



HECVAT Solution Provider Response

Version: October 11, 2026

TRIOPilot is made by Tamahagane, LLC, a Wyoming limited liability company that operates from Florida. We are not SOC 2 certified, and no independent auditor or penetration tester has assessed us yet. Below is our completed HECVAT (Higher Education Community Vendor Assessment Toolkit), a self-assessment published by EDUCAUSE. Every Yes describes a control in place today. Every No says so plainly and states what we do instead. Student records, documents and backups are stored in the United States (AWS us-east-1, through Supabase). Each program's data is isolated by database row level security, and staff sign in with an emailed one-time code, so we store no passwords.

The same answers are published as the completed Excel workbook at <https://triopilot.com/security>. Questions: hello@triopilot.com.

HECVAT is a product of EDUCAUSE. Questions © 2025 EDUCAUSE.

START HERE

General

GNRL-01 Solution Provider Name

ANSWER Tamahagane, LLC (product: TRIOPilot)

GNRL-02 Solution Name

ANSWER TRIOPilot

GNRL-03 Solution Description

ANSWER TRIOPilot is a cloud-based, multi-tenant student services platform for Federal TRIO college access programs (EOC, Talent Search, Upward Bound, UBMS, SSS, McNair, and VUB). It provides online student applications and intake, advising and case management, contact and service logging, document management, scheduling, optional two-way SMS, and Annual Performance Report (APR) generation for program staff.

GNRL-04 Solution Provider Contact Name

ANSWER Matt Acevedo

GNRL-05 Solution Provider Contact Title

ANSWER Founder

GNRL-06 Solution Provider Contact Email

ANSWER hello@triopilot.com

GNRL-07 Solution Provider Contact Phone Number

ANSWER 305-204-1204

GNRL-08 Country of Company Headquarters

ANSWER United States

GNRL-09 Employee Work Locations (all)

ANSWER United States only (Florida; fully remote, no offices)

Company Information

COMP-01 Do you have a dedicated software and system development team(s) (e.g., customer support, implementation, product management, etc.)?*

ANSWER Yes

ADDITIONAL INFORMATION TRIOPilot is developed, implemented, and supported by its founder, who works on the product full time. Product management, engineering, implementation, and customer support are handled directly by the founder; there is no offshore or contracted development.

COMP-02 Describe your organization's business background and ownership structure, including all parent and subsidiary relationships.

ANSWER Tamahagane, LLC is a privately held United States limited liability company, wholly owned by its founder, Matt Acevedo. It has no parent company and no subsidiaries. All operations and personnel are located in the United States, and student records, documents and backups are stored in United States cloud regions; there is no offshoring and there are no multinational agreements.

COMP-03 Have you operated without unplanned disruptions to this solution in the past 12 months?

ANSWER No

ADDITIONAL INFORMATION One transient availability incident occurred on August 17, 2026: roughly 75 minutes of elevated errors caused by an upstream network stall between the hosting provider and the database provider. Service recovered fully within the same hour with no data loss and no security impact, and the root cause class was remediated by adding strict request timeouts to all database and storage calls. No other unplanned disruptions in the past 12 months.

COMP-04 Do you have a dedicated information security staff or office?

ANSWER No

ADDITIONAL INFORMATION There is no separate security office. The founder is the named Security Owner and is accountable for the security program (risk register, policies, evidence, incident response). A documented security roadmap, risk register, and control backlog are maintained, and recurring internal security audits are performed with written reports.

COMP-05 Use this area to share information about your environment that will assist those who are assessing your company's data security program.

ANSWER TRIOPilot is a multi-tenant SaaS application: Next.js on Vercel (serverless) with Supabase managed PostgreSQL, authentication, and object storage, all running on AWS in the United States (primary region us-east-1). Tenant isolation is enforced at the database layer with PostgreSQL Row Level Security on every tenant-scoped table and is verified by automated cross-tenant isolation test suites. Authentication is passwordless (emailed one-time codes), so no user passwords exist to steal or reuse. All traffic is TLS encrypted and data is encrypted at rest. Error monitoring (Sentry, hosted in the United States, under a data processing agreement signed 2026-09-18) receives the context needed to resolve an incident, including student identity and request bodies; credentials are always stripped before events leave the platform. A detailed audit log of staff actions on student records is visible to institution administrators inside the product. Backups: daily encrypted database backups (point-in-time recovery is not enabled) plus a nightly copy of student documents to a separate backup project, with independent failure alerting. Every release passes a required type check, lint and full automated test run and a staging environment before production. Recurring internal adversarial security audits (data loss audit, supply chain and malicious code audit, authentication architecture audit) are documented; summaries are available on request.

Required Questions

REQU-01 Are you offering a product or platform?

ANSWER Yes

REQU-02 Does your product or service have an interface?

ANSWER Yes

REQU-03 Are you providing consulting services?

ANSWER No

ADDITIONAL INFORMATION Software subscription only; no consulting services.

REQU-04 Does your solution have AI features, or are there plans to implement AI features in the next 12 months?

