR-05

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

Response: Yes. Classification: Compensating control.

The development lifecycle is documented as a gated release chain rather than as a separate SDLC policy document: version control for every change, a type check, unit tests over the security and validation code, an accessibility scan, an artifact freshness gate, and a manual deployment step. There is no formal SDLC document, and no separate design or security review stage.

Control inventory: vuln-version-control-and-review, appsec-release-gate-fails-closed.

PPPR-06

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

Response: No. Classification: Gap, disclosed.

Pallas performs no background screening or multi-state background checks. This is published as not yet formalised rather than answered from intent.

Control inventory: personnel-no-formal-screening-program.

PPPR-07

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

Response: No. Classification: Gap, disclosed.

There is no documented set of new-employee agreements or policy review requirements, because there is no formalised onboarding programme.

Control inventory: personnel-no-formal-screening-program.

PPPR-08

Do you have a documented information security policy?

Response: Yes. Classification: Compensating control.

Security practice is documented in the published security whitepaper, which is generated from the control inventory and cannot silently drift from it: the release chain fails closed if it does. This is documentation, not certification. No document in the set has been reviewed by an auditor, and there is no separately maintained internal information security policy instrument.

Control inventory: procurement-documentation-published, vuln-no-independent-certification.

PPPR-09

Are information security principles designed into the product lifecycle?

Response: Yes. Classification: Implemented.

Security controls are built into the product rather than added around it: Row-Level Security on every table from creation, OAuth-only authentication with no password path, a hostname and IP-literal denylist on every submitted scan URL, output escaping before untrusted content reaches HTML or email, and sandboxed rendering of scanned third-party markup on a dedicated origin.

Control inventory: tenant-rls-every-table, auth-oauth-only, appsec-ssrf-guard, appsec-output-escaping, appsec-sandboxed-rendering.

PPPR-10

Will you comply with applicable breach notification laws?

Response: Yes. Classification: Implemented.

Pallas notifies affected customers without undue delay and in any event within 72 hours of becoming aware of a breach affecting their data, and notifies the relevant supervisory authority on the same timetable.

Control inventory: incident-72-hour-notification, incident-authority-notification.

PPPR-11

Do you have an information security awareness program?

Response: No. Classification: Gap, disclosed.

There is no information security awareness programme. This is published as not yet formalised.

Control inventory: personnel-no-formal-screening-program.

PPPR-12

Is security awareness training mandatory for all employees?

Response: No. Classification: Gap, disclosed.

There is no mandatory security awareness training and no annual training record.

Control inventory: personnel-no-formal-screening-program.

PPPR-13

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?

Response: No. Classification: Gap, disclosed.

There is no recurring documented review of privileged account access lists. The scope of the server-side operator functions that bypass Row-Level Security by necessity is documented, and every administrative action they take appends to a tamper-evident audit chain, but the review itself is not a scheduled documented process.

Control inventory: personnel-no-formal-screening-program, tenant-service-role-bypass-disclosed, audit-sha256-ledger.

PPPR-14

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

Response: No. Classification: Gap, disclosed.

There are no internal audit processes or procedures. Pallas holds no SOC 2, ISO 27001, or other independent security certification, and performs no internal audit function of its own.

Control inventory: vuln-no-independent-certification, personnel-no-formal-screening-program.

PPPR-15

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

Response: N/A. Classification: Not applicable.

N/A - not applicable to Pallas because it operates no data centre, server cage, office server room, or other facility in which institutional data is held. Physical and environmental security for every system holding institutional data belongs to Supabase and Cloudflare, and Pallas can neither demonstrate nor test those controls.

Control inventory: physical-security-subprocessor-operated.

Product (41 questions)

AAAI-01

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

Response: Yes. Classification: Implemented.

Yes in the OAuth 2.0 / OIDC sense only: Pallas authenticates users and administrators through Google and Microsoft as identity providers, using OAuth 2.0 / OpenID Connect. SAML is not supported, and there is no generic connector for an arbitrary institutional identity provider (AAAI-06 and AAAI-15). Pallas stores no passwords, offers no password login, and has no password reset flow.

Control inventory: auth-oauth-only.

AAAI-02

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

Response: N/A. Classification: Not applicable.

N/A - not applicable to Pallas because there is no local-account path. OAuth through Google or Microsoft is the only authentication mechanism; local accounts do not exist.

Control inventory: auth-oauth-only.

AAAI-03

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

Response: N/A. Classification: Not applicable.

N/A - not applicable to Pallas because no passwords exist to apply complexity rules to. Credential policy is enforced by the institution's identity provider.

Control inventory: auth-oauth-only.

AAAI-04

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

Response: N/A. Classification: Not applicable.

N/A - not applicable to Pallas because the product has no password field anywhere.

Control inventory: auth-oauth-only.

AAAI-05

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

Response: N/A. Classification: Not applicable.

N/A - not applicable to Pallas because there is no password to reset. Account recovery is handled entirely by the institution's identity provider.

Control inventory: auth-oauth-only.

AAAI-06

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

Response: No. Classification: Gap, disclosed.

Pallas does not participate in InCommon or any other eduGAIN-affiliated trust federation. Authentication is Google and Microsoft OAuth only. An institution that requires federated access through InCommon should treat this as an open item.

Control inventory: auth-oauth-only.

AAAI-07

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

Response: No. Classification: Implemented.

No passwords or passphrases are hard-coded. Production secrets are held in the platform secret store and never in either repository; Worker configuration files carry placeholders rather than values, and this is checked rather than asserted.

Control inventory: encryption-no-secrets-in-repo, auth-oauth-only.

AAAI-08

Are you storing any passwords in plaintext?*

Response: No. Classification: Implemented.

No passwords are stored in any form, plaintext or hashed, because Pallas has no password authentication path at all.

Control inventory: auth-oauth-only.

AAAI-09

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

Response: No. Classification: Compensating control.

The audit chain records authenticated actions with actor attribution, an action name validated against a registry rather than accepted as free text, and a timestamp, and it is append-only with UPDATE and DELETE refused at the database level. Sign-in and sign-out are handled by Supabase Auth. Source IP address is not part of the Pallas audit event schema, so the four elements this question requires together are not all present, and the answer is no rather than a qualified yes.

Control inventory: audit-sha256-ledger, audit-action-registry, audit-ledger-append-only, auth-session-jwt.

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: Every audit event appends an entry to a SHA-256 hash chain, each entry hashed together with the previous entry hash, so that removing or altering an entry breaks the chain and is detectable. The ledger table is append-only in the strong sense: Row-Level Security is enabled with zero policies, and UPDATE and DELETE are refused with specific error codes (PA030 for update, PA031 for delete). Action names are validated against a registry table, so an unrecognised action cannot be written. Rows carry a seven-year retention floor enforced by a database CHECK constraint that an administrator cannot lower. Lawful removal under a retention policy or GDPR Article 17 appends a redaction entry recording that the removal happened rather than silently deleting. Actor name and email are snapshotted onto the row at write time, so attribution survives erasure of the user.. Classification: Informational.

There is no SIEM or external log collector integration, and no log forwarding to a customer-controlled destination. Institutional customers read audit data through the application and through the organisation export path rather than through a streaming integration.

Control inventory: audit-sha256-ledger, audit-ledger-append-only, audit-error-codes, audit-action-registry, audit-seven-year-floor, audit-lawful-redaction-recorded, audit-actor-attribution-survives-erasure.

AAAI-11

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)?*

Response: Yes. Classification: Implemented.

Retention is documented: audit rows carry a seven-year floor enforced by a CHECK constraint, and archived events past their window are purged nightly with each purge run logged. Protection is documented: the ledger is append-only with modification refused at the database level. Customer access is through the organisation data export rather than through direct log access.

Control inventory: audit-seven-year-floor, retention-audit-purge, audit-ledger-append-only, gdpr-org-dsar-export.

AAAI-12

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

Response: N/A. Classification: Not applicable.

N/A - not applicable to Pallas because there is no local-account path for an alternative authentication system to serve.

Control inventory: auth-oauth-only.

AAAI-13

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

Response: No. Classification: Gap, disclosed.

Pallas consumes the standard OAuth profile claims from Google and Microsoft and does not support configurable attribute mapping. eduPerson attributes including ePPA, ePPN, and ePE are not consumed.

Control inventory: auth-oauth-only.

AAAI-14

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

Response: N/A. Classification: Not applicable.

N/A - not applicable to Pallas because there is no local-account path requiring directory integration.

Control inventory: auth-oauth-only.

AAAI-15

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

Response: Yes. Classification: Compensating control.

OIDC is supported, through Google and Microsoft as identity providers. Other federation protocols and CAS are not supported, and there is no generic OIDC connector for an arbitrary institutional identity provider. An institution whose federation requires another protocol should treat this as an open item.

Control inventory: auth-oauth-only.

AAAI-16

Do you support differentiation between email address and user identifier?

Response: Yes. Classification: Implemented.

The user identifier is a UUID distinct from the email address. Audit attribution snapshots actor name and

email onto the row at write time while the identifier remains the stable key, so the two are separable by design.

Control inventory: audit-actor-attribution-survives-erasure, auth-profile-trigger-fail-safe.

AAAI-17

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

Response: N/A. Classification: Not applicable.

N/A - not applicable to Pallas because there is no local-account path. Multifactor authentication is enforced by the institution's identity provider at Google or Microsoft, and Pallas inherits the result rather than implementing a second factor of its own.

Control inventory: auth-oauth-only.

AAAI-18

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

Response: Yes. Classification: Implemented.

Sessions are JWT-based through Supabase Auth, and refresh tokens rotate on use, so a session expires rather than persisting indefinitely. No authentication state, entitlement, or quota is trusted from browser storage; authorisation decisions are made server side.

Control inventory: auth-session-jwt, auth-no-browser-storage-for-entitlements.

DATA-01

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?*

Response: Yes. Classification: Compensating control.

Institutional data is held in Supabase managed PostgreSQL and Storage, which are reached at provider-managed endpoints on the public internet rather than inside a private network Pallas operates. The answer is yes because that is the honest reading of the question. Access is constrained by TLS 1.3 in transit, authenticated access, and Row-Level Security enabled on every application table with policies resolving membership through SECURITY DEFINER helpers with a pinned search_path.

Control inventory: encryption-in-transit, tenant-rls-every-table, tenant-org-scoping-helpers, network-perimeter-subprocessor-operated.

DATA-02

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

Response: Yes. Classification: Implemented.

All connections are TLS 1.3, enforced by Cloudflare at the edge and by Supabase for database and Storage access.

Control inventory: encryption-in-transit.

DATA-03

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

Response: Yes. Classification: Implemented.

Data is encrypted at rest with AES-256 through Supabase-managed infrastructure. This is a subprocessor capability that Pallas relies on rather than implements; no Pallas code performs the encryption.

Control inventory: encryption-at-rest.

DATA-04

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

Response: No. Classification: Gap, disclosed.

Pallas makes no FIPS 140-2 or 140-3 validation claim. Cryptography is provided by Supabase and Cloudflare, and Pallas does not assert validation status on their behalf. A buyer with a FIPS requirement should verify it with those providers directly.

Control inventory: encryption-at-rest, encryption-in-transit, subprocessors-certifications-are-theirs.

DATA-05

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

Response: Yes. Classification: Implemented.

Data remains available within the system until the organisation's retention policy applies or the organisation is deleted. Retention defaults are 365 days for scan data, 7 days for uploaded source files, and 730 days for reports, configurable per organisation.

Control inventory: retention-per-org-policies, gdpr-org-deletion.

DATA-06

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

Response: Yes. Classification: Implemented.

Ownership of institutional data, inputs, outputs, and metadata rests with the institution under the published institutional terms of service, and that allocation is not contingent on a change of control at Lonia AI.

Control inventory: procurement-documentation-published, gdpr-controller-split-documented.

DATA-07

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

Response: No. Classification: Implemented.

Backups remain within the provider region. The default processing location is the United States: Supabase hosts the database and Storage in us-east-1, and backups are provider-operated within that footprint.

Control inventory: data-location-default-us, backup-provider-operated.

DATA-08

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

Response: Yes. Classification: Implemented.

Long-term retention media are provider-operated. Pallas holds no media of its own, so the environmental protection this question asks about is entirely a Supabase and Cloudflare facility control, relied on rather than owned.

Control inventory: physical-security-subprocessor-operated, backup-provider-operated.

DATA-09

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

Response: Yes. Classification: Implemented.

An organisation administrator can export the full organisation data set and can delete the organisation. Deletion cancels the Stripe subscription, wipes Storage under the organisation prefix, and removes the organisation's rows; the retention sweep issues real DELETE statements rather than storing a preference.

Control inventory: gdpr-org-dsar-export, gdpr-org-deletion, retention-deletion-actually-deletes.

DATA-10

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

Response: Yes. Classification: Implemented.

An organisation administrator can export the full organisation data set at any time, and any individual user can export the personal data Pallas holds about them across every organisation they belong to.

Control inventory: gdpr-org-dsar-export, gdpr-art15-art20-user-export.

DATA-11

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

Response: No. Classification: Not applicable.

Provider backups cover database and Storage content. They do not include operating system software, utilities, or application images, because Pallas deploys none: the application is rebuilt and redeployed from version control rather than restored from a system image.

Control inventory: backup-provider-operated, vuln-version-control-and-review.

DATA-12

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

Response: Yes. Classification: Implemented.

Backups are provider-operated and held separately from the primary database by Supabase, with point-in-time recovery available on the provider tier. Pallas runs no backup schedule of its own and has not customised the provider posture.

Control inventory: backup-provider-operated.

DATA-13

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

Response: N/A. Classification: Not applicable.

N/A - not applicable to Pallas because there is no physical media to move. All storage is provider-managed and no tapes, disks, or other removable media exist.

Control inventory: physical-security-subprocessor-operated.

DATA-14

Are data backups encrypted?

Response: Yes. Classification: Implemented.

Backups inherit AES-256 encryption at rest through Supabase-managed infrastructure. This is a provider assertion that Pallas relies on rather than a property Pallas implements or can test.

Control inventory: encryption-at-rest, backup-provider-operated.

DATA-15

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?

Response: No. Classification: Not applicable.

Pallas handles no physical media, so it maintains no media handling, end-of-life, repurposing, or sanitisation process. Media lifecycle for the systems holding institutional data is a Supabase and Cloudflare responsibility. Logical deletion of customer data is separately implemented and is answered at DATA-09.

Control inventory: physical-security-subprocessor-operated, retention-deletion-actually-deletes.

DATA-16

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

Response: No. Classification: Not applicable.

Pallas asserts no conformance to DoD 5220.22-M or NIST SP 800-88, because it operates no media to sanitise. It does not assert those standards on behalf of its providers either.

Control inventory: physical-security-subprocessor-operated, subprocessors-certifications-are-theirs.

DATA-17

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

Response: Yes. Classification: Compensating control.

Server-side operator functions run under service credentials that bypass Row-Level Security by necessity, so operator access to institutional data is possible. The scope of those functions is documented rather than hidden, and every administrative action they take appends to a tamper-evident audit chain that the operator cannot silently alter. Subprocessors also hold the data they process, as published on the subprocessor list.

Control inventory: tenant-service-role-bypass-disclosed, audit-sha256-ledger, audit-ledger-append-only, subprocessors-published-list.

DATA-18

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)?

Response: No. Classification: Gap, disclosed.

There is no documented strategy for securing operator workstations when working remotely, and no managed device programme. This is a genuine gap rather than an inapplicable question.

Control inventory: personnel-no-formal-screening-program.

DATA-19

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).

Response: No. Classification: Compensating control.

Pallas is multi-tenant and offers no dedicated single-tenant deployment. Separation is logical and enforced in the database: Row-Level Security is enabled on every application table, tenant-scoped policies resolve membership through two SECURITY DEFINER helpers with a pinned search_path rather than through a client-supplied value, and the evidence, source-files, and reports Storage buckets are private with per-organisation policies on storage objects.

Control inventory: tenant-rls-every-table, tenant-org-scoping-helpers, tenant-storage-per-org.

DATA-20

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

Response: Yes. Classification: Implemented.

The institution retains ownership of its data, inputs, outputs, and metadata. Pallas distinguishes the two controller roles in its schema: Lonia AI is controller for user account data, and the institution is controller for the data it brings.

Control inventory: gdpr-controller-split-documented, procurement-documentation-published.

DATA-21

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?

Response: Yes. Classification: Compensating control.

Export is available continuously while the subscription is live: an organisation administrator can export the full organisation data set at any time without needing to request it. A specific post-termination window is agreed in the institutional agreement rather than published as a fixed number here, and Pallas will not quote a term it has not written down.

Control inventory: gdpr-org-dsar-export, gdpr-art15-art20-user-export, procurement-documentation-published.

DATA-22

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

Response: Yes. Classification: Implemented.

Automated backups and point-in-time recovery run on the Supabase provider schedule, with the recoverable window set by the provider tier. No restore test has been performed, so recoverability is a provider assertion rather than a demonstrated property.

Control inventory: backup-provider-operated, backup-no-restore-test.

DATA-23

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.)?

Response: No. Classification: Not applicable.

Pallas operates no cryptographic key management process because it manages no customer-data encryption keys. Key generation, storage, rotation, and replacement for data at rest are performed by Supabase, and there is no bring-your-own-key or customer-managed-key option. Application secrets are held in the platform secret store and never in either repository.

Control inventory: encryption-at-rest, encryption-no-secrets-in-repo.

Infrastructure (51 questions)

APPL-01

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)?*

Response: Yes. Classification: Implemented.

Organisation membership carries one of four roles: org_admin, manager, contributor, viewer. Every

tenant-scoped policy resolves membership through two SECURITY DEFINER helpers with a pinned search_path rather than through a client-supplied identifier.

Control inventory: access-org-roles, tenant-org-scoping-helpers, tenant-rls-every-table.

APPL-02

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

Response: Yes. Classification: Implemented.

Traffic reaches Pallas through the Cloudflare edge, which provides the web application firewall and DDoS mitigation. This is a provider capability Pallas relies on rather than operates; Pallas runs no firewall of its own.

Control inventory: network-perimeter-subprocessor-operated.

APPL-03

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?*

Response: Yes. Classification: Implemented.

Runtime and platform versions are provider-managed and current. Dependency advisories are monitored and triaged by whether a request path reaches the affected code, and the release chain fails closed rather than degrading.