ANSWER Yes

ADDITIONAL INFORMATION An optional staff-facing AI assistant is generally available. It looks up students and counts, builds lists, answers questions from the help center, and drafts contact log entries and text messages that a person reviews and sends. It is disabled by default for every program; each program's administrators decide whether to turn it on. Each program's AI traffic can run under its own API credential and spend limit, which TRIOPilot can revoke for that program alone. AI processing uses Anthropic's commercial API, whose terms of service incorporate the Anthropic Data Processing Addendum by reference, contractually prohibit training models on customer content, and automatically delete API inputs and outputs within 30 days. See the AI tab.

REQU-05 Does your solution process protected health information (PHI) or any data covered by the Health Insurance Portability and Accountability Act (HIPAA)?

ANSWER No

ADDITIONAL INFORMATION TRIOPilot is not a HIPAA covered entity or business associate and does not process protected health information.

REQU-06 Is the solution designed to process, store, or transmit credit card information?

ANSWER No

ADDITIONAL INFORMATION The platform does not collect, process, store, or transmit cardholder data from students or institutional users. The only payment in the relationship is the institution's annual subscription which, when paid by card, is handled entirely on Stripe's PCI DSS Level 1 hosted checkout; card data never touches TRIOPilot systems.

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?

ANSWER No

ADDITIONAL INFORMATION Fully hosted SaaS. No on-premises appliance, agent, or inbound firewall exception is required; institutional users access the service over HTTPS.

REQU-08 Does your solution have access to personal or institutional data?

ANSWER Yes

ADDITIONAL INFORMATION The solution stores student education records (FERPA) entered by program staff and by applicants: demographics, eligibility, educational status, service contacts, documents, and APR outcome data.

Organization

Documentation

DOCU-01 Do you have a well-documented business continuity plan (BCP), with a clear owner, that is tested annually?*

ANSWER No

ADDITIONAL INFORMATION A formal, annually tested business continuity plan is not yet in place. The service is serverless with no company-operated infrastructure, the application is redeployable from source control in minutes, and the backup and recovery architecture is documented. A formal BCP with an annual test is on the security roadmap.

DOCU-02 Do you have a well-documented disaster recovery plan (DRP), with a clear owner, that is tested annually?*

ANSWER No

ADDITIONAL INFORMATION A documented backup and restore strategy exists (daily encrypted database backups, a nightly cross-project backup of student documents with independent failure alerting, and a tombstone-based record recovery system in the product), but a formal DRP with a named owner and an annual test has not yet been executed. It is on the security roadmap.

DOCU-03 Have you undergone a SSAE 18/SOC 2 audit?

ANSWER No

ADDITIONAL INFORMATION TRIOPilot has not yet undergone a SOC 2 audit. The infrastructure providers that hold all customer data (AWS, Supabase, Vercel) each maintain SOC 2 Type 2 attestations, and TRIOPilot maintains a documented SOC 2 readiness roadmap.

DOCU-04 Do you conform with a specific industry standard security framework (e.g., NIST Cybersecurity Framework, CIS Controls, ISO 27001, etc.)?

ANSWER No

ADDITIONAL INFORMATION No formal framework certification yet. The security program is built against the HECVAT control set and the SOC 2 trust services criteria, with a documented risk register, control backlog, evidence plan, and a named Security Owner.

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?

ANSWER Yes

ADDITIONAL INFORMATION Architecture and data flow documentation is maintained (system documentation plus a data inventory with classification and per-flow descriptions of every path that moves student data). Diagrams and the inventory can be provided under NDA.

DOCU-06 Does your organization have a data privacy policy?

ANSWER Yes

ADDITIONAL INFORMATION <https://triopilot.com/privacy>

DOCU-07 Do you have a documented, and currently implemented, employee onboarding and offboarding policy?

ANSWER No

ADDITIONAL INFORMATION The company currently has no employees beyond the founder, so no onboarding or offboarding has occurred. A workforce security policy (screening, agreements, training, access provisioning and revocation) will be adopted before the first hire; role definitions are already documented.

Assessment of Third Parties

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)?*

ANSWER Yes

ADDITIONAL INFORMATION Subprocessors are limited to major cloud providers selected in part for their published security attestations (SOC 2 Type 2 or equivalent), which are reviewed at selection. A documented subprocessor inventory with data classifications is maintained, and an annual reassessment cadence is defined in the security program.

THRD-02 Do you have contractual language in place with third parties governing access to institutional data?*

ANSWER Yes

ADDITIONAL INFORMATION [Supabase] Managed PostgreSQL database, sign-in, and document storage, on AWS in us-east-1. Data: All student and program data at rest. Agreement: its published terms and data processing addendum. [Vercel] Application hosting and content delivery; Web Analytics and Speed Insights. Data: All data in transit; for analytics, redacted page paths and page timings only, with no cookies and no identifiers. Agreement: its published terms and data processing addendum. [Resend] Transactional email; and TRIOPilot product announcement emails to program staff, sent from a separate domain (updates.triopilot.com) with an unsubscribe link. Data: Names and email addresses, sign-in codes, and staff notification emails that can name a student; for announcements, staff names and email addresses only, never student data. Agreement: its published terms and data processing addendum. [Twilio] Two-way text messages and call forwarding, on a subaccount for each program. Data: Phone numbers and message text. Only when the program turns texting on. Agreement: its published terms and data processing addendum. [Google reCAPTCHA] Bot protection on the public application form. Data: Interaction signals and IP address of the person filling in the form. Agreement: its published terms and data processing addendum. [Google Translate] Translation of the application form. Data: Application question and answer choice text written by the program, never student records. Agreement: its published terms and data processing addendum. [Mapbox] Address autocomplete and report map tiles. Data: Partial address text as it is typed; for map tiles, the viewer's IP address and the area shown. Agreement: its published terms and data processing addendum. [Sentry] Error monitoring, hosted in the United States. Data: The context needed to resolve an error, including student identity and request contents; credentials are always stripped. Agreement: Sentry data processing addendum, signed 2026-09-18. [Upstash] Rate limiting, with its primary region in AWS us-east-1. Data: IP addresses, user ids, and sign-in email addresses, used as counter keys. Agreement: its published terms and data processing addendum. [Stripe] Program subscription billing on hosted checkout. Data: Billing contact and payment details of the paying program; no student data. Agreement: its published terms and data processing addendum. [Anthropic] The in-app staff assistant, over the commercial API; and the operator's support tooling. Data: Staff questions and the records the assistant looks up; support reports and error details, which can identify a student. Each program's assistant traffic can run under its own API credential and spend limit, which TRIOPilot can revoke for that program alone. Only when the program turns the assistant on (for the assistant). Agreement: for the assistant, Anthropic commercial terms, which include its data processing addendum; for the support tooling, a Claude Max plan under Anthropic consumer terms, with model training turned off. [GitHub] Source code and support records. Data: Support report text, which can name a student, and the reporter's name and sign-in email. Agreement: its published terms and data processing addendum. [Microsoft] Outlook calendar sync for advisors who connect a calendar. Data: Appointment time and place, the student's first name and last initial, and the student's email as the attendee. Only when an advisor connects an Outlook calendar. Agreement: its published terms and data processing addendum. This list is published at <https://triopilot.com/security>.

THRD-03 Do the contracts in place with these third parties address liability in the event of a data breach?*

ANSWER Yes

ADDITIONAL INFORMATION Each subprocessor's data processing agreement addresses security incidents and breach notification per its standard terms.

THRD-04 Do you have an implemented third-party management strategy?*

ANSWER Yes

ADDITIONAL INFORMATION A documented subprocessor inventory records each third party, the data shared, and the purpose; it is reviewed on change with an annual reassessment cadence. The list in THRD-02 is the complete set of third parties that touch institutional data.

THRD-05 Do you have a process and implemented procedures for managing your hardware supply chain (e.g., telecommunications equipment, export licensing, computing devices)?

ANSWER NA

ADDITIONAL INFORMATION TRIOPilot operates no hardware. The service is fully serverless on managed cloud platforms; there is no hardware supply chain in our custody.

Change Management

CHNG-01 Will the institution be notified of major changes to your environment that could impact the institution's security posture?*

ANSWER Yes

ADDITIONAL INFORMATION Material changes affecting security posture, data handling, or subprocessors are communicated to institutional contacts in advance by email.

CHNG-02 Does the system support client customizations from one release to another?*

ANSWER Yes

ADDITIONAL INFORMATION All tenant-level configuration (branding, custom fields, application form definitions, terminology, reporting settings) persists across releases. All tenants run the current release; customizations are data, not code forks.

CHNG-03 Do you have an implemented system configuration management process (e.g., secure "gold" images, etc.)?*

ANSWER Yes

ADDITIONAL INFORMATION There are no hand-configured servers. Application builds are immutable artifacts deployed atomically, and infrastructure configuration is version controlled and code reviewed.

CHNG-04 Do you have a documented change management process?

ANSWER Yes

ADDITIONAL INFORMATION Changes flow through version control, a required check (type check, lint, full automated test run), and a staging environment before controlled production promotion. Database migrations are applied to the non-production project first, verified, then to production.

CHNG-05 Does your change management process minimally include authorization, impact analysis, testing, and validation before moving changes to production?

ANSWER Yes

ADDITIONAL INFORMATION Every change is authorized by the accountable owner, tested by the full automated test suite, exercised on staging, and verified after production deployment.

CHNG-06 Does your change management process verify that all required third-party libraries and dependencies are still supported with each major change?

ANSWER Yes

ADDITIONAL INFORMATION Dependency health is monitored continuously (GitHub Dependabot alerts plus dependency audits); the lockfile is integrity pinned, and framework or library upgrades must pass the full automated test run before release.

CHNG-07 Do you have policy and procedure, currently implemented, managing how critical patches are applied to all systems and applications?

ANSWER Yes

ADDITIONAL INFORMATION The infrastructure layers (OS, runtime, database) are patched by the managed providers with no action required from us. For application dependencies, security advisories are triaged on receipt (Dependabot), assessed for applicability, and patched promptly; the environment currently carries zero known critical or high severity dependency vulnerabilities.

CHNG-08 Have you implemented policies and procedures that guide how security risks are mitigated until patches can be applied?

ANSWER Yes

ADDITIONAL INFORMATION Each advisory is triaged for actual applicability to our configuration; where a patch cannot be applied immediately, the applicability analysis and compensating controls are documented until remediation.

CHNG-09 Do clients have the option to not participate in or postpone an upgrade to a new release?