Control inventory: vuln-advisory-triage-artifact, appsec-release-gate-fails-closed.

APPL-04

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

Response: No. Classification: Implemented.

Pallas requires no access to location or GPS data and collects none. The data classes it holds are enumerated in the control inventory.

Control inventory: data-classes-enumerated.

APPL-05

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

Response: Yes. Classification: Compensating control.

Within the application, four roles separate administration from standard use, and an organisation cannot be left without an administrator because removing or demoting the last org_admin is refused at the database level. On the operator side, separation of duties is limited by team size: the same person holds the operator functions, and the compensating control is that their actions append to a tamper-evident audit chain.

Control inventory: access-org-roles, access-last-admin-guard, tenant-service-role-bypass-disclosed, audit-sha256-ledger.

APPL-06

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

Response: No. Classification: Gap, disclosed.

There is no dedicated static application security testing tool in the release chain. What the chain does run is a type check across the whole codebase, a unit suite over the security and validation code specifically, an automated accessibility scan against the built artifact, and a Turnstile configuration check, all failing closed. That is not SAST and is not offered as a substitute for it.

Control inventory: appsec-release-gate-fails-closed, vuln-no-penetration-test.

APPL-07

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

Response: Yes. Classification: Implemented.

A single release command runs the unit test suite over the security and validation code, the build, an automated accessibility scan against the built artifact, and a Turnstile check. The chain fails closed, so a failing test blocks the release rather than warning about it.

Control inventory: appsec-release-gate-fails-closed.

APPL-08

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

Response: No. Classification: Gap, disclosed.

There is no staff role-based access control scheme, because there is no multi-person staff. Operator access runs through scoped service roles whose bypass of Row-Level Security is documented rather than hidden, and every action they take is audit-chained.

Control inventory: personnel-no-formal-screening-program, tenant-service-role-bypass-disclosed, audit-sha256-ledger.

APPL-09

Does the system provide data input validation and error messages?

Response: Yes. Classification: Implemented.

Every submitted scan URL is validated against a hostname and IP-literal denylist before it is fetched, fetched third-party responses are capped at 10 MB against both the declared Content-Length and the observed byte count, and untrusted content is escaped before it reaches HTML or email.

Control inventory: appsec-ssrf-guard, appsec-response-cap, appsec-output-escaping.

APPL-10

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

Response: Yes. Classification: Implemented.

Dependencies reach production only through version control, and advisories are triaged against actual reachability with the triage recorded rather than asserted. The dependency set is deliberately small: the marketing site ships two runtime dependencies.

Control inventory: vuln-advisory-triage-artifact, vuln-version-control-and-review.

APPL-11

Have your developers been trained in secure coding techniques?

Response: No. Classification: Gap, disclosed.

There is no secure coding training programme and no training record. This is a personnel programme gap and is published as one.

Control inventory: personnel-no-formal-screening-program.

APPL-12

Was your application developed using secure coding techniques?

Response: Yes. Classification: Implemented.

Specific classes of defect are addressed structurally: server-side request forgery by a denylist applied before any fetch, cross-site scripting by escaping untrusted content before it reaches HTML or email, tenant leakage by Row-Level Security on every table, and hostile markup by rendering scanned third-party HTML on a dedicated origin with an empty storage partition and a restrictive Content-Security-Policy.

Control inventory: appsec-ssrf-guard, appsec-output-escaping, appsec-sandboxed-rendering, tenant-rls-every-table.

APPL-13

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

Response: N/A. Classification: Not applicable.

N/A - not applicable to Pallas because it ships no mobile application. Pallas is reached through a web browser only.

Control inventory: none. This is an identity or contact field and asserts no control.

APPL-14

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

Response: No. Classification: Gap, disclosed.

There is no documented procedure governing how operator personnel obtain administrative access to an institutional instance. The scope of the service-role functions that make such access possible is documented, and their use is audit-chained, but the authorisation procedure itself is not written down.

Control inventory: tenant-service-role-bypass-disclosed, personnel-no-formal-screening-program,

audit-sha256-ledger.

DCTR-01

Select your hosting option.

Response: Third-party cloud hosting. Supabase provides managed PostgreSQL, Auth, and Storage in us-east-1. Cloudflare provides the edge network, Workers, and Pages hosting.. Classification: Informational.

Pallas owns and operates no data centre, rack, or server. Every system that holds institutional data is provider-operated.

Control inventory: subprocessors-published-list, data-location-default-us, physical-security-subprocessor-operated.

DCTR-02

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

Response: Yes. Classification: Implemented.

Supabase and Cloudflare publish SOC 2 Type 2 reports covering their infrastructure. Those reports belong to those providers. Pallas holds no SOC 2 report of its own, and a provider report must never be read as covering the Pallas application built on top of it.

Control inventory: subprocessors-certifications-are-theirs, vuln-no-independent-certification.

DCTR-03

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

Response: No. Classification: Gap, disclosed.

The processing location is the United States for all customers. No European Union hosting exists and none is offered. A buyer with a regional storage requirement should treat this as an open item.

Control inventory: data-location-eu-option, data-location-default-us.

DCTR-04

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

Response: Yes. Classification: Implemented.

Facility staffing is a Supabase and Cloudflare control. Pallas relies on it and can neither demonstrate nor test it; a buyer needing evidence should read the provider audit reports rather than treat this answer as evidence.

Control inventory: physical-security-subprocessor-operated.

DCTR-05

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

Response: Yes. Classification: Implemented.

Pallas operates no servers of its own. Physical separation within the facilities where Supabase and Cloudflare operate the systems holding institutional data is a provider control described in their published

audit reports, relied on rather than owned.

Control inventory: physical-security-subprocessor-operated.

DCTR-06

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

Response: Yes. Classification: Implemented.

Enclosure of the physical space is a provider control at Supabase and Cloudflare. Pallas has no devices in any facility and therefore no physical contact surface of its own.

Control inventory: physical-security-subprocessor-operated.

DCTR-07

Are your primary and secondary data centers geographically diverse?

Response: Yes. Classification: Implemented.

Geographic diversity is a property of the Supabase and Cloudflare platforms rather than an architecture Pallas designed. Pallas has not published a recovery time or recovery point objective and has performed no restore test, so the practical value of that diversity to a Pallas recovery is untested.

Control inventory: physical-security-subprocessor-operated, backup-provider-operated, backup-no-restore-test.

DCTR-08

Is the service hosted in a high-availability environment?

Response: Yes. Classification: Implemented.

The service runs on Cloudflare's edge and Supabase's managed platform, both of which are high-availability environments by design. The published availability target is 99.9 percent monthly, offered on commercially reasonable efforts and not as a contractual service credit.

Control inventory: network-perimeter-subprocessor-operated, backup-provider-operated.

DCTR-09

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

Response: Yes. Classification: Implemented.

Redundant power is a Supabase and Cloudflare facility control. Pallas relies on it and cannot demonstrate it.

Control inventory: physical-security-subprocessor-operated.

DCTR-10

Are redundant power strategies tested?*

Response: Yes. Classification: Implemented.

Power redundancy testing is performed by the facility operators under their own audit programmes. Pallas neither performs nor witnesses those tests.

Control inventory: physical-security-subprocessor-operated, subprocessors-certifications-are-theirs.

DCTR-11

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

Response: Yes. Classification: Implemented.

Cooling and fire suppression are facility controls at Supabase and Cloudflare, covered by their published audit reports. Pallas relies on them.

Control inventory: physical-security-subprocessor-operated.

DCTR-12

Do you have Internet Service Provider (ISP) redundancy?

Response: Yes. Classification: Implemented.

Network redundancy is provided by the Cloudflare edge, which is the ingress path for all Pallas traffic. Pallas contracts with no internet service provider of its own.

Control inventory: network-perimeter-subprocessor-operated.

DCTR-13

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

Response: Yes. Classification: Implemented.

Carrier diversity into the facilities is a provider control. Pallas has no facility and therefore no carrier arrangements to describe.

Control inventory: physical-security-subprocessor-operated, network-perimeter-subprocessor-operated.

DCTR-14

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

Response: Yes. Classification: Compensating control.

Operator access to the Supabase, Cloudflare, and Stripe consoles is through Google and Microsoft accounts with multifactor authentication enforced at the identity provider. This is an operator configuration statement: it is not verifiable from either repository, and it is offered as an assertion rather than as a demonstrated control.

Control inventory: auth-oauth-only, tenant-service-role-bypass-disclosed.

DCTR-15

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

Response: No. Classification: Not applicable.

Pallas deploys no virtual machines and no server images, so there are no hardening tools or pre-hardened images to apply. Compute is Cloudflare Workers and Supabase managed services, hardened by the provider rather than configured by Pallas.

Control inventory: network-perimeter-subprocessor-operated.

DCTR-16

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

Response: Yes. Classification: Compensating control.

Encryption keys for data at rest are generated and held by Supabase. Pallas offers no bring-your-own-key or customer-managed-key option, so the hosting provider does hold the keys. A buyer whose control requires customer-held keys should treat this as an open item.

Control inventory: encryption-at-rest.

FIDP-01

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

Response: Yes. Classification: Implemented.

Stateful filtering and DDoS mitigation are performed at the Cloudflare edge, through which all Pallas traffic passes. Pallas operates no firewall of its own, so this is reliance on a provider capability rather than an owned control.

Control inventory: network-perimeter-subprocessor-operated.

FIDP-02

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

Response: No. Classification: Not applicable.

There is no firewall change request policy because Pallas operates no firewall to change. Edge rule configuration is provider-managed.

Control inventory: network-perimeter-subprocessor-operated.

FIDP-03

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

Response: No. Classification: Gap, disclosed.

Pallas operates no network intrusion detection system and has not configured one at a provider. A buyer requiring a monitored perimeter under vendor control should treat this as an open item.

Control inventory: network-perimeter-subprocessor-operated.

FIDP-04

Do you employ host-based intrusion detection?*

Response: N/A. Classification: Not applicable.

N/A - not applicable to Pallas because it operates no hosts. Compute is Cloudflare Workers and Supabase managed services, so there is no host on which to run an agent.

Control inventory: network-perimeter-subprocessor-operated.

FIDP-05

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

Response: No. Classification: Not applicable.

Pallas operates no network, firewall, IDS, or IPS, so it holds no change logs for them. Audit logging over application and administrative actions is separately implemented and is answered at AAAI-10.

Control inventory: network-perimeter-subprocessor-operated, audit-sha256-ledger.

FIDP-06

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

Response: No. Classification: Not applicable.

There is no firewall change approval authority to document, because there is no firewall under Pallas control.

Control inventory: network-perimeter-subprocessor-operated.

FIDP-07

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

Response: No. Classification: Gap, disclosed.

Pallas operates no network intrusion prevention system. Cloudflare's managed rules run in front of Pallas traffic, but they are not configured or tuned by Pallas as an IPS and are not claimed as one.

Control inventory: network-perimeter-subprocessor-operated.

FIDP-08

Do you employ host-based intrusion prevention?

Response: N/A. Classification: Not applicable.

N/A - not applicable to Pallas because it operates no hosts on which a host-based prevention agent could run.

Control inventory: network-perimeter-subprocessor-operated.

FIDP-09

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

Response: No. Classification: Gap, disclosed.

Pallas employs no next-generation persistent threat monitoring. Worker observability and logging are enabled on every deployed Worker so that failures surface rather than passing silently, which is operational monitoring and not threat monitoring.

Control inventory: network-perimeter-subprocessor-operated, incident-detection-monitoring.

FIDP-10

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

Response: Neither. Pallas performs no intrusion monitoring internally and retains no third-party monitoring service.. Classification: Informational.

What exists instead is operational observability: logging is enabled on every deployed Worker so that failures surface rather than passing silently. That is a monitoring capability for availability and errors, not for intrusion, and it is not staffed around the clock.

Control inventory: network-perimeter-subprocessor-operated, incident-detection-monitoring.

FIDP-11

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

Response: No. Classification: Gap, disclosed.

There is no 24 by 7 intrusion monitoring and no security operations centre, staffed or retained. The published support response window is 2 to 3 business days.

Control inventory: network-perimeter-subprocessor-operated, incident-detection-monitoring.

HFIH-01

Do you have a formal incident response plan?

Response: Yes. Classification: Compensating control.

The incident response position is documented as a published commitment set: notification to affected customers without undue delay and within 72 hours of awareness, authority notification following the jurisdiction, and a full technical postmortem to affected customers within 30 days. It is a commitment set rather than an exercised runbook, and no tabletop exercise has been performed.

Control inventory: incident-72-hour-notification, incident-authority-notification, incident-post-incident-report, procurement-documentation-published.

HFIH-02

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

Response: No. Classification: Gap, disclosed.

There is no internal incident response team and no retained external team. The operator responds. A buyer requiring a named or retained response capability should treat this as an open item.

Control inventory: personnel-no-formal-screening-program, incident-detection-monitoring.

HFIH-03

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

Response: No. Classification: Gap, disclosed.

There is no 24 by 7 incident response capability and no on-call rotation. The published support response window is 2 to 3 business days. The 72 hour breach notification commitment is a separate obligation and is met regardless of the support window.

Control inventory: incident-detection-monitoring, incident-72-hour-notification.

HFIH-04

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

Response: No. Classification: Gap, disclosed.

Pallas does not publish a cyber liability policy or certificate of cover. Where a contract requires evidence of cover, the matter is addressed in the agreement during procurement rather than left implied.

Control inventory: insurance-no-published-cover.

VULN-01

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

Response: No. Classification: Gap, disclosed.

There is no authenticated vulnerability scan before release. The release chain runs a type check, the unit suite over the security and validation code, an accessibility scan, and a Turnstile check, all failing closed. None of those is a vulnerability scanner and none is offered as one.

Control inventory: appsec-release-gate-fails-closed, vuln-no-penetration-test.

VULN-02

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

Response: No. Classification: Compensating control.

There are no vulnerability scan results to provide, because no scanning programme is run. What is available on request from support@lonia.ai is the dependency advisory triage record, which covers every open advisory with the specific reason it is or is not reachable in the current build, and carries a review date.

Control inventory: vuln-advisory-triage-artifact, vuln-no-penetration-test.

VULN-03

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?*

Response: Yes. Classification: Implemented.

Institutional vulnerability testing against the Pallas application is permitted at a mutually agreed time and date, arranged during procurement. Testing that would reach Supabase or Cloudflare infrastructure is subject to those providers' own testing policies rather than to Pallas consent alone.

Control inventory: vuln-no-penetration-test, subprocessors-published-list.

VULN-04

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

Response: No. Classification: Gap, disclosed.

Pallas has not commissioned an independent penetration test or third-party security assessment. No date for an independent test is promised. If a current report is required before signing, that should be raised during procurement.

Control inventory: vuln-no-penetration-test, vuln-no-independent-certification.

VULN-05

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

Response: No. Classification: Compensating control.

No web application vulnerability scanner is run on a schedule. The specific classes this question names are addressed structurally instead: injection by parameterised database access under Row-Level Security, cross-site scripting by escaping untrusted content before it reaches HTML or email, and cross-site request forgery by Turnstile verification that fails closed on every unauthenticated write endpoint. Structural controls and scanning are not equivalent, and the absence of scanning is stated rather than papered over.

Control inventory: appsec-output-escaping, access-turnstile-fails-closed, tenant-rls-every-table, vuln-no-penetration-test.

VULN-06

Are your systems and applications regularly scanned externally for vulnerabilities?

Response: No. Classification: Gap, disclosed.

Systems and applications are not regularly scanned externally for vulnerabilities. This is a genuine gap and is listed as one.

Control inventory: vuln-no-penetration-test.

IT Accessibility (18 questions)

ITAC-01

Solution Provider Accessibility Contact Name

Response: Pallas Support. Classification: Informational.

Accessibility correspondence is handled through the general support mailbox rather than a separate named accessibility officer.

Control inventory: none. This is an identity or contact field and asserts no control.

ITAC-02

Solution Provider Accessibility Contact Title

Response: Support and Accessibility Contact. Classification: Informational.

Accessibility is the subject matter of the product, so accessibility questions are handled by the operator directly rather than routed to a separate function.

Control inventory: none. This is an identity or contact field and asserts no control.

ITAC-03

Solution Provider Accessibility Contact Email

Response: support@lonia.ai. Classification: Informational.

No separate accessibility mailbox is published. Accessibility feedback submitted to support@lonia.ai is handled under the response commitment published at pallas.lonia.ai/accessibility.

Control inventory: none. This is an identity or contact field and asserts no control.

ITAC-04

Solution Provider Accessibility Contact Phone Number

Response: Not published. Accessibility contact is by email at support@lonia.ai.. Classification: Informational.

No telephone line is published for accessibility or for general support. A buyer whose accessibility policy requires a telephone route should raise it during procurement.

Control inventory: none. This is an identity or contact field and asserts no control.

ITAC-05

Web Link to Accessibility Statement or VPAT

Response: https://pallas.lonia.ai/accessibility and the VPAT 2.5 Accessibility Conformance Report at https://pallas.lonia.ai/documents/pallas-vpat-2.5-acr.pdf. Classification: Informational.

Both are published rather than supplied on request. The conformance report is generated from a single content source and the build fails if the published PDF drifts from it.

Control inventory: scan-vpat-published, procurement-documentation-published.

ITAC-06

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

Response: Yes. Classification: Implemented.

A VPAT 2.5 Accessibility Conformance Report is published for Pallas and has been updated within the past 12 months. It is regenerated from its content source rather than edited by hand, and a build gate reads the published verdict counts back out of the PDF to confirm they match the source.

Control inventory: scan-vpat-published.

ITAC-07

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

Response: Yes. Classification: Implemented.

Pallas commits contractually to WCAG 2.2 AA, which supersedes and includes WCAG 2.1 AA. WCAG 2.2 AA is treated as a floor rather than a target, and Section 508 and EN 301 549 alignment are also published.

Control inventory: scan-vpat-published, scan-508-and-en301549-are-tag-presets, procurement-documentation-published.

ITAC-08

Does the solution substantially conform to WCAG 2.1 AA?*

Response: Yes. Classification: Implemented.

Pallas substantially conforms to WCAG 2.1 AA and is built to WCAG 2.2 AA. The published VPAT 2.5 report states the per-criterion verdicts, including the criteria where conformance is partial, rather than asserting blanket conformance.

Control inventory: scan-vpat-published.

ITAC-09

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

Response: Yes. Classification: Implemented.