ANSWER No

ADDITIONAL INFORMATION Single-version SaaS: all tenants run the current release. Upgrades are non-breaking and zero downtime and cannot be deferred per tenant.

CHNG-10 Do you have a fully implemented solution support strategy that defines how many concurrent versions you support?

ANSWER Yes

ADDITIONAL INFORMATION Exactly one production version is supported at any time, and 100 percent of customers run it.

CHNG-11 Do you have a release schedule for product updates?

ANSWER Yes

ADDITIONAL INFORMATION Continuous delivery: improvements ship as they pass the required checks, with zero downtime deploys. Significant functional changes are announced to institutional contacts.

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?

ANSWER Yes

ADDITIONAL INFORMATION An active product roadmap covering more than the next two years is maintained and can be shared with the institution.

CHNG-13 Can solution updates be completed without institutional involvement (i.e., technically or organizationally)?

ANSWER Yes

ADDITIONAL INFORMATION All updates are applied by TRIOPilot with no institutional involvement and no downtime.

CHNG-14 Are upgrades or system changes installed during off-peak hours or in a manner that does not impact the customer?

ANSWER Yes

ADDITIONAL INFORMATION Deployments are atomic and zero downtime, so deployment timing has no customer impact.

CHNG-15 Do procedures exist to provide that emergency changes are documented and authorized (including after-the-fact approval)?

ANSWER Yes

ADDITIONAL INFORMATION Every change, including emergency fixes, is recorded in version control and the deployment log with author and timestamp; the accountable owner authorizes all production changes, including after-the-fact documentation for emergencies.

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)?

ANSWER Yes

ADDITIONAL INFORMATION Cloud services and application configuration are managed as code; the company operates no servers or appliances. Workforce endpoints are limited to the founder's workstation, which is disk encrypted, screen locked, and kept current on OS security updates.

Policies, Processes, and Procedures

PPPR-01 Do you have a documented patch management process?*

ANSWER Yes

ADDITIONAL INFORMATION See CHNG-07: provider-managed platform patching plus documented dependency triage and prompt remediation at the application layer.

PPPR-02 Can your organization comply with institutional policies on privacy and data protection with regard to users of institutional systems, if required?*

ANSWER Yes

ADDITIONAL INFORMATION TRIOPilot operates as a school official under FERPA for its customers and will comply with institutional privacy and data protection policies as incorporated in the service agreement.

PPPR-03 Is your company subject to the institution's geographic region's laws and regulations?*

ANSWER Yes

ADDITIONAL INFORMATION Tamahagane, LLC is a United States company (a Wyoming limited liability company, operating from Florida), governed and regulated by the United States: the same jurisdiction as the institution.

PPPR-04 Can you accommodate encryption requirements using open standards?

ANSWER Yes

ADDITIONAL INFORMATION TLS 1.2+ for all transport, AES-256 for data at rest, AES-256-GCM for application-layer encryption of stored credentials. All open, standard algorithms.

PPPR-05 Do you have a documented systems development life cycle (SDLC)?

ANSWER Yes

ADDITIONAL INFORMATION The development lifecycle is documented in the engineering documentation: version control, a required pre-release check (type check, lint, full automated test run), staging verification, controlled production promotion, and a documented database migration workflow.

PPPR-06 Do you perform background screenings or multi-state background checks on all employees prior to their first day of work?

ANSWER NA

ADDITIONAL INFORMATION No employees beyond the founder, and no contractors have access to systems or data. A background screening policy will be adopted before the first hire.

PPPR-07 Do you require new employees to fill out agreements and review policies?

ANSWER NA

ADDITIONAL INFORMATION See PPPR-06; agreements and policy review will be in place before the first hire.

PPPR-08 Do you have a documented information security policy?

ANSWER No

ADDITIONAL INFORMATION A formal approved information security policy document is in progress. What exists today and is available for review: a named Security Owner, a documented security roadmap built against the HECVAT and SOC 2 control sets, a risk register, a control backlog, an evidence plan, and a data inventory with classification.

PPPR-09 Are information security principles designed into the product lifecycle?

ANSWER Yes

ADDITIONAL INFORMATION Security is designed in rather than bolted on: database-enforced row level security on every tenant table, a passwordless authentication model that eliminates password storage, least-privilege role capabilities, credential stripping on outbound telemetry, and adversarial security review of changes as standard engineering practice.

PPPR-10 Will you comply with applicable breach notification laws?

ANSWER Yes

ADDITIONAL INFORMATION Yes, including FERPA obligations and applicable state breach notification laws.

PPPR-11 Do you have an information security awareness program?

ANSWER NA

ADDITIONAL INFORMATION No employees. A security awareness program will accompany the first hire; the founder maintains working knowledge of FERPA and secure development practice.

PPPR-12 Is security awareness training mandatory for all employees?

ANSWER NA

ADDITIONAL INFORMATION See PPPR-11.

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?

ANSWER Yes

ADDITIONAL INFORMATION Platform-level privileged access is held solely by the founder; there are no other privileged platform accounts to review. Institution-side roles are assigned and managed by the institution's own administrators, and every role change is recorded in the audit log visible to the institution.

PPPR-14 Do you have documented, and currently implemented, internal audit processes and procedures?

ANSWER Yes

ADDITIONAL INFORMATION Recurring internal audits are documented with written reports: a destructive-path data loss audit, a supply chain and malicious code audit (integrity verification of every locked dependency), an authentication architecture audit, and cross-tenant isolation sweeps. Summaries are available on request.

PPPR-15 Does your organization have physical security controls and policies in place?

ANSWER Yes

ADDITIONAL INFORMATION TRIOPilot maintains no facilities that hold institutional data. All data resides in AWS data centers (via Supabase and Vercel) covered by those providers' SOC 2 Type 2 physical security controls.

Product

Authentication, Authorization, and Account Management

AAAI-01 Does your solution support single sign-on (SSO) protocols for user and administrator authentication?*

ANSWER No

ADDITIONAL INFORMATION Not yet. Authentication is passwordless email verification (an emailed one-time code) for all users and administrators. Institutional SSO (SAML or OIDC) is on the product roadmap and is prioritized by customer need.

AAAI-02 Does your solution support local authentication protocols for user and administrator authentication?*

ANSWER Yes

ADDITIONAL INFORMATION Passwordless email one-time codes, natively supported for all users and administrators. No passwords exist in the system.

AAAI-03 Can you enforce password/passphrase complexity requirements (provided by the institution)?*

ANSWER NA

ADDITIONAL INFORMATION There are no passwords: authentication is passwordless one-time email verification, so there is no password complexity to configure and no password database to protect.

AAAI-04 Does the system have password complexity or length limitations and/or restrictions?*

ANSWER NA

ADDITIONAL INFORMATION See AAAI-03; the system stores no passwords.

AAAI-05 Do you have documented password/passphrase reset procedures that are currently implemented in the system and/or customer support?*

ANSWER NA

ADDITIONAL INFORMATION No passwords exist to reset. Every sign-in uses a freshly issued, expiring one-time code delivered to the user's verified email address.

AAAI-06 Does your organization participate in InCommon or another eduGAIN-affiliated trust federation?*

ANSWER No

AAAI-07 Are there any passwords/passphrases hard-coded into your systems or solutions?*

ANSWER No

ADDITIONAL INFORMATION No hard-coded credentials. Secrets are held in encrypted platform environment configuration, a build-time guard prevents secret exposure in client bundles, and the repository, including its full git history, has been audited for embedded credentials (zero found).

AAAI-08 Are you storing any passwords in plaintext?*

ANSWER No

ADDITIONAL INFORMATION No passwords exist in the system at all.

AAAI-09 Are audit logs available that include AT LEAST all of the following: login, logout, actions performed, and source IP address?*

ANSWER Yes

ADDITIONAL INFORMATION Two complementary layers: (1) the managed authentication service logs sign-in and sign-out events with source IP; (2) the application audit log records staff actions on student records (views, edits, exports, deletions, role changes, settings changes, SMS sends) with actor, timestamp, and action detail, and is visible to institution administrators inside the product.

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.*

ANSWER Authentication events (sign-ins, token issuance, sign-outs, failures) are captured by the managed authentication service with source IP. Security-relevant application actions are captured in the audit log: student record views, edits, exports and deletions, contact and document actions, role and permission changes, settings changes, SMS sends, and user invitations, each with actor, timestamp, and detail. Authorization denials return structured errors carried in server logs with request identifiers, and server errors are captured in monitoring (credentials stripped). An account archived in every program it belongs to is refused at sign-in. No institutional setup is required; logging is on for every tenant by default.

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)?*

ANSWER Yes

ADDITIONAL INFORMATION The application audit log is retained for the life of the customer relationship and is directly accessible to institution administrators in the product (Audit Log screen). Platform and authentication logs are retained per the managed providers' schedules. A written retention summary can be provided.

AAAI-12 Does your application support integration with other authentication and authorization systems?

ANSWER No

ADDITIONAL INFORMATION Not currently; SSO integration is roadmapped. See AAAI-01.

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)

ANSWER No

ADDITIONAL INFORMATION Not applicable until SSO ships; account attributes (name, email, role) are managed in-app by institution administrators.

AAAI-14 Does your application support directory integration for user accounts?

ANSWER No

ADDITIONAL INFORMATION Directory integration is roadmapped with SSO. Accounts are provisioned by institution administrators in the product.

AAAI-15 Does your solution support any of the following web SSO standards: SAML2 (with redirect flow), OIDC, CAS, or other?

ANSWER No

ADDITIONAL INFORMATION Not yet; SAML2 and OIDC support is on the roadmap. See AAAI-01.

AAAI-16 Do you support differentiation between email address and user identifier?

ANSWER Yes

ADDITIONAL INFORMATION Users are identified internally by an immutable unique identifier; the email address is a changeable login attribute. Changing the sign-in email takes two one-time codes, one sent to the current address and one to the new address.

AAAI-17 If you don't support SSO, does your application and/or user frontend/portal support multifactor authentication (e.g., Duo, Google Authenticator, OTP, etc.)?

ANSWER No

ADDITIONAL INFORMATION Authentication is itself an email possession factor: a one-time code is sent to the verified address on every sign-in, and there is no stored password to compromise. An additional second factor is not currently offered; it is planned alongside SSO.

AAAI-18 Does your application automatically lock the session or log out an account after a period of inactivity?