A feedback route and a response commitment are published at pallas.lonia.ai/accessibility. Reported issues are tracked through the same version control and release process as any other change.

Control inventory: scan-vpat-published, vuln-version-control-and-review, procurement-documentation-published.

ITAC-10

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

Response: Yes. Classification: Implemented.

The published VPAT 2.5 report documents the accessibility features and the per-criterion conformance position, and the accessibility statement documents the standard adopted and the known limitations.

Control inventory: scan-vpat-published, procurement-documentation-published.

ITAC-11

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

Response: No. Classification: Gap, disclosed.

No independent third-party accessibility audit of the current version has been commissioned. The VPAT is self-produced. Automated testing runs against every release build, and PDF tag conformance is confirmed by

the operator with PAC 2024, but neither is an independent expert audit and neither is offered as one.

Control inventory: scan-vpat-published, scan-wcag-coverage, vuln-no-independent-certification.

ITAC-12

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

Response: Yes. Classification: Implemented.

An automated accessibility test runs against the built artifact on every release and fails the build rather than warning. Its coverage is bounded and the bound is published: automated detection covers approximately 17 of the WCAG 2.2 success criteria, and the remainder require human review.

Control inventory: appsec-release-gate-fails-closed, scan-wcag-coverage, scan-vpat-published.

ITAC-13

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

Response: Yes. Classification: Implemented.

WCAG 2.2 AA is the adopted technical standard. Section 508 and EN 301 549 alignment are also published, with the disclosure that those results are produced by applying the corresponding rule tag presets rather than by an independent evaluation against each standard's own text.

Control inventory: scan-vpat-published, scan-508-and-en301549-are-tag-presets.

ITAC-14

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

Response: No. Classification: Gap, disclosed.

No accessibility roadmap with delivery timelines is published. Known limitations are published in the VPAT and the accessibility statement, but without committed dates against them.

Control inventory: scan-vpat-published, scan-wcag-coverage.

ITAC-15

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

Response: Yes. Classification: Compensating control.

Accessibility expertise is the subject matter of the product rather than an adjacent skill, and the expectation is enforced mechanically by an accessibility gate that fails every release build that regresses. There is no formal training curriculum, certification requirement, or training record, so the expectation is not evidenced by a programme.

Control inventory: appsec-release-gate-fails-closed, personnel-no-formal-screening-program.

ITAC-16

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

Response: Yes. Classification: Implemented.

Accessibility testing is part of the release chain rather than a separate activity: the automated scan runs against the built artifact on every release and fails closed, so an inaccessible regression cannot ship through the normal path.

Control inventory: appsec-release-gate-fails-closed, scan-wcag-coverage.

ITAC-17

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

Response: Yes. Classification: Implemented.

All functions are operable by keyboard alone, with visible focus indication on every interactive element. Keyboard operability is among the criteria covered by the automated gate that runs against every release build, and the per-criterion position is published in the VPAT.

Control inventory: scan-vpat-published, appsec-release-gate-fails-closed.

ITAC-18

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?

Response: No. Classification: Implemented.

Pallas uses no accessibility overlay, no accessibility mode, no lite version, and no alternate interface. Accessibility is a property of the single interface everyone uses. Pallas publishes its reasoning on this at pallas.lonia.ai/why-not-an-overlay.

Control inventory: scan-vpat-published, procurement-documentation-published.

Case-Specific (60 questions)

CONS-01

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

Response: Left blank in the workbook, marked not applicable by a START HERE scoping answer. Classification: Not applicable.

N/A - not applicable to Pallas because Pallas is a product, not a consulting engagement. REQU-03 on the START HERE worksheet is answered No, which marks this section not applicable.

Control inventory: data-classes-enumerated.

CONS-02

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

Response: Left blank in the workbook, marked not applicable by a START HERE scoping answer. Classification: Not applicable.

N/A - not applicable to Pallas because Pallas is a product, not a consulting engagement. REQU-03 on the

START HERE worksheet is answered No, which marks this section not applicable.

Control inventory: data-classes-enumerated.

CONS-03

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

Response: Left blank in the workbook, marked not applicable by a START HERE scoping answer.
Classification: Not applicable.

N/A - not applicable to Pallas because Pallas is a product, not a consulting engagement. REQU-03 on the START HERE worksheet is answered No, which marks this section not applicable.

Control inventory: data-classes-enumerated.

CONS-04

Can access be restricted based on source IP address?*

Response: Left blank in the workbook, marked not applicable by a START HERE scoping answer.
Classification: Not applicable.

N/A - not applicable to Pallas because Pallas is a product, not a consulting engagement. REQU-03 on the START HERE worksheet is answered No, which marks this section not applicable.

Control inventory: data-classes-enumerated.

CONS-05

Will the consulting take place on-premises?

Response: Left blank in the workbook, marked not applicable by a START HERE scoping answer.
Classification: Not applicable.

N/A - not applicable to Pallas because Pallas is a product, not a consulting engagement. REQU-03 on the START HERE worksheet is answered No, which marks this section not applicable.

Control inventory: data-classes-enumerated.

CONS-06

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

Response: Left blank in the workbook, marked not applicable by a START HERE scoping answer.
Classification: Not applicable.

N/A - not applicable to Pallas because Pallas is a product, not a consulting engagement. REQU-03 on the START HERE worksheet is answered No, which marks this section not applicable.

Control inventory: data-classes-enumerated.

CONS-07

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

Response: Left blank in the workbook, marked not applicable by a START HERE scoping answer.

Classification: Not applicable.

N/A - not applicable to Pallas because Pallas is a product, not a consulting engagement. REQU-03 on the START HERE worksheet is answered No, which marks this section not applicable.

Control inventory: data-classes-enumerated.

CONS-08

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

Response: Left blank in the workbook, marked not applicable by a START HERE scoping answer.
Classification: Not applicable.

N/A - not applicable to Pallas because Pallas is a product, not a consulting engagement. REQU-03 on the START HERE worksheet is answered No, which marks this section not applicable.

Control inventory: data-classes-enumerated.

CONS-09

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

Response: Left blank in the workbook, marked not applicable by a START HERE scoping answer.
Classification: Not applicable.

N/A - not applicable to Pallas because Pallas is a product, not a consulting engagement. REQU-03 on the START HERE worksheet is answered No, which marks this section not applicable.

Control inventory: data-classes-enumerated.

HIPA-01

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?*

Response: Left blank in the workbook, marked not applicable by a START HERE scoping answer.
Classification: Not applicable.

N/A - not applicable to Pallas because it processes no protected health information and no data covered by HIPAA. REQU-05 on the START HERE worksheet is answered No, which marks this section not applicable. Pallas is not a business associate and will not execute a business associate agreement.

Control inventory: data-classes-enumerated.

HIPA-02

Have you identified areas of risk?*

Response: Left blank in the workbook, marked not applicable by a START HERE scoping answer.
Classification: Not applicable.

N/A - not applicable to Pallas because it processes no protected health information and no data covered by HIPAA. REQU-05 on the START HERE worksheet is answered No, which marks this section not applicable.

Control inventory: data-classes-enumerated.

HIPA-03

Have the relevant policies/plans been tested?*

Response: Left blank in the workbook, marked not applicable by a START HERE scoping answer.
Classification: Not applicable.

N/A - not applicable to Pallas because it processes no protected health information and no data covered by HIPAA. REQU-05 on the START HERE worksheet is answered No, which marks this section not applicable.

Control inventory: data-classes-enumerated.

HIPA-04

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

Response: Left blank in the workbook, marked not applicable by a START HERE scoping answer.
Classification: Not applicable.

N/A - not applicable to Pallas because it processes no protected health information and no data covered by HIPAA. REQU-05 on the START HERE worksheet is answered No, which marks this section not applicable.

Control inventory: data-classes-enumerated.

HIPA-05

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

Response: Left blank in the workbook, marked not applicable by a START HERE scoping answer.
Classification: Not applicable.

N/A - not applicable to Pallas because it processes no protected health information and no data covered by HIPAA. REQU-05 on the START HERE worksheet is answered No, which marks this section not applicable.

Control inventory: data-classes-enumerated.

HIPA-06

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

Response: Left blank in the workbook, marked not applicable by a START HERE scoping answer.
Classification: Not applicable.

N/A - not applicable to Pallas because it processes no protected health information and no data covered by HIPAA. REQU-05 on the START HERE worksheet is answered No, which marks this section not applicable.

Control inventory: data-classes-enumerated.

HIPA-07

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

Response: Left blank in the workbook, marked not applicable by a START HERE scoping answer.

Classification: Not applicable.

N/A - not applicable to Pallas because it processes no protected health information and no data covered by HIPAA. REQU-05 on the START HERE worksheet is answered No, which marks this section not applicable.

Control inventory: data-classes-enumerated.

HIPA-08

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

Response: Left blank in the workbook, marked not applicable by a START HERE scoping answer.
Classification: Not applicable.

N/A - not applicable to Pallas because it processes no protected health information and no data covered by HIPAA. REQU-05 on the START HERE worksheet is answered No, which marks this section not applicable.

Control inventory: data-classes-enumerated.

HIPA-09

Have you taken actions to mitigate the identified risks?

Response: Left blank in the workbook, marked not applicable by a START HERE scoping answer.
Classification: Not applicable.

N/A - not applicable to Pallas because it processes no protected health information and no data covered by HIPAA. REQU-05 on the START HERE worksheet is answered No, which marks this section not applicable.

Control inventory: data-classes-enumerated.

HIPA-10

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

Response: Left blank in the workbook, marked not applicable by a START HERE scoping answer.
Classification: Not applicable.

N/A - not applicable to Pallas because it processes no protected health information and no data covered by HIPAA. REQU-05 on the START HERE worksheet is answered No, which marks this section not applicable.

Control inventory: data-classes-enumerated.

HIPA-11

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

Response: Left blank in the workbook, marked not applicable by a START HERE scoping answer.
Classification: Not applicable.

N/A - not applicable to Pallas because it processes no protected health information and no data covered by HIPAA. REQU-05 on the START HERE worksheet is answered No, which marks this section not applicable.

Control inventory: data-classes-enumerated.

HIPA-12

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

Response: Left blank in the workbook, marked not applicable by a START HERE scoping answer.
Classification: Not applicable.

N/A - not applicable to Pallas because it processes no protected health information and no data covered by HIPAA. REQU-05 on the START HERE worksheet is answered No, which marks this section not applicable.

Control inventory: data-classes-enumerated.

HIPA-13

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

Response: Left blank in the workbook, marked not applicable by a START HERE scoping answer.
Classification: Not applicable.

N/A - not applicable to Pallas because it processes no protected health information and no data covered by HIPAA. REQU-05 on the START HERE worksheet is answered No, which marks this section not applicable.

Control inventory: data-classes-enumerated.

HIPA-14

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

Response: Left blank in the workbook, marked not applicable by a START HERE scoping answer.
Classification: Not applicable.

N/A - not applicable to Pallas because it processes no protected health information and no data covered by HIPAA. REQU-05 on the START HERE worksheet is answered No, which marks this section not applicable.

Control inventory: data-classes-enumerated.

HIPA-15

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

Response: Left blank in the workbook, marked not applicable by a START HERE scoping answer.
Classification: Not applicable.

N/A - not applicable to Pallas because it processes no protected health information and no data covered by HIPAA. REQU-05 on the START HERE worksheet is answered No, which marks this section not applicable.

Control inventory: data-classes-enumerated.

HIPA-16

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

Response: Left blank in the workbook, marked not applicable by a START HERE scoping answer.

Classification: Not applicable.

N/A - not applicable to Pallas because it processes no protected health information and no data covered by HIPAA. REQU-05 on the START HERE worksheet is answered No, which marks this section not applicable.

Control inventory: data-classes-enumerated.

HIPA-17

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

Response: Left blank in the workbook, marked not applicable by a START HERE scoping answer.
Classification: Not applicable.

N/A - not applicable to Pallas because it processes no protected health information and no data covered by HIPAA. REQU-05 on the START HERE worksheet is answered No, which marks this section not applicable.

Control inventory: data-classes-enumerated.

HIPA-18

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

Response: Left blank in the workbook, marked not applicable by a START HERE scoping answer.
Classification: Not applicable.

N/A - not applicable to Pallas because it processes no protected health information and no data covered by HIPAA. REQU-05 on the START HERE worksheet is answered No, which marks this section not applicable.

Control inventory: data-classes-enumerated.

HIPA-19

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

Response: Left blank in the workbook, marked not applicable by a START HERE scoping answer.
Classification: Not applicable.

N/A - not applicable to Pallas because it processes no protected health information and no data covered by HIPAA. REQU-05 on the START HERE worksheet is answered No, which marks this section not applicable.

Control inventory: data-classes-enumerated.

HIPA-20

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

Response: Left blank in the workbook, marked not applicable by a START HERE scoping answer.
Classification: Not applicable.

N/A - not applicable to Pallas because it processes no protected health information and no data covered by HIPAA. REQU-05 on the START HERE worksheet is answered No, which marks this section not applicable.

Control inventory: data-classes-enumerated.

HIPA-21

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

Response: Left blank in the workbook, marked not applicable by a START HERE scoping answer.
Classification: Not applicable.

N/A - not applicable to Pallas because it processes no protected health information and no data covered by HIPAA. REQU-05 on the START HERE worksheet is answered No, which marks this section not applicable.

Control inventory: data-classes-enumerated.

HIPA-22

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?

Response: Left blank in the workbook, marked not applicable by a START HERE scoping answer.
Classification: Not applicable.

N/A - not applicable to Pallas because it processes no protected health information and no data covered by HIPAA. REQU-05 on the START HERE worksheet is answered No, which marks this section not applicable.

Control inventory: data-classes-enumerated.

HIPA-23

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

Response: Left blank in the workbook, marked not applicable by a START HERE scoping answer.
Classification: Not applicable.

N/A - not applicable to Pallas because it processes no protected health information and no data covered by HIPAA. REQU-05 on the START HERE worksheet is answered No, which marks this section not applicable.

Control inventory: data-classes-enumerated.

HIPA-24

Can the application logs be archived?

Response: Left blank in the workbook, marked not applicable by a START HERE scoping answer.
Classification: Not applicable.

N/A - not applicable to Pallas because it processes no protected health information and no data covered by HIPAA. REQU-05 on the START HERE worksheet is answered No, which marks this section not applicable.

Control inventory: data-classes-enumerated.

HIPA-25

Can the application logs be saved externally?

Response: Left blank in the workbook, marked not applicable by a START HERE scoping answer.

Classification: Not applicable.

N/A - not applicable to Pallas because it processes no protected health information and no data covered by HIPAA. REQU-05 on the START HERE worksheet is answered No, which marks this section not applicable.

Control inventory: data-classes-enumerated.

HIPA-26

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

Response: Left blank in the workbook, marked not applicable by a START HERE scoping answer.
Classification: Not applicable.

N/A - not applicable to Pallas because it processes no protected health information and no data covered by HIPAA. REQU-05 on the START HERE worksheet is answered No, which marks this section not applicable.

Control inventory: data-classes-enumerated.

HIPA-27

Can you provide a HIPAA compliance attestation document?

Response: Left blank in the workbook, marked not applicable by a START HERE scoping answer.
Classification: Not applicable.

N/A - not applicable to Pallas because it processes no protected health information and no data covered by HIPAA. REQU-05 on the START HERE worksheet is answered No, which marks this section not applicable.

Control inventory: data-classes-enumerated.

HIPA-28

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

Response: Left blank in the workbook, marked not applicable by a START HERE scoping answer.
Classification: Not applicable.

N/A - not applicable to Pallas because it processes no protected health information and no data covered by HIPAA. REQU-05 on the START HERE worksheet is answered No, which marks this section not applicable.

Control inventory: data-classes-enumerated.

HIPA-29

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

Response: Left blank in the workbook, marked not applicable by a START HERE scoping answer.
Classification: Not applicable.

N/A - not applicable to Pallas because it processes no protected health information and no data covered by HIPAA. REQU-05 on the START HERE worksheet is answered No, which marks this section not applicable.

Control inventory: data-classes-enumerated.

PCID-01

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

Response: Left blank in the workbook, marked not applicable by a START HERE scoping answer.
Classification: Not applicable.

N/A - not applicable to Pallas because it neither processes, stores, nor transmits cardholder data. Payment is handled by Stripe, which collects card details directly; no card number, expiry, or verification value reaches Pallas systems. REQU-06 on the START HERE worksheet is answered No, which marks this section not applicable.

Control inventory: data-classes-enumerated, subprocessors-published-list.

PCID-02

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

Response: Left blank in the workbook, marked not applicable by a START HERE scoping answer.
Classification: Not applicable.

N/A - not applicable to Pallas because no cardholder data reaches Pallas systems; payment is handled directly by Stripe. REQU-06 on the START HERE worksheet is answered No, which marks this section not applicable.

Control inventory: data-classes-enumerated, subprocessors-published-list.

PCID-03

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

Response: Left blank in the workbook, marked not applicable by a START HERE scoping answer.
Classification: Not applicable.

N/A - not applicable to Pallas because no cardholder data reaches Pallas systems; payment is handled directly by Stripe. REQU-06 on the START HERE worksheet is answered No, which marks this section not applicable.

Control inventory: data-classes-enumerated, subprocessors-published-list.

PCID-04

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

Response: Left blank in the workbook, marked not applicable by a START HERE scoping answer.
Classification: Not applicable.

N/A - not applicable to Pallas because no cardholder data reaches Pallas systems; payment is handled directly by Stripe. REQU-06 on the START HERE worksheet is answered No, which marks this section not applicable.

Control inventory: data-classes-enumerated, subprocessors-published-list.

PCID-05

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

Response: Left blank in the workbook, marked not applicable by a START HERE scoping answer. Classification: Not applicable.

N/A - not applicable to Pallas because no cardholder data reaches Pallas systems; payment is handled directly by Stripe. REQU-06 on the START HERE worksheet is answered No, which marks this section not applicable.

Control inventory: data-classes-enumerated, subprocessors-published-list.

PCID-06

Are you classified as a service provider?

Response: Left blank in the workbook, marked not applicable by a START HERE scoping answer. Classification: Not applicable.

N/A - not applicable to Pallas because no cardholder data reaches Pallas systems; payment is handled directly by Stripe. REQU-06 on the START HERE worksheet is answered No, which marks this section not applicable.

Control inventory: data-classes-enumerated, subprocessors-published-list.