ANSWER No

ADDITIONAL INFORMATION A sign-in stays active on that browser for up to 400 days unless the user signs out; access tokens are short-lived and refresh while the session lasts. An automatic inactivity logout is not currently enforced; it is a planned hardening item. Users can sign out from any screen, and institution administrators can archive an account, which refuses its next request.

Data

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?*

ANSWER Yes

ADDITIONAL INFORMATION The managed database endpoint is provider hosted and reachable only over TLS with authenticated, per-request authorization (signed tokens plus database row level security). There is no unauthenticated network path to data, and the application never exposes direct database access. This is the standard architecture of the managed platform (Supabase on AWS).

DATA-02 Is the transport of sensitive data encrypted using security protocols/algorithms (e.g., system-to-client)?*

ANSWER Yes

ADDITIONAL INFORMATION TLS 1.2+ on every connection: browser to application, application to database and storage, and all subprocessor APIs.

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)?*

ANSWER Yes

ADDITIONAL INFORMATION AES-256 encryption at rest for the database and document storage (provider managed). Per-tenant SMS credentials receive an additional application layer of AES-256-GCM encryption. Outlook calendar tokens, held for advisors who connect a calendar, and a program's own AI assistant API credential, when it has one, also receive AES-256-GCM encryption, each under its own key.

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)?*

ANSWER No

ADDITIONAL INFORMATION Cryptography is provided by the managed platforms (AWS-based TLS and AES-256 at rest). We have not verified formal FIPS 140-2 or 140-3 validation for every module in the chain and do not claim it.

DATA-05 Will the institution's data be available within the system for a period of time at the completion of this contract?*

ANSWER Yes

ADDITIONAL INFORMATION At contract end the institution's data remains available for an agreed wind-down period for export before deletion.

DATA-06 Are these rights retained even through a provider acquisition or bankruptcy event?*

ANSWER Yes

ADDITIONAL INFORMATION Data ownership by the institution and its export rights are contractual and survive a change of control; see also DATA-21.

DATA-07 Do backups containing the institution's data ever leave the institution's data zone either physically or via network routing?*

ANSWER No

ADDITIONAL INFORMATION All backups remain within United States cloud regions: database backups with the managed provider, and the nightly document storage backup in a separate, credential-isolated project, also in the United States.

DATA-08 Is media used for long-term retention of business data and archival purposes stored in a secure, environmentally protected area?*

ANSWER Yes

ADDITIONAL INFORMATION Backup media is managed entirely by the cloud providers in SOC 2 attested facilities; no physical media exists in our custody.

DATA-09 At the completion of this contract, will data be returned to the institution and deleted from all your systems and archives?

ANSWER Yes

ADDITIONAL INFORMATION Program administrators can export all program data themselves at any time (Settings > Account > Export All Program Data): every record as CSV and JSON Lines plus every uploaded document, confirmed by an emailed code, with a notice email to every administrator of the program. At contract completion the institution takes this export (TRIOPilot can also run it on request), after which data is deleted from production and ages out of backup retention. A written offboarding runbook is available.

DATA-10 Can the institution extract a full or partial backup of data?

ANSWER Yes

ADDITIONAL INFORMATION Program administrators can export all program data themselves at any time (Settings > Account > Export All Program Data): every record as CSV and JSON Lines plus every uploaded document, confirmed by an emailed code, with a notice email to every administrator of the program. Student lists and APR participant files can also be exported as CSV from their screens.

DATA-11 Do current backups include all operating system software, utilities, security software, application software, and data files necessary for recovery?

ANSWER Yes

ADDITIONAL INFORMATION Database backups capture all data; application code and infrastructure configuration are version controlled and redeployable from source, so recovery does not depend on backing up servers.

DATA-12 Are you performing off-site backups (i.e., digitally moved off site)?

ANSWER Yes

ADDITIONAL INFORMATION Database backups are managed off-instance by the provider; the document store is additionally copied nightly to a separate, credential-isolated cloud project, with independent alerting if the backup fails to run.

DATA-13 Are physical backups taken off-site (i.e., physically moved off site)?

ANSWER NA

ADDITIONAL INFORMATION No physical backup media exists.

DATA-14 Are data backups encrypted?

ANSWER Yes

ADDITIONAL INFORMATION Backups are encrypted at rest by the providers; the cross-project document backup resides in a private bucket accessible only to service credentials.

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?

ANSWER NA

ADDITIONAL INFORMATION Fully cloud hosted; no media in our custody. Provider (AWS) media lifecycle and sanitization controls apply, as covered by their attestations.

DATA-16 Does the process described in DATA-15 adhere to DoD 5220.22-M and/or NIST SP 800-88 standards?

ANSWER NA

ADDITIONAL INFORMATION See DATA-15.

DATA-17 Does your staff (or third party) have access to institutional data (e.g., financial, PHI, or other sensitive information) through any means?

ANSWER Yes

ADDITIONAL INFORMATION The founder (platform operator) can access institutional data for support and operations; such access is deliberate and minimal, and staff-level actions on student records are captured in the audit log. Subprocessors hold data only as described in the Organization tab, THRD-02.

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)?

ANSWER Yes

ADDITIONAL INFORMATION The company is fully remote with a single operator. The workstation is disk encrypted, screen locked, and kept current on OS security updates, and production access requires authenticated provider consoles. A formal written endpoint policy accompanies the first hire.