PCID-07

Are you on the list of Visa approved service providers?

Response: Left blank in the workbook, marked not applicable by a START HERE scoping answer. Classification: Not applicable.

N/A - not applicable to Pallas because no cardholder data reaches Pallas systems; payment is handled directly by Stripe. REQU-06 on the START HERE worksheet is answered No, which marks this section not applicable.

Control inventory: data-classes-enumerated, subprocessors-published-list.

PCID-08

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

Response: Left blank in the workbook, marked not applicable by a START HERE scoping answer. Classification: Not applicable.

N/A - not applicable to Pallas because no cardholder data reaches Pallas systems; payment is handled directly by Stripe. REQU-06 on the START HERE worksheet is answered No, which marks this section not applicable.

Control inventory: data-classes-enumerated, subprocessors-published-list.

PCID-09

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

Response: Left blank in the workbook, marked not applicable by a START HERE scoping answer. Classification: Not applicable.

N/A - not applicable to Pallas because no cardholder data reaches Pallas systems; payment is handled directly by Stripe. REQU-06 on the START HERE worksheet is answered No, which marks this section not applicable.

Control inventory: data-classes-enumerated, subprocessors-published-list.

PCID-10

What payment processors/gateways does the system support?

Response: Left blank in the workbook, marked not applicable by a START HERE scoping answer. Classification: Not applicable.

N/A - not applicable to Pallas because no cardholder data reaches Pallas systems; payment is handled directly by Stripe. REQU-06 on the START HERE worksheet is answered No, which marks this section not applicable.

Control inventory: data-classes-enumerated, subprocessors-published-list.

PCID-11

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

Response: Left blank in the workbook, marked not applicable by a START HERE scoping answer. Classification: Not applicable.

N/A - not applicable to Pallas because no cardholder data reaches Pallas systems; payment is handled directly by Stripe. REQU-06 on the START HERE worksheet is answered No, which marks this section not applicable.

Control inventory: data-classes-enumerated, subprocessors-published-list.

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: Left blank in the workbook, marked not applicable by a START HERE scoping answer. Classification: Not applicable.

N/A - not applicable to Pallas because no cardholder data reaches Pallas systems; payment is handled directly by Stripe. REQU-06 on the START HERE worksheet is answered No, which marks this section not applicable.

Control inventory: data-classes-enumerated, subprocessors-published-list.

OPEM-01

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

Response: Left blank in the workbook, marked not applicable by a START HERE scoping answer. Classification: Not applicable.

N/A - not applicable to Pallas because it requires no physical or virtual appliance in the institution's environment and no inbound firewall exception. REQU-07 on the START HERE worksheet is answered No, which marks this section not applicable.

Control inventory: network-perimeter-subprocessor-operated.

OPEM-02

Can your employees access customer systems remotely?

Response: Left blank in the workbook, marked not applicable by a START HERE scoping answer. Classification: Not applicable.

N/A - not applicable to Pallas because it requires no on-premises appliance and no inbound firewall exception. REQU-07 on the START HERE worksheet is answered No, which marks this section not applicable.

Control inventory: network-perimeter-subprocessor-operated.

OPEM-03

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?

Response: Left blank in the workbook, marked not applicable by a START HERE scoping answer. Classification: Not applicable.

N/A - not applicable to Pallas because it requires no on-premises appliance and no inbound firewall exception. REQU-07 on the START HERE worksheet is answered No, which marks this section not applicable.

Control inventory: network-perimeter-subprocessor-operated.

OPEM-04

Do you require remote management of the system?

Response: Left blank in the workbook, marked not applicable by a START HERE scoping answer. Classification: Not applicable.

N/A - not applicable to Pallas because it requires no on-premises appliance and no inbound firewall exception. REQU-07 on the START HERE worksheet is answered No, which marks this section not applicable.

Control inventory: network-perimeter-subprocessor-operated.

OPEM-05

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

Response: Left blank in the workbook, marked not applicable by a START HERE scoping answer.
Classification: Not applicable.

N/A - not applicable to Pallas because it requires no on-premises appliance and no inbound firewall exception. REQU-07 on the START HERE worksheet is answered No, which marks this section not applicable.

Control inventory: network-perimeter-subprocessor-operated.

OPEM-06

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

Response: Left blank in the workbook, marked not applicable by a START HERE scoping answer.
Classification: Not applicable.

N/A - not applicable to Pallas because it requires no on-premises appliance and no inbound firewall exception. REQU-07 on the START HERE worksheet is answered No, which marks this section not applicable.

Control inventory: network-perimeter-subprocessor-operated.

OPEM-07

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

Response: Left blank in the workbook, marked not applicable by a START HERE scoping answer.
Classification: Not applicable.

N/A - not applicable to Pallas because it requires no on-premises appliance and no inbound firewall exception. REQU-07 on the START HERE worksheet is answered No, which marks this section not applicable.

Control inventory: network-perimeter-subprocessor-operated.

OPEM-08

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

Response: Left blank in the workbook, marked not applicable by a START HERE scoping answer.
Classification: Not applicable.

N/A - not applicable to Pallas because it requires no on-premises appliance and no inbound firewall exception. REQU-07 on the START HERE worksheet is answered No, which marks this section not applicable.

Control inventory: network-perimeter-subprocessor-operated.

OPEM-09

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

Response: Left blank in the workbook, marked not applicable by a START HERE scoping answer. Classification: Not applicable.

N/A - not applicable to Pallas because it requires no on-premises appliance and no inbound firewall exception. REQU-07 on the START HERE worksheet is answered No, which marks this section not applicable.

Control inventory: network-perimeter-subprocessor-operated.

OPEM-10

Do you have existing higher education customers?

Response: Left blank in the workbook, marked not applicable by a START HERE scoping answer. Classification: Not applicable.

N/A - not applicable to Pallas because it requires no on-premises appliance and no inbound firewall exception. REQU-07 on the START HERE worksheet is answered No, which marks this section not applicable.

Control inventory: network-perimeter-subprocessor-operated.

AI (31 questions)

AIQU-01

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

Response: Left blank in the workbook, marked not applicable by a START HERE scoping answer. Classification: Not applicable.

N/A - not applicable to Pallas because it performs no machine learning processing and none is planned within the next 12 months. Accessibility findings are produced by deterministic rule evaluation in axe-core, and no model runtime, inference client, or AI provider SDK is present in either repository. REQU-04 on the START HERE worksheet is answered No, which marks this worksheet not applicable.

Control inventory: ai-no-model-processing.

AIQU-02

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

Response: Left blank in the workbook, marked not applicable by a START HERE scoping answer. Classification: Not applicable.

N/A - not applicable to Pallas because it uses no large language model. No model runtime, inference client, or AI provider SDK is present in either repository. REQU-04 on the START HERE worksheet is answered No, which marks this worksheet not applicable.

Control inventory: ai-no-model-processing.

AIGN-01

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

Response: Left blank in the workbook, marked not applicable by a START HERE scoping answer.
Classification: Not applicable.

N/A - not applicable to Pallas because it performs no AI or machine learning processing of any kind. REQU-04 is answered No, which marks this worksheet not applicable.

Control inventory: ai-no-model-processing.

AIGN-02

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

Response: Left blank in the workbook, marked not applicable by a START HERE scoping answer.
Classification: Not applicable.

N/A - not applicable to Pallas because it performs no AI or machine learning processing of any kind. REQU-04 is answered No, which marks this worksheet not applicable.

Control inventory: ai-no-model-processing.

AIGN-03

Have your staff completed responsible AI training?*

Response: Left blank in the workbook, marked not applicable by a START HERE scoping answer.
Classification: Not applicable.

N/A - not applicable to Pallas because it performs no AI or machine learning processing of any kind. REQU-04 is answered No, which marks this worksheet not applicable.

Control inventory: ai-no-model-processing.

AIGN-04

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

Response: Left blank in the workbook, marked not applicable by a START HERE scoping answer.
Classification: Not applicable.

N/A - not applicable to Pallas because it performs no AI or machine learning processing of any kind. REQU-04 is answered No, which marks this worksheet not applicable.

Control inventory: ai-no-model-processing.

AIGN-05

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

Response: Left blank in the workbook, marked not applicable by a START HERE scoping answer.
Classification: Not applicable.

N/A - not applicable to Pallas because it performs no AI or machine learning processing of any kind.

REQU-04 is answered No, which marks this worksheet not applicable.

Control inventory: ai-no-model-processing.

AIPL-01

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?*

Response: Left blank in the workbook, marked not applicable by a START HERE scoping answer.
Classification: Not applicable.

N/A - not applicable to Pallas because it performs no AI or machine learning processing of any kind. REQU-04 is answered No, which marks this worksheet not applicable.

Control inventory: ai-no-model-processing.

AIPL-02

Have you identified and measured AI risks?*

Response: Left blank in the workbook, marked not applicable by a START HERE scoping answer.
Classification: Not applicable.

N/A - not applicable to Pallas because it performs no AI or machine learning processing of any kind. REQU-04 is answered No, which marks this worksheet not applicable.

Control inventory: ai-no-model-processing.

AIPL-03

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

Response: Left blank in the workbook, marked not applicable by a START HERE scoping answer.
Classification: Not applicable.

N/A - not applicable to Pallas because it performs no AI or machine learning processing of any kind. REQU-04 is answered No, which marks this worksheet not applicable.

Control inventory: ai-no-model-processing.

AIPL-04

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

Response: Left blank in the workbook, marked not applicable by a START HERE scoping answer.
Classification: Not applicable.

N/A - not applicable to Pallas because it performs no AI or machine learning processing of any kind. REQU-04 is answered No, which marks this worksheet not applicable.

Control inventory: ai-no-model-processing.

AIPL-05

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

Response: Left blank in the workbook, marked not applicable by a START HERE scoping answer.
Classification: Not applicable.

N/A - not applicable to Pallas because it performs no AI or machine learning processing of any kind. REQU-04 is answered No, which marks this worksheet not applicable.

Control inventory: ai-no-model-processing.

AISC-01

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

Response: Left blank in the workbook, marked not applicable by a START HERE scoping answer.
Classification: Not applicable.

N/A - not applicable to Pallas because it performs no AI or machine learning processing of any kind. REQU-04 is answered No, which marks this worksheet not applicable.

Control inventory: ai-no-model-processing.

AISC-02

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

Response: Left blank in the workbook, marked not applicable by a START HERE scoping answer.
Classification: Not applicable.

N/A - not applicable to Pallas because it performs no AI or machine learning processing of any kind. REQU-04 is answered No, which marks this worksheet not applicable.

Control inventory: ai-no-model-processing.

AISC-03

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

Response: Left blank in the workbook, marked not applicable by a START HERE scoping answer.
Classification: Not applicable.

N/A - not applicable to Pallas because it performs no AI or machine learning processing of any kind. REQU-04 is answered No, which marks this worksheet not applicable.

Control inventory: ai-no-model-processing.

AISC-04

Please describe how you validate user inputs.

Response: Left blank in the workbook, marked not applicable by a START HERE scoping answer.

Classification: Not applicable.

N/A - not applicable to Pallas because it performs no AI or machine learning processing of any kind. REQU-04 is answered No, which marks this worksheet not applicable.

Control inventory: ai-no-model-processing.

AISC-05

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

Response: Left blank in the workbook, marked not applicable by a START HERE scoping answer.
Classification: Not applicable.

N/A - not applicable to Pallas because it performs no AI or machine learning processing of any kind. REQU-04 is answered No, which marks this worksheet not applicable.

Control inventory: ai-no-model-processing.

AIML-01

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

Response: Left blank in the workbook, marked not applicable by a START HERE scoping answer.
Classification: Not applicable.

N/A - not applicable to Pallas because it leverages no machine learning. AIQU-01 is answered not applicable and REQU-04 is answered No.

Control inventory: ai-no-model-processing.

AIML-02

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

Response: Left blank in the workbook, marked not applicable by a START HERE scoping answer.
Classification: Not applicable.

N/A - not applicable to Pallas because it leverages no machine learning. AIQU-01 is answered not applicable and REQU-04 is answered No.

Control inventory: ai-no-model-processing.

AIML-03

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

Response: Left blank in the workbook, marked not applicable by a START HERE scoping answer.
Classification: Not applicable.

N/A - not applicable to Pallas because it leverages no machine learning. AIQU-01 is answered not applicable and REQU-04 is answered No.

Control inventory: ai-no-model-processing.

AIML-04

Is your ML training data monitored and audited?

Response: Left blank in the workbook, marked not applicable by a START HERE scoping answer.
Classification: Not applicable.

N/A - not applicable to Pallas because it leverages no machine learning. AIQU-01 is answered not applicable and REQU-04 is answered No.

Control inventory: ai-no-model-processing.

AIML-05

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

Response: Left blank in the workbook, marked not applicable by a START HERE scoping answer.
Classification: Not applicable.

N/A - not applicable to Pallas because it leverages no machine learning. AIQU-01 is answered not applicable and REQU-04 is answered No.

Control inventory: ai-no-model-processing.

AIML-06

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

Response: Left blank in the workbook, marked not applicable by a START HERE scoping answer.
Classification: Not applicable.

N/A - not applicable to Pallas because it leverages no machine learning. AIQU-01 is answered not applicable and REQU-04 is answered No.

Control inventory: ai-no-model-processing.

AIML-07

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

Response: Left blank in the workbook, marked not applicable by a START HERE scoping answer.
Classification: Not applicable.

N/A - not applicable to Pallas because it leverages no machine learning. AIQU-01 is answered not applicable and REQU-04 is answered No.

Control inventory: ai-no-model-processing.

AIML-08

Do you watermark your ML training data?

Response: Left blank in the workbook, marked not applicable by a START HERE scoping answer.
Classification: Not applicable.

N/A - not applicable to Pallas because it leverages no machine learning. AIQU-01 is answered not applicable and REQU-04 is answered No.

Control inventory: ai-no-model-processing.

AILM-01

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

Response: Left blank in the workbook, marked not applicable by a START HERE scoping answer.
Classification: Not applicable.

N/A - not applicable to Pallas because it uses no large language model. AIQU-02 is answered not applicable and REQU-04 is answered No.

Control inventory: ai-no-model-processing.

AILM-02

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

Response: Left blank in the workbook, marked not applicable by a START HERE scoping answer.
Classification: Not applicable.

N/A - not applicable to Pallas because it uses no large language model. AIQU-02 is answered not applicable and REQU-04 is answered No.

Control inventory: ai-no-model-processing.

AILM-03

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

Response: Left blank in the workbook, marked not applicable by a START HERE scoping answer.
Classification: Not applicable.

N/A - not applicable to Pallas because it uses no large language model. AIQU-02 is answered not applicable and REQU-04 is answered No.

Control inventory: ai-no-model-processing.

AILM-04

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

Response: Left blank in the workbook, marked not applicable by a START HERE scoping answer.
Classification: Not applicable.

N/A - not applicable to Pallas because it uses no large language model. AIQU-02 is answered not applicable and REQU-04 is answered No.

Control inventory: ai-no-model-processing.

AILM-05

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

Response: Left blank in the workbook, marked not applicable by a START HERE scoping answer. Classification: Not applicable.

N/A - not applicable to Pallas because it uses no large language model. AIQU-02 is answered not applicable and REQU-04 is answered No.

Control inventory: ai-no-model-processing.

AILM-06

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

Response: Left blank in the workbook, marked not applicable by a START HERE scoping answer. Classification: Not applicable.

N/A - not applicable to Pallas because it uses no large language model. AIQU-02 is answered not applicable and REQU-04 is answered No.

Control inventory: ai-no-model-processing.

Privacy (65 questions)

PRGN-01

Does your solution process FERPA-related data?

Response: No. Classification: Implemented.

Pallas holds account identity for institutional users, organisation records, accessibility findings about institutional web properties, generated reports, and transiently uploaded source files. It does not receive or process student education records, so it does not process FERPA-regulated data in the ordinary course.

Control inventory: data-classes-enumerated.

PRGN-02

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

Response: Yes. Classification: Implemented.

GDPR-regulated personal data is processed where an institutional user is in the EEA or UK. PIPL-regulated data is not processed: Pallas neither collects from, processes in, nor stores in China. Transfers to the United States are covered by the published Standard Contractual Clauses and Transfer Impact Assessment.

Control inventory: gdpr-controller-split-documented, data-location-default-us, procurement-documentation-published.

PRGN-03

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

Response: Yes. Classification: Implemented.

Personal data regulated by state law, including CCPA and CPRA, is processed for users in those states. Any signed-in user can erase their own account, which serves the CCPA and CPRA right to delete alongside GDPR Article 17.

Control inventory: gdpr-art17-user-erasure, gdpr-art15-art20-user-export.

PRGN-04

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

Response: Yes. Classification: Implemented.

Users can upload source files for scanning, and those files are user-provided content whose contents Pallas does not control and may contain regulated information. They are held transiently: the default retention for uploaded source files is 7 days, and a scheduled purge removes them from Storage daily.

Control inventory: data-classes-enumerated, retention-per-org-policies, retention-source-file-purge.

PRGN-05

Web Link to Product/Service Privacy Notice

Response: https://pallas.lonia.ai/privacy. Classification: Informational.

The privacy notice is published alongside a cookie policy at pallas.lonia.ai/legal/cookies, a Data Processing Agreement, a Data Protection Impact Assessment, a Transfer Impact Assessment, and the EU Standard Contractual Clauses.

Control inventory: gdpr-controller-split-documented, procurement-documentation-published.

PCOM-01

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?*

Response: No. Classification: Implemented.

Pallas has had no personal data breach requiring notification to a governmental agency, to individuals, or to another organisation. The commitment if one occurs is notification to affected customers without undue delay and within 72 hours of awareness, with authority notification on the same timetable. This is an operator statement about incident history and is not independently attested.

Control inventory: incident-72-hour-notification, incident-authority-notification.

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: Privacy is enforced in the schema rather than only in the policy text. Pallas distinguishes the two controller roles: Lonia AI is controller for user account data, and the institution is controller for the data it brings. Any signed-in user can export the personal data Pallas holds about them across every organisation they belong to, and can erase their own account. An organisation administrator can export the full

organisation data set for a subject access request and can delete the organisation, which cancels the subscription, wipes Storage under the organisation prefix, and removes the organisation's rows. Retention is configured per organisation with defaults of 365 days for scan data, 7 days for uploaded source files, and 730 days for reports, and the sweep issues real DELETE statements rather than storing a preference. Erasure of a user does not destroy audit attribution, because actor name and email are snapshotted onto the audit row at write time.. Classification: Informational.