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).

ANSWER No

ADDITIONAL INFORMATION Multi-tenant with strict logical isolation: every tenant-scoped table carries PostgreSQL Row Level Security enforced at the database layer, so isolation does not depend on application code alone. Each program runs on its own subdomain. Isolation is verified by automated cross-tenant test suites that create real tenants and attempt cross-tenant reads and writes.

DATA-20 Are ownership rights to all data, inputs, outputs, and metadata retained by the institution?

ANSWER Yes

ADDITIONAL INFORMATION The institution retains ownership of all its data, inputs, outputs, and metadata.

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?

ANSWER Yes

DATA-22 Are involatile backup copies made according to predefined schedules and securely stored and protected?

ANSWER Yes

ADDITIONAL INFORMATION Daily encrypted database backups (rolling provider retention) and a nightly document storage backup to an isolated project. Backup jobs carry independent failure alerting: a missed run alerts the operator. Point-in-time recovery is not enabled; the recovery point is the most recent daily backup.

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.)?

ANSWER Yes

ADDITIONAL INFORMATION TLS certificates are automated and rotated by the platform. At-rest keys are managed by the cloud provider's key management. Application secrets live in encrypted platform configuration with access limited to the founder. The three application encryption keys, one for per-program SMS credentials, one for Outlook calendar tokens and one for per-program AI assistant API credentials, are separate dedicated 256-bit keys, so one leak exposes one kind of secret; each is rotatable on demand, and a build-time guard prevents secrets from reaching client bundles.

Infrastructure

Application/Service Security

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)?*

ANSWER Yes

ADDITIONAL INFORMATION Role-based access control with five program roles (administrator, advisor, assistant, observer, guest) plus a per-program capability matrix that the program's administrators set; every authorization is additionally enforced at the database layer by row level security.

APPL-02 Are you using a web application firewall (WAF)?*

ANSWER Yes

ADDITIONAL INFORMATION All traffic enters through the hosting platform's edge network with its managed firewall and DDoS mitigation; application-layer protections add bot detection (reCAPTCHA v3) on public forms and rate limiting on abuse-prone endpoints.

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?*

ANSWER Yes

ADDITIONAL INFORMATION Serverless runtimes are kept current by the platform; the application tracks current framework releases, and dependencies are monitored (Dependabot) with zero known critical or high severity vulnerabilities at submission. The web application supports current modern browsers.

APPL-04 Does your application require access to location or GPS data?

ANSWER No

ADDITIONAL INFORMATION No device location or GPS access. Address autocomplete operates on text the applicant types.

APPL-05 Does your application provide separation of duties between security administration, system administration, and standard user functions?*

ANSWER Yes

ADDITIONAL INFORMATION Institutional roles separate administration from advising from read-only access; platform administration is separate from institutional accounts; and the database independently rejects out-of-role writes.

APPL-06 Do you subject your code to static code analysis and/or static application security testing prior to release?*

ANSWER Yes

ADDITIONAL INFORMATION Every release passes strict static type checking and lint analysis as a required check, and dependency vulnerability scanning runs continuously. Dedicated security-focused static analysis tooling is a planned addition.

APPL-07 Do you have software testing processes (dynamic or static) that are established and followed?*

ANSWER Yes

ADDITIONAL INFORMATION Every release runs the full automated test suite (900+ test files, including regression tests that are mutation tested); changes are additionally exercised on a staging environment before production.

APPL-08 Are access controls for staff within your organization based on structured rules, such as RBAC, ABAC, or PBAC?

ANSWER Yes

ADDITIONAL INFORMATION Platform access is limited to the founder under least privilege; institutional staff access is role based as described in APPL-01.

APPL-09 Does the system provide data input validation and error messages?

ANSWER Yes

ADDITIONAL INFORMATION Server-side validation on all inputs (required-field enforcement, format validation, allowlisted fields on public submissions) with structured error messages that do not leak internals.

APPL-10 Do you have a process and implemented procedures for managing your software supply chain (e.g., libraries, repositories, frameworks, etc.)

ANSWER Yes

ADDITIONAL INFORMATION Dependencies are lockfile pinned with integrity hashes; a full supply chain audit verified the integrity of every lockfile entry; Dependabot alerts are enabled; and the engineering standard prefers in-repo implementations over new dependencies, keeping the surface small. All development is in-house.

APPL-11 Have your developers been trained in secure coding techniques?

ANSWER Yes

ADDITIONAL INFORMATION The developer (founder) applies secure coding practice as standard: parameterized data access, output encoding by framework default, least privilege, and adversarial review of security-relevant changes.

APPL-12 Was your application developed using secure coding techniques?

ANSWER Yes

ADDITIONAL INFORMATION See APPL-11; security-relevant paths receive dedicated adversarial review, and internal security audits examine the application for injection, cross-site scripting, authorization, and data-destruction classes.

APPL-13 If mobile, is the application available from a trusted source (e.g., App Store, Google Play Store)?

ANSWER NA

ADDITIONAL INFORMATION No mobile application; the product is a responsive web application.

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?

ANSWER Yes

ADDITIONAL INFORMATION Platform-level support access is limited to the founder, is used only for support and operations, and staff-level actions on student records are captured in the tenant-visible audit log.