The gaps are stated with the same specificity: there is no dedicated privacy office, no privacy awareness training programme, no data protection officer, and no privacy framework certification. Those are answered individually at PCOM-04, PRPO-06, PRPO-07, INTL-02, and PDOC-02.

Control inventory: gdpr-controller-split-documented, gdpr-art15-art20-user-export, gdpr-art17-user-erasure, gdpr-org-dsar-export, gdpr-org-deletion, retention-per-org-policies, retention-deletion-actually-deletes, audit-actor-attribution-survives-erasure.

PCOM-03

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

Response: No. Classification: Implemented.

There have been no violations of internal privacy policy or applicable privacy law in the past 36 months. This is an operator statement about history and is not independently attested.

Control inventory: incident-72-hour-notification.

PCOM-04

Do you have a dedicated data privacy staff or office?

Response: No. Classification: Gap, disclosed.

There is no dedicated data privacy staff or office. Data protection correspondence is handled at support@lonia.ai by the operator.

Control inventory: personnel-no-formal-screening-program.

PDOC-01

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

Response: N/A. Classification: Not applicable.

N/A - not applicable to Pallas because it has not completed a SOC 2 audit of any kind, so there is no report in which a Privacy Trust Service Principle could be included.

Control inventory: vuln-no-independent-certification.

PDOC-02

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

Response: No. Classification: Gap, disclosed.

Pallas asserts no conformance to the NIST Privacy Framework, ISO 27701, or an equivalent. GDPR-aligned practice is documented in the published Data Processing Agreement, Data Protection Impact Assessment, and Transfer Impact Assessment, but documentation is not framework certification and is not offered as one.

Control inventory: vuln-no-independent-certification, procurement-documentation-published.

PDOC-03

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

Response: No. Classification: Gap, disclosed.

There is no onboarding and offboarding policy, and therefore no security or privacy training embedded in one.

Control inventory: personnel-no-formal-screening-program.

PTHP-01

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

Response: Yes. Classification: Implemented.

Each subprocessor is engaged under that provider's published data processing terms, which carry the provider's regulatory commitments. The full list with purpose, data categories, processing location, and published certifications is published, and a new subprocessor is published with 30 days advance notice before it processes any customer data.

Control inventory: subprocessors-published-list, subprocessors-change-notice.

PTHP-02

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?

Response: No. Classification: Gap, disclosed.

Pallas performs no privacy impact assessment of its subprocessors. It relies on the certifications each provider publishes. The published Data Protection Impact Assessment covers Pallas processing rather than per-subprocessor assessment.

Control inventory: subprocessors-certifications-are-theirs, procurement-documentation-published.

PCHG-01

Does your change management process include privacy review and approval?

Response: Yes. Classification: Compensating control.

The release chain enforces a privacy checkpoint mechanically rather than procedurally: a freshness gate fails the build if a published privacy instrument, meaning the Data Processing Agreement, Data Protection Impact Assessment, Transfer Impact Assessment, or Standard Contractual Clauses, no longer matches the control

inventory it was generated from. A change that alters a privacy-relevant control therefore cannot ship without the privacy documentation being regenerated. There is no separate human privacy approval step.

Control inventory: appsec-release-gate-fails-closed, procurement-documentation-published.

PCHG-02

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

Response: No. Classification: Gap, disclosed.

There is no documented privacy risk register or documented procedure for mitigating a privacy risk while it remains open. The equivalent discipline exists for security dependency advisories, where reachability triage is recorded with a review date, but no equivalent artifact exists on the privacy side.

Control inventory: vuln-advisory-triage-artifact.

PDAT-01

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

Response: No. Classification: Implemented.

Pallas collects no demographic information. The data classes it holds are enumerated in the control inventory and do not include age, race, gender, or comparable attributes.

Control inventory: data-classes-enumerated.

PDAT-02

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

Response: No. Classification: Implemented.

Pallas captures and creates no genetic, biometric, or behaviometric information. There is no facial recognition, fingerprint capture, or behavioural profiling anywhere in the product.

Control inventory: data-classes-enumerated.

PDAT-03

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

Response: No. Classification: Implemented.

Pallas does not combine institutional data with personal data from other sources. Organisation data is isolated by Row-Level Security on every table, with policies resolving membership through SECURITY DEFINER helpers rather than through a client-supplied identifier, so cross-organisation combination is prevented structurally rather than by policy alone.

Control inventory: data-classes-enumerated, tenant-rls-every-table, tenant-org-scoping-helpers.

PDAT-04

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

Response: Yes. Classification: Implemented.

The default processing location is the United States, so data from an institution outside the United States enters it. Supabase hosts the database and Storage in us-east-1. Transfers out of the EEA and the UK are covered by the published Standard Contractual Clauses and the Transfer Impact Assessment. No European Union hosting exists and none is offered.

Control inventory: data-location-default-us, data-location-eu-option, procurement-documentation-published.

PDAT-05

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

Response: Yes. Classification: Compensating control.

IP address is processed transiently for abuse prevention: unauthenticated marketing endpoints carry a per-IP burst cap, and every unauthenticated write endpoint verifies a Cloudflare Turnstile token and refuses the request when verification fails. MAC addresses are not collected. Marketing suppression is keyed on a hash of the email address rather than the address itself.

Control inventory: access-rate-limiting-anonymous, access-turnstile-fails-closed, subscriber-suppression-list.

PDAT-06

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

Response: No. Classification: Implemented.

There are no advertising cookies and no analytics or tracking cookies, and no web-tracking pixels. Cookie use is limited to essential technologies, as documented at pallas.lonia.ai/legal/cookies. Because there is no tracking, there is nothing to opt out of for tracking purposes.

Control inventory: procurement-documentation-published, subscriber-consent-recorded.

PDAT-07

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

Response: Yes. Classification: Compensating control.

Server-side operator functions run under service credentials that bypass Row-Level Security by necessity, so operator access to institutional data is possible. The scope of those functions is documented rather than hidden, and every administrative action appends to a tamper-evident audit chain the operator cannot silently alter. Subprocessors also hold the data they process, as published on the subprocessor list.

Control inventory: tenant-service-role-bypass-disclosed, audit-sha256-ledger, audit-ledger-append-only, subprocessors-published-list.

PDAT-08

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

Response: Yes. Classification: Implemented.

Pallas commits to handling personal data in accordance with applicable law and institutional policy, on the terms set out in the published Data Processing Agreement. The controller split is enforced in the schema rather than asserted only in the policy text.

Control inventory: gdpr-controller-split-documented, procurement-documentation-published.

PRPO-01

Do you have a documented privacy management process?

Response: Yes. Classification: Implemented.

The privacy management position is documented across a published Data Processing Agreement, Data Protection Impact Assessment, Transfer Impact Assessment, and Standard Contractual Clauses, each generated from the control inventory and gated against drift on every release. This is documented process, not audited process; no document in the set carries independent assurance.

Control inventory: procurement-documentation-published, gdpr-controller-split-documented.

PRPO-02

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

Response: Yes. Classification: Implemented.

Privacy properties are structural rather than configured after the fact: Row-Level Security on every table from creation, retention that issues real DELETE statements rather than storing a preference, self-service erasure for any signed-in user, and audit attribution that survives that erasure by snapshotting actor name and email at write time.

Control inventory: tenant-rls-every-table, retention-deletion-actually-deletes, gdpr-art17-user-erasure, audit-actor-attribution-survives-erasure.

PRPO-03

Will you comply with applicable breach notification laws?

Response: Yes. Classification: Implemented.

Pallas notifies affected customers without undue delay and within 72 hours of becoming aware of a breach affecting their data, and notifies the relevant supervisory authority on the same timetable, following the jurisdiction.

Control inventory: incident-72-hour-notification, incident-authority-notification.

PRPO-04

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

Response: Yes. Classification: Implemented.

Pallas commits to the institution's privacy and data protection policies on the terms agreed in the institutional agreement, and supports them operationally through the organisation subject access export and organisation deletion paths.

Control inventory: gdpr-controller-split-documented, gdpr-org-dsar-export, gdpr-org-deletion.

PRPO-05

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

Response: Yes. Classification: Implemented.

Pallas accepts the laws and regulations of the institution's region as set out in the published Data Processing Agreement, and its authority notification routing follows the jurisdiction rather than defaulting to a single regulator.

Control inventory: incident-authority-notification, procurement-documentation-published.

PRPO-06

Do you have a privacy awareness/training program?*

Response: No. Classification: Gap, disclosed.

There is no privacy awareness or training programme. This is published as not yet formalised rather than answered from intent.

Control inventory: personnel-no-formal-screening-program.

PRPO-07

Is privacy awareness training mandatory for all employees?

Response: No. Classification: Gap, disclosed.

There is no mandatory privacy training for personnel and no training record.

Control inventory: personnel-no-formal-screening-program.

PRPO-08

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

Response: N/A. Classification: Not applicable.

N/A - not applicable to Pallas because no personnel work with AI. Pallas performs no artificial intelligence or machine learning processing, so there is no population for AI privacy and ethics training to cover.

Control inventory: ai-no-model-processing, personnel-no-formal-screening-program.

PRPO-09

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

Response: No. Classification: Implemented.

Pallas has no automated decision-making about people. Automated processing evaluates web pages against accessibility rules and produces findings about those pages, not decisions about individuals, and it has no legal or similarly significant effect on any person. No profiling is performed and no model is involved.

Control inventory: ai-no-model-processing, scan-single-page-static-only.

PRPO-10

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

Response: N/A. Classification: Not applicable.

N/A - not applicable to Pallas because it performs no automated decision-making about individuals, as answered at PRPO-09, so there is no automated decision process to validate, monitor, or handle data subject objections against.

Control inventory: ai-no-model-processing.

PRPO-11

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

Response: Yes. Classification: Implemented.

The position on government and law enforcement access is documented in the published Transfer Impact Assessment, which sets out the approach to access requests, including the commitment to require lawful process, to challenge requests that are overbroad or unlawful, and to notify the affected customer wherever notification is lawfully permitted.

Control inventory: procurement-documentation-published, gdpr-controller-split-documented.

PRPO-12

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

Response: No. Classification: Implemented.

Pallas does not disclose institutional data to law enforcement without valid legal process. Lawful process is required, overbroad or unlawful requests are challenged, and the affected customer is notified wherever notification is lawfully permitted.

Control inventory: procurement-documentation-published, gdpr-controller-split-documented.

PRPO-13

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

Response: No. Classification: Gap, disclosed.

There is no incident response team, and therefore no privacy analyst or privacy officer within one. Incident handling is performed by the operator, who also handles data protection correspondence at support@lonia.ai.

Control inventory: personnel-no-formal-screening-program, incident-72-hour-notification.

INTL-01

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

Response: No. Classification: Implemented.

Data is not collected in, processed in, or stored in the EEA. The default and only processing location is the United States, with Supabase hosting the database and Storage in us-east-1. Personal data of EEA data subjects is transferred to the United States under the published Standard Contractual Clauses. No European Union hosting exists and none is offered.

Control inventory: data-location-default-us, data-location-eu-option, procurement-documentation-published.

INTL-02

Do you have a data protection officer (DPO)?

Response: No. Classification: Gap, disclosed.

No data protection officer has been appointed. Pallas does not meet the GDPR Article 37 mandatory appointment criteria at its current scale, and has chosen not to appoint one voluntarily. Data protection correspondence is handled at support@lonia.ai.

Control inventory: personnel-no-formal-screening-program.

INTL-03

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

Response: Yes. Classification: Implemented.

Pallas publishes the EU Standard Contractual Clauses rather than supplying them on request, reproduced verbatim from the Annex to Commission Implementing Decision (EU) 2021/914 with Module Two selected. The UK International Data Transfer Addendum is not yet issued alongside them; a UK buyer should treat it as an open item to be executed with the Clauses. A signable render carrying the executing party block and signature lines is provided on request.

Control inventory: procurement-documentation-published, gdpr-controller-split-documented.

INTL-04

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

Response: No. Classification: Implemented.

No data is collected from, processed in, or stored in China. The default and only processing location is the United States.

Control inventory: data-location-default-us.

INTL-05

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

Response: N/A. Classification: Not applicable.

N/A - not applicable to Pallas because it performs no processing in China and stores no data there, so PIPL security, privacy, and data localisation requirements do not attach.

Control inventory: data-location-default-us.

DRPV-01

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

Response: Yes. Classification: Implemented.

A Data Protection Impact Assessment is published rather than held internally. It is generated from the control inventory and gated against drift on every release, so it cannot silently fall out of step with the controls it describes.

Control inventory: procurement-documentation-published.

DRPV-02

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?

Response: Yes. Classification: Implemented.

A privacy notice is published at pallas.lonia.ai/privacy identifying the purposes for which personal information is collected, used, retained, and disclosed, alongside a cookie policy and the published Data Processing Agreement.

Control inventory: gdpr-controller-split-documented, procurement-documentation-published.

DRPV-03

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?

Response: Yes. Classification: Implemented.

Marketing list membership records the source of the signup and the moment consent was given alongside the enrolment timestamp, so consent is evidenced rather than assumed. The unsubscribe route is dispatched ahead of the CORS, method, and bot-verification checks, so a misconfigured gate cannot make withdrawal of consent unreachable.

Control inventory: subscriber-consent-recorded, subscriber-unsubscribe-always-reachable, gdpr-controller-split-documented.

DRPV-04

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?

Response: Yes. Classification: Implemented.

The data classes Pallas holds are enumerated in the control inventory and are limited to what the service requires. The controller split is enforced in the schema, so data the institution brings is held under the institution's purposes rather than merged into Lonia AI's own.

Control inventory: data-classes-enumerated, gdpr-controller-split-documented.

DRPV-05

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

Response: Yes. Classification: Implemented.

The data classes are enumerated in src/data/control-inventory.ts, which is the single source the published privacy documents are generated from, so the list a buyer reads and the list the engineering team maintains cannot diverge without failing the release.

Control inventory: data-classes-enumerated, procurement-documentation-published.

DRPV-06

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?

Response: Yes. Classification: Implemented.

Retention is configured per organisation with defaults of 365 days for scan data, 7 days for uploaded source files, and 730 days for reports. A scheduled job applies those policies daily and issues real DELETE statements rather than storing a preference. Archived audit events past their window are purged nightly, and each purge run is logged.

Control inventory: retention-per-org-policies, retention-daily-sweep, retention-deletion-actually-deletes, retention-audit-purge.

DRPV-07

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

Response: Yes. Classification: Implemented.

Any signed-in user can export the personal data Pallas holds about them across every organisation they belong to, and can erase their own account. Both functions are callable only by the service role, with the acting user id derived from a verified session rather than accepted from the client.

Control inventory: gdpr-art15-art20-user-export, gdpr-art17-user-erasure, gdpr-rights-service-role-only.

DRPV-08

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?

Response: Yes. Classification: Implemented.

Personal information is disclosed only to the subprocessors published on the subprocessor list, each for the purpose stated there. A new subprocessor is published with 30 days advance notice before it processes any customer data.

Control inventory: subprocessors-published-list, subprocessors-change-notice.

DRPV-09

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

Response: Yes. Classification: Implemented.

Logical protection is enforced in the database: Row-Level Security on every application table, private per-organisation Storage buckets, TLS 1.3 in transit, and AES-256 at rest. Physical protection is a Supabase and Cloudflare facility control that Pallas relies on and cannot itself demonstrate.

Control inventory: tenant-rls-every-table, tenant-storage-per-org, encryption-in-transit, encryption-at-rest, physical-security-subprocessor-operated.

DRPV-10

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

Response: Yes. Classification: Implemented.

Users can review and correct the personal data held about them through the export and account paths, which is the mechanism by which accuracy is maintained. Data minimisation limits what is held in the first place to the enumerated classes.

Control inventory: gdpr-art15-art20-user-export, data-classes-enumerated.

DRPV-11

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

Response: Yes. Classification: Implemented.

Privacy complaints are handled at support@lonia.ai, and the published documentation sets out the escalation route to the relevant supervisory authority, including the right to lodge a complaint with that authority directly.

Control inventory: procurement-documentation-published, incident-authority-notification.

DRPV-12

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

Response: Yes. Classification: Compensating control.

Two specific masking measures are implemented rather than a general anonymisation programme: the marketing suppression list is keyed on a hash of the email address rather than the address itself, so a withdrawn address is honoured without being retained in the clear; and lawful removal of an audit row appends a redaction entry recording that the removal happened rather than exposing the removed content. Pallas does not otherwise produce anonymised or de-identified data sets.

Control inventory: subscriber-suppression-list, audit-lawful-redaction-recorded.

DRPV-13

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)?

Response: No. Classification: Implemented.

Neither Pallas nor its subprocessors use masked or de-identified data for any purpose beyond providing the service. There is no sharing with ad networks or data brokers, no marketing use of institutional data, no profile creation, and no analytics unrelated to the service provided to the institution.

Control inventory: subprocessors-published-list, data-classes-enumerated.

DRPV-14

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

Response: Yes. Classification: Compensating control.

For Pallas processing, a stop-processing request is honoured by mechanisms that actually delete: user erasure, organisation deletion which wipes Storage under the organisation prefix and removes the organisation's rows, and a retention sweep that issues real DELETE statements. Propagation to subprocessors is contractual, resting on each provider's data processing terms, and Pallas cannot technically verify a provider's execution of it. Certification is therefore given for Pallas processing and asserted contractually for subprocessor processing.

Control inventory: gdpr-art17-user-erasure, gdpr-org-deletion, retention-deletion-actually-deletes, subprocessors-published-list.

DRPV-15

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

Response: No. Classification: Gap, disclosed.

There is no formal ethics review stage in the code review process. The release chain enforces type safety, security and validation unit tests, accessibility conformance, and documentation freshness, none of which is an ethics review and none of which is offered as one.

Control inventory: appsec-release-gate-fails-closed.

DPAI-01

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

Response: No. Classification: Implemented.

Pallas uses no artificial intelligence for the processing of institutional data. Accessibility findings are produced by deterministic rule evaluation in axe-core, and no model runtime, inference client, or AI provider SDK is present in either repository.

Control inventory: ai-no-model-processing.

DPAI-02

Is any institutional data retained in AI processing?*

Response: N/A. Classification: Not applicable.

N/A - not applicable to Pallas because there is no AI processing in which institutional data could be retained. DPAI-01 is answered No.

Control inventory: ai-no-model-processing.

DPAI-03

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

Response: N/A. Classification: Not applicable.

N/A - not applicable to Pallas because neither Pallas nor any published subprocessor processes institutional data with AI, so there is no AI-specific term for such an agreement to carry. Subprocessor data protection terms are in place generally and are answered at PTHP-01.

Control inventory: ai-no-model-processing, subprocessors-published-list.

DPAI-04

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

Response: N/A. Classification: Not applicable.

N/A - not applicable to Pallas because no published subprocessor processes institutional data through an AI service on Pallas's behalf. The subprocessor set is Supabase, Cloudflare, Stripe, and Resend, each engaged for the purpose published on the subprocessor list.

Control inventory: ai-no-model-processing, subprocessors-published-list.

DPAI-05

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

Response: N/A. Classification: Not applicable.

N/A - not applicable to Pallas because there is no AI processing to be licensed, commercial or otherwise.

Control inventory: ai-no-model-processing.

DPAI-06

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

Response: N/A. Classification: Not applicable.

N/A - not applicable to Pallas because institutional data is not used or processed by any AI service, shared or dedicated.

Control inventory: ai-no-model-processing.

DPAI-07

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

Response: N/A. Classification: Not applicable.

N/A - not applicable to Pallas because there is no AI query path against which safeguards would be needed. The safeguard that does exist is structural: no model, inference client, or AI provider SDK is present in either repository, so there is no code path by which institutional data could reach one.

Control inventory: ai-no-model-processing.

DPAI-08

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

Response: N/A. Classification: Not applicable.

N/A - not applicable to Pallas because there is no AI use to opt out of.

Control inventory: ai-no-model-processing.

10. Control inventory rows cited

Every row named above, rendered from the inventory with its implementation status, its evidence basis, and its disclosure text unaltered.

An organisation cannot be left without an administrator. Removing or demoting the last org_admin is refused at the database layer.

> Control access-last-admin-guard. Status: Implemented. Backed by a file in the pallas-app repository, verified read-only on 2026-08-30, not gated from the marketing repository.
>
> Implementation. app: pallas_guard_last_admin, migration 010:106, rebuilt 025:162.
>
> Verification. app: supabase/migrations/015_drop_duplicate_last_admin_trigger.sql.

Organisation membership carries one of four roles: org_admin, manager, contributor, viewer. Read is available to any member; write and update require contributor or above; delete requires org_admin.

> Control access-org-roles. Status: Implemented. Backed by a file in the pallas-app repository, verified read-only on 2026-08-30, not gated from the marketing repository.

Implementation. app: pallas_organization_users.role, migration 001:30; app: supabase/migrations/020_storage_bucket_rls.sql, role model section.

Verification. app: pallas_user_org_role, migration 002:17 hardened 031:68.

Unauthenticated marketing endpoints are rate limited. The newsletter and resource gate endpoint carries a per-IP burst ceiling of 12 per 60 seconds and a per-email burst ceiling of 5 per 60 seconds, keyed on the normalised address; the anonymous checkout endpoint carries 5 per 60 seconds.

Control access-rate-limiting-anonymous. Status: Partial. Demonstrated in the pallas-marketing repository and checked by a release gate.

Disclosure. The Cloudflare native rate limiting binding supports a 10 second or 60 second period only. The email gate therefore carries per-IP and per-email burst ceilings and nothing else: there is no daily global signup ceiling on that endpoint and none is claimed. What bounds abuse there is the Turnstile gate plus the unique constraint on (email, source) in pallas_subscribers, which makes a repeat submission of the same pair produce no new row. A daily ceiling would require a Durable Object binding the operator has not provisioned.

Implementation. marketing: workers/pallas-email-gate/wrangler.toml, native SIGNUP_RATE_LIMIT binding, 12 per 60 seconds; marketing: workers/pallas-email-gate/wrangler.toml, native SIGNUP_EMAIL_RATE_LIMIT binding, 5 per 60 seconds, keyed on the trimmed and lowercased email; the Worker refuses with a 500 if either binding is absent; app: workers/pallas-checkout/wrangler.toml, native PURCHASE_LIMITER binding, 5 per 60 seconds, Worker returns 503 if the binding is absent.

Verification. marketing: tests/email-gate.test.ts.

Every unauthenticated write endpoint verifies a Cloudflare Turnstile token and refuses the request when the verification secret is unset, rather than running with the bot gate off.

Control access-turnstile-fails-closed. Status: Implemented. Demonstrated in the pallas-marketing repository and checked by a release gate.

Implementation. marketing: src/lib/turnstile.ts; marketing: pallas-scan-email and pallas-email-gate, both returning 500 when TURNSTILE_SECRET_KEY is unset.

Verification. marketing: tests/turnstile.test.ts; marketing: scripts/test-turnstile.mjs.

Pallas performs no artificial intelligence or machine learning processing on any data. Accessibility findings are produced by deterministic rule evaluation in axe-core, and no model, inference service, or AI provider is present in either repository.

Control ai-no-model-processing. Status: Implemented. Backed by a file in the pallas-app repository, verified read-only on 2026-08-30, not gated from the marketing repository.

Disclosure. The absence of an AI dependency is demonstrable in both repositories by inspection of the dependency sets, and that is the strongest form this claim takes. It is a statement about what is installed, not a runtime proof that no network call ever reaches a third-party model, which no dependency list can establish. A buyer whose control requires attested absence of model processing should ask for it contractually; the answers to the AI worksheet rest on this row and on nothing stronger than it.

Implementation. marketing: package.json dependency set: astro and axe-core at runtime, with no model runtime, inference client, or AI provider SDK; app: package.json dependency set: @supabase/supabase-js, axe-core, pdf-lib, jszip, react and react-router-dom, with no model runtime, inference client, or AI provider SDK.

Verification. marketing: scripts/test-a11y.mjs.

Untrusted content is escaped before it reaches HTML or email. The only place untrusted input meets raw HTML on the marketing site is JSON-LD, fed exclusively by a serializer that escapes the closing angle bracket and the U+2028 and U+2029 line separators.

Control appsec-output-escaping. Status: Implemented. Demonstrated in the pallas-marketing repository and checked by a release gate.

Implementation. marketing: src/lib/jsonld.ts, serializeJsonLd(); marketing: src/lib/html-escape.ts; marketing: src/lib/safe-url.ts.

Verification. marketing: tests/safe-url.test.ts and tests/scan-report.test.ts; marketing: SECURITY_ADVISORY_TRIAGE.md, section titled The one place untrusted input meets HTML.

The build command itself runs every gate: a type check, the typography and published-document freshness checks, the six written-claim verification gates, the unit test suite over the security and validation code, the build, an automated accessibility test against every built page, a Turnstile configuration check against the built artifact, and a sweep of the built output for forbidden claims. The hosting platform runs that command on every push, so a non-zero exit at any step fails the build and nothing deploys; the failing guards remove the dist directory so a failed build leaves nothing to deploy.

Control appsec-release-gate-fails-closed. Status: Implemented. Demonstrated in the pallas-marketing repository and checked by a release gate.

Implementation. marketing: package.json, the build script.

Verification. marketing: scripts/test-a11y.mjs, scripts/test-turnstile.mjs, scripts/check-dashes.mjs, scripts/verify-doc-artifact-freshness.mjs.

Fetched third-party responses are capped at 10 MB, enforced against the declared Content-Length and again against the bytes actually received.

Control appsec-response-cap. Status: Implemented. Demonstrated in the pallas-marketing repository and checked by a release gate.

Implementation. marketing: src/lib/response-cap.ts; app: workers/pallas-cors-proxy/src/index.ts:261, MAX_RESPONSE_BYTES.

Verification. marketing: tests/response-cap.test.ts.

Scanned third-party markup renders on a dedicated origin with nothing in its storage, pinned shut with Content-Security-Policy, so retrieved markup cannot reach the application session, cookies, or IndexedDB.

Control appsec-sandboxed-rendering. Status: Implemented. Backed by a file in the pallas-app repository, verified read-only on 2026-08-30, not gated from the marketing repository.

Implementation. app: workers/pallas-scanner-sandbox/src/index.ts.

Verification. app: docs/OPERATOR_ACTIONS.md section 1.1, mitigations table.

The public scan tool validates every submitted URL against a hostname and IP-literal denylist before fetching it, blocking loopback, link-local, unique-local, IPv4-mapped private addresses, cloud metadata endpoints, and the private, CGNAT, and multicast IPv4 ranges.

Control appsec-ssrf-guard. Status: Implemented. Demonstrated in the pallas-marketing repository and checked by a release gate.

Implementation. marketing: src/lib/ssrf-guard.ts; app: workers/pallas-cors-proxy/src/index.ts, isBlockedHost and isBlockedIpv4.

Verification. marketing: tests/ssrf-guard.test.ts.

Audit action names are validated against a registry table rather than accepted as free text, so an unrecognised action cannot be written.

Control audit-action-registry. Status: Implemented. Backed by a file in the pallas-app repository, verified read-only on 2026-08-30, not gated from the marketing repository.

Implementation. app: pallas_audit_action_registry, created migration 024:143, RLS enabled 024:164; app: pallas_assert_audit_action, migration 024:431.

Verification. app: supabase/migrations/043_audit_action_registry_documentation.sql.

Audit attribution survives user erasure. Actor name and email are snapshotted onto the audit row at write time, so severing the identity link under Article 17 does not orphan the audit trail.

Control audit-actor-attribution-survives-erasure. Status: Implemented. Backed by a file in the pallas-app repository, verified read-only on 2026-08-30, not gated from the marketing repository.

Implementation. app: pallas_actor_snapshot 024:379, pallas_fill_audit_actor_snapshot 040:195; app: supabase/migrations/040_user_fk_set_null.sql.

Verification. app: migration 041, whose update allowlist requires actor_name_snapshot and actor_email_snapshot unchanged.

Attempts to modify or delete an audit event are refused with specific error codes: PA030 for update, PA031 for delete, PA032 for forged chain metadata on insert.

Control audit-error-codes. Status: Implemented. Observed in the production database by catalog query on 2026-09-16 and recorded in the pallas-app deployed-objects manifest. The migration that created the object is held out of the repository as a trade secret, so the observation, not a file, is the evidence; objects are cited by name only.

Implementation. app: migration 041, immutability triggers on pallas_audit_events.

Verification. marketing: src/pages/trust.astro, Security posture, Audit trail.

Lawful removal of an audit row, whether under a retention policy or under GDPR Article 17, appends a redaction entry recording the sequence number, the hash before, the hash after, the reason, and the timestamp. The ledger outlives the row it describes, so a reviewer can distinguish a lawful purge from a concealment.

Control audit-lawful-redaction-recorded. Status: Implemented. Observed in the production database by catalog query on 2026-09-16 and recorded in the pallas-app deployed-objects manifest. The migration that created the object is held out of the repository as a trade secret, so the observation, not a file, is the evidence; objects are cited by name only.

Disclosure. The delete allowlist is a declaration, not an authorisation control. Anything holding service_role and a SQL connection can set the redaction reason. The control is not that setting it is hard; the control is that setting it does not buy silence, because the redaction entry lands in a table that role cannot subsequently edit or truncate. An audit row can be deleted. It cannot be deleted quietly. This distinction is stated here because a reviewer will press on it, and a document that presented the flag as an access control would be overclaiming.

Implementation. app: pallas_audit_delete_reason_allowed, migration 041; the redaction hash is computed inside the same migration; app: update and delete triggers on pallas_audit_events, migration 041.

Verification. app: migration 041, which carries the update and delete allowlists.

The ledger table is append-only in the strong sense: Row-Level Security is enabled with zero policies, and INSERT, UPDATE, DELETE, and TRUNCATE are revoked from every role including service_role. Only SECURITY DEFINER trigger functions can write to it.

Control audit-ledger-append-only. Status: Implemented. Observed in the production database by catalog query on 2026-09-16 and recorded in the pallas-app deployed-objects manifest. The migration that created the object is held out of the repository as a trade secret, so the observation, not a file, is the evidence; objects are cited by name only.

Implementation. app: pallas_audit_chain, created by migration 041 with Row-Level Security enabled; app: SECURITY DEFINER trigger functions inside migration 041.

Verification. app: pallas_audit_chain, migration 041; the table answers permission denied to the anon role through the API.

Audit rows carry a seven-year (2555 day) retention floor enforced by a database CHECK constraint. An administrator cannot configure a shorter audit retention than the regulatory minimum.

Control audit-seven-year-floor. Status: Implemented. Backed by a file in the pallas-app repository, verified read-only on 2026-08-30, not gated from the marketing repository.

Implementation. app: chk_audit_log_retention_min_2555 on pallas_retention_policies, migration 016:34; app: pallas_apply_retention_policies, migration 042.

Verification. app: supabase/migrations/016_audit_retention_floor_check.sql.

Every audit event appends an entry to a SHA-256 hash chain. Each entry is hashed together with the previous entry hash, so modification, deletion, or reordering of historical events breaks the chain and is detectable.

Control audit-sha256-ledger. Status: Implemented. Observed in the production database by catalog query on 2026-09-16 and recorded in the pallas-app deployed-objects manifest. The migration that created the object is held out of the repository as a trade secret, so the observation, not a file, is the evidence; objects are cited by name only.

Implementation. app: supabase/migrations/041_audit_tamper_evidence.sql; app: hashing helpers inside migration 041; row_hash and prev_row_hash columns on pallas_audit_events; app: insert trigger on pallas_audit_events, migration 041.

Verification. app: pallas_verify_audit_chain, migration 041; app: pallas_verify_audit_row, migration 041.

No authentication state, entitlement, or quota is trusted from browser storage. Authorisation decisions are made server side.

Control auth-no-browser-storage-for-entitlements. Status: Implemented. Backed by a file in the pallas-app repository,

verified read-only on 2026-08-30, not gated from the marketing repository.

Implementation. app: Row-Level Security policies on every pallas_ table, enumerated in the tenant-isolation rows below; app: pallas-app-api.

Verification. marketing: Rule sweep for browser storage API calls across src/.

Pallas authenticates users through Google and Microsoft OAuth only. It stores no passwords, offers no password login, and has no password reset flow.

Control auth-oauth-only. Status: Implemented. Backed by a file in the pallas-app repository, verified read-only on 2026-08-30, not gated from the marketing repository.

Implementation. app: src/contexts/AuthContext.tsx:172 and :181; app: src/pages/Onboarding.tsx:123.

Verification. app: Search src/ for signInWithPassword and signUp(.

The trigger that provisions a Pallas profile on first sign-in cannot block a sign-in if it fails.

Control auth-profile-trigger-fail-safe. Status: Implemented. Backed by a file in the pallas-app repository, verified read-only on 2026-08-30, not gated from the marketing repository.

Implementation. app: handle_pallas_new_user, migration 001:105, corrected in 003 and 021:260.

Verification. app: supabase/migrations/021_reconcile_live_state.sql section 5.

Sessions are JWT-based through Supabase Auth, and refresh tokens rotate on use.

Control auth-session-jwt. Status: Implemented. A statement by a subprocessor. Pallas configures and relies on it; no Pallas code implements it and neither Pallas repository can demonstrate it.

Disclosure. Token rotation behaviour is a property of Supabase Auth. Pallas configures it and relies on it; no Pallas code implements it, and neither Pallas repository can demonstrate it independently.

Implementation. vendor: Supabase Auth refresh token rotation.

Verification. marketing: src/pages/trust.astro, Security posture, Session security.

Pallas does not publish a recovery time objective or a recovery point objective.

Control backup-no-published-rto-rpo. Status: Not implemented. A commitment the operator makes contractually. No code enforces it.

Disclosure. No RTO or RPO is published, because a number that cannot be evidenced from a restore test is worth nothing on a questionnaire. No restore test has been performed. A negotiated RTO and RPO with service credits is an Enterprise onboarding item. Any questionnaire field asking for an RTO or RPO must be answered as not published rather than filled with an estimate.

Verification. marketing: src/pages/trust.astro:126.

Pallas has not performed a documented restore test.

Control backup-no-restore-test. Status: Not implemented. A commitment the operator makes contractually. No code enforces it.

Disclosure. No restore test has been carried out, so the recoverability of the backups is a provider assertion rather

than a demonstrated property. This is a genuine gap and it is listed as one. A buyer for whom tested recoverability is a control requirement should treat this as an open item, and the operator should schedule a restore test into a non-production project as the remediation.

Application data is held in Supabase managed PostgreSQL with provider-operated automated backups and point-in-time recovery. The recoverable window is set by the provider tier.

Control backup-provider-operated. Status: Implemented. A statement by a subprocessor. Pallas configures and relies on it; no Pallas code implements it and neither Pallas repository can demonstrate it.

Disclosure. Pallas runs no backup schedule of its own. The backup posture is entirely the Supabase provider tier posture, and the operator has not customised it.

Implementation. vendor: Supabase automated backups and point-in-time recovery.

Verification. marketing: src/pages/trust.astro, Backup and disaster recovery questionnaire answer.

Pallas does not maintain a business continuity plan or a disaster recovery plan that is documented, assigned to a named owner, and exercised annually.

Control continuity-no-tested-bcp-drp. Status: Not implemented. A commitment the operator makes contractually. No code enforces it.

Disclosure. There is no annually tested BCP or DRP with a named owner. Continuity rests on the managed platform underneath: Supabase provider backups with point-in-time recovery, and Cloudflare for edge and Pages hosting. Because no restore test has been performed, recoverability is a provider assertion rather than a demonstrated property. A questionnaire item asking for a documented and tested plan is answered no, not answered yes from the existence of provider backups.

Verification. marketing: src/pages/trust.astro, Backup and disaster recovery questionnaire answer.

Pallas holds account identity, organisation records, scan findings, generated reports, transiently uploaded source files, audit events, and marketing list membership. It holds no payment card data, no special category data by design, and no health or student records.

Control data-classes-enumerated. Status: Implemented. Backed by a file in the pallas-app repository, verified read-only on 2026-08-30, not gated from the marketing repository.

Disclosure. Pallas does not collect special category data as a matter of design, but it scans customer-supplied URLs and accepts customer-uploaded documents. Content a customer submits is outside Pallas control, so the accurate statement is that Pallas does not solicit or intentionally process special category data, not that none can ever transit the system. Uploaded source files carry a 7 day default retention precisely because they are the class most likely to contain something unintended.

Implementation. app: The 29 tables enumerated in tenant-rls-every-table, plus the three Storage buckets in migration 020.

Verification. marketing: src/pages/trust.astro, What Pallas holds and What Pallas never collects.

The default processing location is the United States. Supabase hosts the database and Storage in us-east-1; Cloudflare serves from its global edge network.

Control data-location-default-us. Status: Implemented. A statement by a subprocessor. Pallas configures and relies on it; no Pallas code implements it and neither Pallas repository can demonstrate it.

Implementation. vendor: Supabase project region us-east-1; marketing: src/pages/legal/subprocessors.astro.

Verification. marketing: src/pages/trust.astro, Data residency options.

Processing takes place in the United States only. No European Union hosting exists and none is offered.

Control data-location-eu-option. Status: Not implemented. A commitment the operator makes contractually. No code enforces it.

Disclosure. No customer data is processed in the European Union and no EU infrastructure subprocessor is engaged or planned. Any procurement document, questionnaire response, or sales conversation must present United States processing as the only option and must not present EU hosting as available, on request, or on a roadmap.

Implementation. marketing: src/pages/trust.astro, Data residency options; marketing: src/pages/legal/subprocessors.astro, six operative entries and no planned entry.

Data is encrypted at rest with AES-256 through Supabase-managed infrastructure.

Control encryption-at-rest. Status: Implemented. A statement by a subprocessor. Pallas configures and relies on it; no Pallas code implements it and neither Pallas repository can demonstrate it.

Disclosure. Encryption at rest is provided and attested by Supabase. No Pallas code implements it and neither Pallas repository can demonstrate it. A buyer who requires independent evidence should request the Supabase SOC 2 Type II report rather than a Pallas assertion.

Implementation. vendor: Supabase managed PostgreSQL and Storage encryption at rest.

Verification. vendor: Supabase SOC 2 Type II report, available to the operator under NDA.

All connections are TLS 1.3, enforced by Cloudflare and Supabase.

Control encryption-in-transit. Status: Implemented. A statement by a subprocessor. Pallas configures and relies on it; no Pallas code implements it and neither Pallas repository can demonstrate it.

Disclosure. TLS termination and version are properties of Cloudflare and Supabase. What this repository demonstrates is the header set and the build gate that refuses to ship without it, not the negotiated cipher.

Implementation. vendor: Cloudflare edge TLS and Supabase connection TLS; marketing: public/_headers.

Verification. marketing: scripts/csp-hashes.mjs.

Production secrets are held in the platform secret store and never in either repository. Worker configuration files carry variable names only.

Control encryption-no-secrets-in-repo. Status: Implemented. Demonstrated in the pallas-marketing repository and checked by a release gate.

Disclosure. Two Cloudflare KV namespace identifiers are committed, at workers/pallas-scan-email/wrangler.toml and in the pallas-app Workers. A KV namespace id is an identifier rather than a credential: reaching the namespace still requires authenticated access to the Cloudflare account. This is recorded as a deliberate decision, with the note that the ids should move to deploy-time values if either repository is shared with a buyer, an auditor, or a contractor.

Implementation. marketing: workers/pallas-scan-email/.dev.vars.example and workers/pallas-email-gate/.dev.vars.example; marketing: .gitignore.

Verification. marketing: Rule sweep for key, token, price identifier, and webhook secret strings.

Any signed-in user can export the personal data Pallas holds about them, across every organisation they belong to. This serves GDPR Article 15 and Article 20, CCPA and CPRA right to know, PIPEDA Principle 9, and Australian Privacy Principle 12.

Control gdpr-art15-art20-user-export. Status: Implemented. Backed by a file in the pallas-app repository, verified read-only on 2026-08-30, not gated from the marketing repository.

Implementation. app: pallas_export_user_data, migration 039:268, extended to ten collections in migration 042; app: pallas-app-api, POST /export-user-data, 3 per hour per user, fails closed.

Verification. app: supabase/migrations/039_gdpr_user_rights.sql header, controller split section.

Any signed-in user can erase their own account. This serves GDPR Article 17, CCPA and CPRA right to delete, and PIPEDA withdrawal of consent.

Control gdpr-art17-user-erasure. Status: Implemented. Backed by a file in the pallas-app repository, verified read-only on 2026-08-30, not gated from the marketing repository.

Disclosure. Erasure of a user does not erase the organisation content that user created. Findings, comments, and evidence belong to the organisation as a separate controller with its own retention obligation. The identity link is severed and the audit trail keeps the attribution snapshot. A data subject asking for erasure receives this explanation rather than a silent partial deletion. The request also returns HTTP 409 rather than proceeding if the caller is the sole org_admin of any organisation, because completing it would leave that organisation unadministrable.

Implementation. app: pallas_delete_user_account, migration 039:506; app: pallas-app-api, POST /delete-user-account, requires the X-Confirm-Deletion header, 3 per hour per user, fails closed.

Verification. app: supabase/migrations/040_user_fk_set_null.sql.

Pallas distinguishes the two controller roles in its schema, not only in its policy text. Lonia AI is controller for user profile data; the customer organisation is controller for its own scan and compliance data. The user export and the organisation export are separate functions, not one filtered by the other.

Control gdpr-controller-split-documented. Status: Implemented. Backed by a file in the pallas-app repository, verified read-only on 2026-08-30, not gated from the marketing repository.

Implementation. app: pallas_export_user_data 039:268 for the individual, pallas_export_org_data 009:13 rebuilt in 032:67 and 037:297 for the organisation.

Verification. app: supabase/migrations/039_gdpr_user_rights.sql, controller split section.

An organisation administrator can delete the organisation. Deletion cancels the Stripe subscription, wipes Storage under the organisation prefix, and removes the database rows, archiving a defined subset of audit actions first.

Control gdpr-org-deletion. Status: Implemented. Backed by a file in the pallas-app repository, verified read-only on 2026-08-30, not gated from the marketing repository.

Implementation. app: pallas_delete_org, migration 008:70, rebuilt 022:71, 024:702, 025:245, and again in migration 041; app: pallas-app-api, POST /delete-org, org_admin plus a typed confirmation phrase, deliberately not rate limited;

app: pallas_retained_audit_events, migration 021:119.

Verification. app: pallas_record_post_delete_failure, migration 025:337.

An organisation administrator can export the full organisation data set for a data subject access request.

Control gdpr-org-dsar-export. Status: Implemented. Backed by a file in the pallas-app repository, verified read-only on 2026-08-30, not gated from the marketing repository.

Implementation. app: pallas_export_org_data, migration 009:13, rebuilt 032:67 and 037:297; app: pallas-app-api, POST /export-org-data, org_admin only, 3 per hour per user and per org, fails closed.

Verification. app: supabase/migrations/032_export_completeness.sql.

The two individual rights functions are callable only by the service role. The acting user id is derived from a verified JWT and is never accepted from a request body.

Control gdpr-rights-service-role-only. Status: Implemented. Backed by a file in the pallas-app repository, verified read-only on 2026-08-30, not gated from the marketing repository.

Implementation. app: supabase/migrations/039_gdpr_user_rights.sql, grant section; app: pallas-app-api.

Verification. app: supabase/migrations/039_gdpr_user_rights.sql header, service_role only section.

Pallas notifies affected customers without undue delay and in any event within 72 hours of becoming aware of a breach affecting their data. The clock starts on awareness, not on confirmation.

Control incident-72-hour-notification. Status: Implemented. A commitment the operator makes contractually. No code enforces it.

Disclosure. This is a contractual commitment. No technical control enforces it and no artifact in either repository can demonstrate it has been met, because no breach has occurred. A buyer should treat it as a term to be captured in the Data Processing Agreement rather than as a verified capability.

Implementation. marketing: src/pages/trust.astro, Breach commitments, Customer notification; marketing: src/pages/legal/dpa.astro.

Authority notification follows the jurisdiction: Ireland DPC, UK ICO, and EU supervisory authorities within 72 hours; Canada OPC under PIPEDA; Australia OAIC under the Notifiable Data Breaches scheme.

Control incident-authority-notification. Status: Implemented. A commitment the operator makes contractually. No code enforces it.

Disclosure. A contractual and regulatory commitment rather than a technical control. Pallas has not been required to make such a notification, so there is no track record to evidence.

Implementation. marketing: src/pages/trust.astro, Breach commitments, Authority notification.

Worker observability and logging are enabled on every deployed Worker so that failures surface rather than passing silently.

Control incident-detection-monitoring. Status: Partial. Demonstrated in the pallas-marketing repository and checked by a release gate.

Disclosure. Observability is enabled and logs are collected. There is no security information and event management system, no alerting pipeline, no on-call rotation, and no documented incident response runbook with named roles. Detection today means an operator reading the Cloudflare dashboard. Any questionnaire asking about 24 by 7 monitoring, SIEM, or a tested incident response plan must be answered no. Pallas is operated by a single operator and a procurement document that implied a staffed security operations centre would be false.

Implementation. marketing: workers/pallas-scan-email/wrangler.toml and workers/pallas-email-gate/wrangler.toml, observability and observability.logs enabled; app: All six pallas-app Workers, observability enabled in wrangler.toml.

Verification. marketing: workers/pallas-email-gate/wrangler.toml observability comment.

A full technical postmortem is provided to affected customers within 30 days.

Control incident-post-incident-report. Status: Implemented. A commitment the operator makes contractually. No code enforces it.

Implementation. marketing: src/pages/trust.astro, Breach commitments, Post-incident report.

Pallas does not publish a cyber liability insurance policy or a certificate of cover.

Control insurance-no-published-cover. Status: Not implemented. A commitment the operator makes contractually. No code enforces it.

Disclosure. No cyber liability certificate is published. A questionnaire field asking for evidence of cover is answered as not published rather than left blank or answered from intent, and where a contract requires evidence of cover the matter is addressed in the agreement during procurement.

Verification. marketing: src/pages/trust.astro, Cyber liability insurance, status Not yet formalized.

Pallas operates no network perimeter, no host, and no network monitoring of its own. Edge filtering, DDoS mitigation, and TLS termination are Cloudflare functions, and the database network boundary is operated by Supabase.

Control network-perimeter-subprocessor-operated. Status: Implemented. A statement by a subprocessor. Pallas configures and relies on it; no Pallas code implements it and neither Pallas repository can demonstrate it.

Disclosure. Pallas runs no firewall of its own, no network intrusion detection or prevention system, and no host-based agent, because it operates no hosts. Stateful filtering, DDoS mitigation, and TLS termination happen at the Cloudflare edge and are answered as provider-operated. Intrusion detection, intrusion prevention tuned by Pallas, next-generation persistent threat monitoring, and 24x7 intrusion monitoring are answered no: no such capability is operated by Pallas or configured by Pallas at a provider. A buyer requiring a monitored perimeter under vendor control, or a staffed security operations centre, should treat this as an open item.

Implementation. vendor: Cloudflare edge network, web application firewall and DDoS mitigation; Supabase managed database network boundary.

Verification. marketing: workers/, whose Workers execute on the Cloudflare edge rather than on any Pallas-operated host.

Pallas does not operate a documented background-screening programme, a security-awareness programme, or a recurring mandatory security or privacy training programme for personnel.

Control personnel-no-formal-screening-program. Status: Not implemented. A commitment the operator makes contractually. No code enforces it.

Disclosure. Pallas is operated by a small team and publishes no background-screening programme, no recurring security-awareness curriculum, and no annual training record. Personnel questions on a vendor questionnaire are answered as not formalised rather than answered yes from intent. What limits operator access instead is technical and is inventoried separately: OAuth-only sign-in with no password to share or leak, least-privilege service roles, and a tamper-evident audit trail over administrative actions that the operator cannot silently alter.

Verification. marketing: src/pages/trust.astro, Personnel screening and security training, status Not yet formalized.

Pallas operates no data centre, server cage, office server room, or other facility in which institutional data is held. Physical and environmental security for every system that holds institutional data belongs to Supabase and Cloudflare.

Control physical-security-subprocessor-operated. Status: Implemented. A statement by a subprocessor. Pallas configures and relies on it; no Pallas code implements it and neither Pallas repository can demonstrate it.

Disclosure. Every physical-security control a questionnaire asks about, including staffed facilities, cages, enclosing barriers, redundant and tested power, cooling, fire suppression, and carrier diversity, belongs to Supabase or Cloudflare. Pallas can neither demonstrate nor test any of them, and does not inherit them as its own controls. Answers to physical-security questions state reliance and name the provider. A buyer who needs evidence should read the provider audit reports; a Pallas assertion is not evidence of a provider control.

Implementation. vendor: Supabase and Cloudflare published data centre physical and environmental security programmes.

Verification. marketing: src/pages/trust.astro, subprocessor list with per-provider processing locations.

Per-plan feature access is enforced server side, in the Row-Level Security policy governing report creation and in the audit export function.

Control plan-feature-flags-server-enforced. Status: Implemented. Backed by a file in the pallas-app repository, verified read-only on 2026-08-30, not gated from the marketing repository.

Disclosure. The 2026-08-30 inventory record lists feature flags as client-side only. That is contradicted by the file set at migration 035:296 and 035:380. This row follows the file set. As with seat caps, the inventory record understated rather than overstated the control.

Implementation. app: pallas_reports INSERT policy, migration 035:296; app: pallas_check_feature_access 035:207, also called from pallas_export_audit_events at 035:380 for the 'audit_export' feature.

Verification. app: src/config/plans.ts:12.

Pallas publishes its security whitepaper, Data Processing Agreement, Data Protection Impact Assessment, Transfer Impact Assessment, EU Standard Contractual Clauses, institutional terms of service, and VPAT 2.5 accessibility conformance report as downloadable documents, each generated from this control inventory and each gated against drift on every release.

Control procurement-documentation-published. Status: Implemented. Demonstrated in the pallas-marketing repository and checked by a release gate.

Disclosure. This row is about documentation, not about certification. That the documents exist, are generated from the inventory, and cannot silently drift from it is demonstrable here and gated on every release. It says nothing about any of them having been reviewed by an auditor, and no document in the set carries independent assurance. A questionnaire item asking whether a policy is DOCUMENTED is answered from this row; an item asking whether it is

AUDITED is not.

Implementation. marketing: src/data/procurement/, the document sources, and scripts/generate-*.mjs, the generators that render them; marketing: src/data/procurement/published-artifacts.ts, the index /trust renders the download list from.

Verification. marketing: scripts/verify-doc-artifact-freshness.mjs; marketing: package.json, the release script, which runs docs:all before check:freshness.

Archived audit events past their retention window are purged nightly at 04:00 UTC, and each purge run is logged.

Control retention-audit-purge. Status: Implemented. True of the migration file set. Live database state is not provable from source, and the operator pre-check that resolves it is named in the disclosure.

Disclosure. Scheduled by the same self-catching DO block pattern as the 03:00 UTC sweep. Existence of the live job is an operator check against cron.job.

Implementation. app: pallas_nightly_retention_purge, '0 4 * * *', scheduled at migration 034:581; app: pallas_purge_expired_retained_audit_events, migration 034:460; app: pallas_retention_purge_log, migration 034:405, RLS enabled 034:416.

Verification. app: supabase/migrations/034_enforce_finding_limit_and_retention_purge.sql section 9.

A scheduled job applies retention policies daily at 03:00 UTC for every organisation with automatic deletion enabled.

Control retention-daily-sweep. Status: Implemented. True of the migration file set. Live database state is not provable from source, and the operator pre-check that resolves it is named in the disclosure.

Disclosure. The job is scheduled by a DO block that catches its own exception, so a database on which pg_cron was not enabled at migration time has no job and the migration still reported success. Whether the job exists and is running on the live database is an operator check against the cron.job and cron.job_run_details tables. This repository can show what was intended to be scheduled; it cannot show what is scheduled.

Implementation. app: pallas-daily-retention, '0 3 * * *', scheduled at migration 021:238; app: pallas_apply_retention_policies, migration 021:197, rebuilt 029:629, migration 041, and migration 042.

Verification. app: supabase/migrations/042_restore_retention_sweeps_and_gaps.sql.

Retention settings cause actual deletion rather than being stored as a preference. The sweep issues DELETE statements against the tables it governs.

Control retention-deletion-actually-deletes. Status: Implemented. Backed by a file in the pallas-app repository, verified read-only on 2026-08-30, not gated from the marketing repository.

Implementation. app: pallas_apply_retention_policies, migration 042.

Verification. app: migration 041, which enumerates the three code paths that lawfully remove audit rows.

Retention is configured per organisation, with defaults of 365 days for scan data, 7 days for uploaded source files, 730 days for reports, and 2555 days (seven years) for the audit log.

Control retention-per-org-policies. Status: Implemented. Backed by a file in the pallas-app repository, verified

read-only on 2026-08-30, not gated from the marketing repository.

Implementation. app: pallas_retention_policies, migration 002:374.

Verification. app: uq_pallas_retention_org, migration 002:385.

Uploaded source files are purged from Storage daily at 05:00 UTC by a Supabase Edge Function invoked from the database.

Control retention-source-file-purge. Status: Partial. True of the migration file set. Live database state is not provable from source, and the operator pre-check that resolves it is named in the disclosure.

Disclosure. This job does no work unless two database settings are present: app.settings.functions_base_url and app.settings.cron_secret. When either is missing the job raises a warning and returns, so source files are NOT purged and nothing fails loudly. Migration 035:619 states this in the job body. The operator must confirm both settings are set on the live database before this control is claimed to a buyer. Separately, the 2026-08-30 inventory record describes this credential as being held in Supabase Vault under the name pallas_enforce_retention_bearer. No file in either repository references Vault or that name; the mechanism on disk is a Supabase Edge Function secret named CRON_SECRET plus a database setting named app.settings.cron_secret. The inventory description and the file set disagree, and the file set is what these repositories can show.

Implementation. app: pallas_daily_source_file_retention, '0 5 * * *', scheduled at migration 035:609; app: supabase/functions/enforce-retention/index.ts.

Verification. app: supabase/functions/enforce-retention/index.ts:239 to :252.

Section 508 and EN 301 549 results are produced by applying the corresponding axe-core tag presets, not by an independent rule engine for each standard.

Control scan-508-and-en301549-are-tag-presets. Status: Partial. Demonstrated in the pallas-marketing repository and checked by a release gate.

Disclosure. Section 508 and EN 301 549 coverage in Pallas is the axe-core tag preset for each standard. Pallas has not implemented, and does not claim, an independent rule engine per standard. A buyer procuring against EN 301 549 specifically should read this as WCAG-derived automated coverage mapped to that standard, and should not treat it as a full EN 301 549 conformance assessment, which includes non-web requirements Pallas does not evaluate at all.

Implementation. marketing: package.json, axe-core dependency, and the tag selection in the scan path.

Verification. marketing: tests/scan-report.test.ts.

The website scanner analyses a single page of static HTML.

Control scan-single-page-static-only. Status: Partial. Demonstrated in the pallas-marketing repository and checked by a release gate.

Disclosure. The scanner fetches one page, strips scripts, and analyses the resulting static markup. It does not crawl, it does not execute JavaScript, and single-page applications that render their content client side will not be represented in the results. A buyer evaluating Pallas against a client-rendered application should understand that the public scan tool will report on the served shell rather than the rendered page.

Implementation. marketing: src/lib/scan-report.ts; app: pallas-cors-proxy and pallas-scanner-sandbox.

Verification. marketing: tests/scan-report.test.ts.

Pallas publishes a VPAT 2.5 Accessibility Conformance Report for its own product.

Control scan-vpat-published. Status: Implemented. Demonstrated in the pallas-marketing repository and checked by a release gate.

Disclosure. PDF content is verifiable in this repository and gated on every release. PDF tagging is not verifiable here and is confirmed by the operator running PAC 2024 against the regenerated file. The build gate can prove the words are right; it cannot prove the tag tree is.

Implementation. marketing: public/documents/pallas-vpat-2.5-acr.pdf.

Verification. marketing: scripts/verify-doc-artifact-freshness.mjs, check 10; marketing: Validate the regenerated PDF with PAC 2024, target zero PDF/UA and zero WCAG failures.

Pallas reports against the WCAG 2.2 success criteria catalogue. Automated detection covers approximately 17 criteria; the remainder require manual review.

Control scan-wcag-coverage. Status: Partial. Demonstrated in the pallas-marketing repository and checked by a release gate.

Disclosure. Listing the full WCAG 2.2 catalogue is not the same as detecting all of it. Roughly 17 success criteria are reliably detectable by automated tooling; the rest depend on human judgement about context, purpose, or equivalence and cannot be settled by a rule engine. Any procurement document that presents the catalogue must state the automated subset in the same sentence, not in a footnote.

Implementation. marketing: src/data/stats.ts; marketing: package.json, axe-core dependency.

Verification. marketing: src/pages/accessibility.astro and src/pages/features.astro.

Certifications listed against each subprocessor are those published by that provider.

Control subprocessors-certifications-are-theirs. Status: Implemented. A statement by a subprocessor. Pallas configures and relies on it; no Pallas code implements it and neither Pallas repository can demonstrate it.

Disclosure. Pallas holds no SOC 2, ISO 27001, or PCI DSS certification of its own. Every certification named on the subprocessor list belongs to the named provider and covers that provider infrastructure, not the Pallas application built on top of it. A procurement document must never present a subprocessor certification in a way that could be read as a Pallas certification. This is the single most consequential misreading available in this inventory, so the distinction is stated wherever the certifications appear.

Implementation. marketing: src/pages/legal/subprocessors.astro.

A new subprocessor is published with 30 days advance notice before it processes any customer data.

Control subprocessors-change-notice. Status: Implemented. A commitment the operator makes contractually. No code enforces it.

Disclosure. This is a contractual commitment by the operator, not a technical control. Nothing in either repository enforces the notice period, and no new subprocessor has yet been added under it.

Implementation. marketing: src/pages/legal/subprocessors.astro, Change Notification section.

The full subprocessor list is published, with each provider purpose, data categories, processing location, and published certifications.

Control subprocessors-published-list. Status: Implemented. Demonstrated in the pallas-marketing repository and checked by a release gate.

Disclosure. The 2026-08-30 inventory record names four subprocessors in use: Supabase, Cloudflare, Stripe, and Resend. The published page carries six operative entries, adding Google and Microsoft as OAuth identity providers. Both are accurate about different things: Google and Microsoft receive an authentication assertion at sign-in and store no Pallas customer data. Procurement artifacts should carry all six operative entries, because a buyer assessing identity provider dependency needs to see the two that the four-entry description omits.

Implementation. marketing: src/pages/legal/subprocessors.astro.

Verification. marketing: src/pages/trust.astro, Sub-processors section.

Marketing list membership records the source of the signup and the moment consent was given, alongside the enrolment time.

Control subscriber-consent-recorded. Status: Implemented. Backed by a file in the pallas-app repository, verified read-only on 2026-08-30, not gated from the marketing repository.

Disclosure. Until 2026-09-06 the pallas_subscribers and pallas_subscriber_suppression tables had no data definition file in either repository. Migration 046 in pallas-app now captures both. The schema, its constraints, and the fact that Row-Level Security is enabled on both tables are under version control and can be shown to a buyer from source. Two limits are worth stating. Migration 046 is a recovery transcription of tables that were created by hand on the live database on 2026-08-30, so it is a description of live rather than the file live was built from; the file itself says as much and carries a verification query in its final section. And the file is in pallas-app, so no release gate in pallas-marketing checks it. Recommended operator action: run the verification query at the foot of migration 046 against the live project and correct the migration if any column, constraint, or policy count disagrees with what live returns.

Implementation. marketing: src/lib/email-gate.ts:338 onward; app: supabase/migrations/046_subscribers_table_ddl_recovery.sql.

Verification. marketing: tests/email-gate.test.ts.

Unsubscribing writes to a suppression table keyed on a hash of the address, so a later signup of the same address is refused without retaining the plaintext address on the suppression list.

Control subscriber-suppression-list. Status: Implemented. Demonstrated in the pallas-marketing repository and checked by a release gate.

Implementation. marketing: src/lib/unsubscribe.ts:245 and :284; marketing: src/lib/email-gate.ts:327.

Verification. marketing: tests/unsubscribe.test.ts.

The unsubscribe route is dispatched ahead of the CORS, method, and Turnstile checks, so a misconfigured bot gate for joining a list cannot take the mechanism for leaving it offline.

Control subscriber-unsubscribe-always-reachable. Status: Implemented. Demonstrated in the pallas-marketing repository and checked by a release gate.

Disclosure. The route stays reachable but it does not claim a removal it could not perform. When the Supabase credentials are missing it reports the removal as unfinished rather than confirming it.

Implementation. marketing: src/lib/unsubscribe-route.ts; marketing: pallas-email-gate, GET and POST /unsubscribe.

Verification. marketing: tests/unsubscribe-route.test.ts and tests/unsubscribe.test.ts.

Every tenant-scoped policy resolves membership through two SECURITY DEFINER helpers with a pinned search_path, rather than by re-entering the membership table under its own RLS.

Control tenant-org-scoping-helpers. Status: Implemented. Backed by a file in the pallas-app repository, verified read-only on 2026-08-30, not gated from the marketing repository.

Implementation. app: pallas_user_has_org_access, migration 002:8, hardened in 031:54; app: pallas_user_org_role, migration 002:17, hardened in 031:68.

Verification. app: supabase/migrations/031_low_severity_hardening.sql.

Row-Level Security is enabled on every Pallas application table. Twenty-nine tables carry it in the migration file set.

Control tenant-rls-every-table. Status: Implemented. True of the migration file set. Live database state is not provable from source, and the operator pre-check that resolves it is named in the disclosure.

Disclosure. Twenty-nine tables carry RLS in the migration file set (twenty-four before migrations 057 and 059 added the digest-run and rule-override tables on 2026-09-16, twenty-six before migration 067 added the two crawl-state tables on 2026-09-17, and twenty-eight before migration 072 added the API-token table). Two of them, pallas_subscribers and pallas_subscriber_suppression, were created directly on the live database on 2026-08-30 and captured into migration 046 only afterwards, so any count taken before that migration was written disagrees with this one. The 2026-08-30 inventory pass recorded twenty-two on the live project. That difference has not been reconciled against the live database, because code in these repositories does not execute SQL. Before this claim is stated to a buyer with a number attached, the operator should run a live count of pg_tables joined to pg_class.relrowsecurity for tables matching pallas_%, and either correct this row or correct the 2026-08-30 inventory record. Until then the safe published form of this claim omits the count and states only that RLS is enabled on every application table.

Implementation. app: ENABLE ROW LEVEL SECURITY on 29 tables across migrations 001, 002, 005, 010, 017, 021, 024, 029, 034, 041, 046, 057, 059, 067, 072.

Verification. app: Search supabase/migrations/*.sql for ENABLE ROW LEVEL SECURITY and compare the count against CREATE TABLE.

Server-side operator functions run under service credentials that bypass Row-Level Security by necessity. Their scope is limited, they are versioned in source, and their actions are covered by the audit trail.

Control tenant-service-role-bypass-disclosed. Status: Implemented. Backed by a file in the pallas-app repository, verified read-only on 2026-08-30, not gated from the marketing repository.

Disclosure. Service-role credentials bypass Row-Level Security. This is a property of PostgreSQL and Supabase, not a Pallas design choice, and it means tenant isolation for service-role code paths rests on the correctness of those code paths rather than on the database refusing them. The mitigating controls are that the paths are few, versioned, and audit-logged, not that they are constrained by RLS.

Implementation. app: pallas-app-api; app: supabase/functions/enforce-retention/index.ts.

Verification. marketing: src/pages/trust.astro, Security posture, Tenant isolation.

The evidence, source-files, and reports Storage buckets are private and carry per-organisation RLS policies on storage.objects, with read, write, update, and delete scoped to organisation role.

Control tenant-storage-per-org. Status: Implemented. Backed by a file in the pallas-app repository, verified read-only on 2026-08-30, not gated from the marketing repository.

Implementation. app: supabase/migrations/020_storage_bucket_rls.sql; app: pallas_storage_org_access, migration 020:50.

Verification. app: supabase/migrations/020_storage_bucket_rls.sql header.

Dependency advisories are triaged by whether a request path actually reaches the affected code, and the triage is recorded in version control with a review date and the reasoning rather than the conclusion alone.

Control vuln-advisory-triage-artifact. Status: Implemented. Demonstrated in the pallas-marketing repository and checked by a release gate.

Disclosure. Three advisories are currently open in npm audit, reported as one low and two high. All ten individual advisories were assessed as unreachable in this build configuration, on the basis that the site is a fully static build with no server runtime, no client hydration, and no build-time image processing. The advisories remain open rather than fixed: the proposed remediation is a two major version Astro upgrade that npm audit labels breaking, and that upgrade is scheduled on its own timeline rather than taken as an emergency for unreachable findings. A buyer running npm audit against this repository will see the counts, and this file is the answer to what they mean.

Implementation. marketing: SECURITY_ADVISORY_TRIAGE.md.

Verification. marketing: SECURITY_ADVISORY_TRIAGE.md, section titled What would invalidate this triage.

Deployment to Cloudflare Pages and to every Worker is a deliberate manual operator step, not an automatic consequence of a merge.

Control vuln-deploys-are-manual. Status: Implemented. Backed by a file in the pallas-app repository, verified read-only on 2026-08-30, not gated from the marketing repository.

Disclosure. Manual deployment is a deliberate choice rather than a missing pipeline: it means a malformed build cannot ship silently. It also means deployment timing depends on operator availability, which a buyer assessing change velocity or emergency patch turnaround should know.

Implementation. app: docs/OPERATOR_ACTIONS.md section 2, standing operator steps.

Verification. app: docs/OPERATOR_ACTIONS.md, items 1 through 4.

Pallas holds no SOC 2, ISO 27001, or other independent security certification.

Control vuln-no-independent-certification. Status: Not implemented. A commitment the operator makes contractually. No code enforces it.

Disclosure. Pallas holds no certification of its own. Certifications named anywhere in Pallas materials belong to subprocessors. Where a buyer requires a converted assurance rather than an assertion, the mechanism is a contractual term in the Institutional Terms of Service, the signable agreement, not a certificate Pallas can produce. There is no separate master services agreement.

Verification. marketing: src/pages/trust.astro, Compliance frameworks, Planned.

Pallas has not commissioned an independent penetration test.

Control vuln-no-penetration-test. Status: Not implemented. A commitment the operator makes contractually. No code enforces it.

Disclosure. No third party penetration test has been performed and no report exists. Security review to date has been internal, through repeated structured audits recorded in this repository. Any questionnaire field asking for the date of the last penetration test or for a report must be answered as none performed. This is a real gap for institutional buyers and it should be presented as one rather than deflected to the internal audit history.

Verification. marketing: src/pages/trust.astro, questionnaire answers section.

Every change reaches production through version control, and the build fails closed rather than degrading.

Control vuln-version-control-and-review. Status: Implemented. Demonstrated in the pallas-marketing repository and checked by a release gate.

Disclosure. Pallas is built and operated by a single operator, so there is no second-party code review before merge and no segregation of duties between the person who writes a change and the person who deploys it. The compensating control is the automated build chain, which the hosting platform runs on every push, is identical for every change, and cannot be selectively skipped. Any questionnaire asking about mandatory peer review or segregation of duties must be answered no.

Implementation. marketing: package.json build script; marketing: scripts/csp-hashes.mjs and scripts/test-turnstile.mjs.

Verification. marketing: src/pages/trust.astro:121.

Appendix A. Controls cited

This document cites 71 of the 84 rows in the Pallas control inventory. Each is listed below with the status and evidence basis it carried at the 2026-08-30 inventory pass. A row absent from this list is not claimed by this document.

- **auth-oauth-only** (Authentication). Implemented.
- **auth-profile-trigger-fail-safe** (Authentication). Implemented.
- **auth-session-jwt** (Authentication). Implemented.
- **auth-no-browser-storage-for-entitlements** (Authentication). Implemented.
- **tenant-rls-every-table** (Multi-tenancy isolation). Implemented.
- **tenant-org-scoping-helpers** (Multi-tenancy isolation). Implemented.
- **tenant-storage-per-org** (Multi-tenancy isolation). Implemented.
- **tenant-service-role-bypass-disclosed** (Multi-tenancy isolation). Implemented.
- **audit-sha256-ledger** (Tamper-evident audit chain). Implemented.
- **audit-ledger-append-only** (Tamper-evident audit chain). Implemented.
- **audit-lawful-redaction-recorded** (Tamper-evident audit chain). Implemented.
- **audit-error-codes** (Tamper-evident audit chain). Implemented.
- **audit-seven-year-floor** (Tamper-evident audit chain). Implemented.
- **audit-action-registry** (Tamper-evident audit chain). Implemented.

- **audit-actor-attribution-survives-erasure** (Tamper-evident audit chain). Implemented.
- **gdpr-art15-art20-user-export** (Data subject rights). Implemented.
- **gdpr-art17-user-erasure** (Data subject rights). Implemented.
- **gdpr-controller-split-documented** (Data subject rights). Implemented.
- **gdpr-org-dsar-export** (Data subject rights). Implemented.
- **gdpr-org-deletion** (Data subject rights). Implemented.
- **gdpr-rights-service-role-only** (Data subject rights). Implemented.
- **retention-per-org-policies** (Retention and deletion). Implemented.
- **retention-daily-sweep** (Retention and deletion). Implemented.
- **retention-audit-purge** (Retention and deletion). Implemented.
- **retention-source-file-purge** (Retention and deletion). Partial.
- **retention-deletion-actually-deletes** (Retention and deletion). Implemented.
- **plan-feature-flags-server-enforced** (Plan and quota enforcement). Implemented.
- **encryption-at-rest** (Encryption). Implemented.
- **encryption-in-transit** (Encryption). Implemented.
- **encryption-no-secrets-in-repo** (Encryption). Implemented.
- **access-org-roles** (Access control). Implemented.
- **access-last-admin-guard** (Access control). Implemented.
- **access-rate-limiting-anonymous** (Access control). Partial.
- **access-turnstile-fails-closed** (Access control). Implemented.
- **personnel-no-formal-screening-program** (Access control). Not implemented.
- **appsec-ssrf-guard** (Application security). Implemented.
- **appsec-response-cap** (Application security). Implemented.
- **appsec-sandboxed-rendering** (Application security). Implemented.
- **appsec-output-escaping** (Application security). Implemented.
- **appsec-release-gate-fails-closed** (Application security). Implemented.
- **scan-single-page-static-only** (Scanning engine capability). Partial.
- **scan-wcag-coverage** (Scanning engine capability). Partial.
- **scan-508-and-en301549-are-tag-presets** (Scanning engine capability). Partial.
- **scan-vpat-published** (Scanning engine capability). Implemented.
- **ai-no-model-processing** (Scanning engine capability). Implemented.
- **subscriber-consent-recorded** (Marketing subscriber management). Implemented.
- **subscriber-unsubscribe-always-reachable** (Marketing subscriber management). Implemented.
- **subscriber-suppression-list** (Marketing subscriber management). Implemented.
- **data-classes-enumerated** (Data classes and processing location). Implemented.
- **data-location-default-us** (Data classes and processing location). Implemented.
- **data-location-eu-option** (Data classes and processing location). Not implemented.
- **subprocessors-published-list** (Subprocessors). Implemented.
- **subprocessors-change-notice** (Subprocessors). Implemented.
- **subprocessors-certifications-are-theirs** (Subprocessors). Implemented.

- **physical-security-subprocessor-operated** (Subprocessors). Implemented.
- **network-perimeter-subprocessor-operated** (Subprocessors). Implemented.
- **incident-72-hour-notification** (Incident response). Implemented.
- **incident-authority-notification** (Incident response). Implemented.
- **incident-detection-monitoring** (Incident response). Partial.
- **incident-post-incident-report** (Incident response). Implemented.
- **insurance-no-published-cover** (Incident response). Not implemented.
- **backup-provider-operated** (Backup and recovery). Implemented.
- **backup-no-published-rto-rpo** (Backup and recovery). Not implemented.
- **backup-no-restore-test** (Backup and recovery). Not implemented.
- **continuity-no-tested-bcp-drp** (Backup and recovery). Not implemented.
- **vuln-advisory-triage-artifact** (Vulnerability management). Implemented.
- **vuln-no-penetration-test** (Vulnerability management). Not implemented.
- **vuln-no-independent-certification** (Vulnerability management). Not implemented.
- **vuln-version-control-and-review** (Vulnerability management). Implemented.
- **vuln-deploys-are-manual** (Vulnerability management). Implemented.
- **procurement-documentation-published** (Published procurement documentation). Implemented.