Datacenter

DCTR-01 Select your hosting option.

ANSWER Hybrid/Other

ADDITIONAL INFORMATION Fully managed platform services: Vercel for application hosting and edge delivery, and Supabase for managed PostgreSQL, authentication, and document storage. Both run on AWS; the primary data region is us-east-1 (United States). TRIOPilot operates no servers of its own.

DCTR-02 Is a SOC 2 Type 2 report available for the hosting environment?

ANSWER Yes

ADDITIONAL INFORMATION AWS, Supabase, and Vercel each maintain SOC 2 Type 2 attestations, available from the providers.

DCTR-03 Are you generally able to accommodate storing each institution's data within its geographic region?

ANSWER Yes

ADDITIONAL INFORMATION Student records, documents and backups are stored in United States regions (AWS us-east-1). The rate limiting service keeps short-lived counter keys (IP addresses, user ids and sign-in email addresses) in its primary region, also AWS us-east-1. Hosting outside the United States is not currently offered.

DCTR-04 Are the data centers staffed 24 hours a day, seven days a week (i.e., $24 \times 7 \times 365$)?

ANSWER Yes

ADDITIONAL INFORMATION AWS data centers are staffed and monitored continuously, per AWS attestations.

DCTR-05 Are your servers separated from other companies via a physical barrier, such as a cage or hard walls?

ANSWER Yes

ADDITIONAL INFORMATION Physical separation and access controls per AWS data center attestations (SOC 2, ISO 27001).

DCTR-06 Does a physical barrier fully enclose the physical space, preventing unauthorized physical contact with any of your devices?*

ANSWER Yes

ADDITIONAL INFORMATION Per AWS physical security attestations (SOC 2, ISO 27001).

DCTR-07 Are your primary and secondary data centers geographically diverse?

ANSWER No

ADDITIONAL INFORMATION The primary data store runs in AWS us-east-1; backups are stored on separate infrastructure, and the application tier is globally distributed at the edge. Multi-region database failover is a roadmap item; recovery today is restore from backup.

DCTR-08 Is the service hosted in a high-availability environment?

ANSWER Yes

ADDITIONAL INFORMATION The application tier is serverless and highly available across availability zones. The managed database is a provider-operated instance with automated daily backups; database high availability upgrades are available from the provider as scale requires.

DCTR-09 Is redundant power available for all data centers where institutional data will reside?

ANSWER Yes

ADDITIONAL INFORMATION Per AWS attestations.

DCTR-10 Are redundant power strategies tested?*

ANSWER Yes

ADDITIONAL INFORMATION Tested by AWS per its attestations.

DCTR-11 Does the center where the data will reside have cooling and fire-suppression systems that are active and regularly tested?

ANSWER Yes

ADDITIONAL INFORMATION Per AWS attestations.

DCTR-12 Do you have Internet Service Provider (ISP) redundancy?

ANSWER Yes

ADDITIONAL INFORMATION Provider edge network and AWS network redundancy.

DCTR-13 Does every data center where the institution's data will reside have multiple telephone company or network provider entrances to the facility?

ANSWER Yes

ADDITIONAL INFORMATION Per AWS data center attestations.

DCTR-14 Do you require multifactor authentication for all administrative accounts in your environment?

ANSWER Yes

ADDITIONAL INFORMATION The provider consoles that administer the environment (hosting, database, source control) are held by the founder with multi-factor authentication enabled, and the founder, the only member of the error monitoring (Sentry) organization, also uses two-factor authentication there. In-app institutional accounts authenticate by possession of the verified email inbox (one-time codes).

DCTR-15 Are you using your cloud provider's available hardening tools or pre-hardened images?

ANSWER Yes

ADDITIONAL INFORMATION The platforms are managed services with hardened defaults; there are no self-built images. Platform security guidance (row level security enforcement, secret handling, key scoping) is followed and audited.

DCTR-16 Does your cloud solution provider have access to your encryption keys?

ANSWER Yes

ADDITIONAL INFORMATION At-rest encryption keys for the database and storage are managed by the cloud provider's key management service, as is standard for managed platforms. The application-layer credential encryption key is held only in our environment.

Firewalls, IDS, IPS, and Networking

FIDP-01 Are you utilizing a stateful packet inspection (SPI) firewall?*

ANSWER Yes

ADDITIONAL INFORMATION Network filtering is provided by the managed platforms (edge firewall, AWS security groups); TRIOPilot manages no network appliances of its own.

FIDP-02 Do you have a documented policy for firewall change requests?*

ANSWER NA

ADDITIONAL INFORMATION No customer-managed firewall exists. Network exposure is defined in version-controlled configuration, and changes flow through the documented change process.

FIDP-03 Have you implemented an intrusion detection system (network-based)?*

ANSWER Yes

ADDITIONAL INFORMATION At the platform layer by the infrastructure providers, covered by their SOC 2 Type 2 attestations; application-layer anomaly and error monitoring with alerting adds coverage.

FIDP-04 Do you employ host-based intrusion detection?*

ANSWER NA

ADDITIONAL INFORMATION Serverless; no hosts in our custody to instrument.

FIDP-05 Are audit logs available for all changes to the network, firewall, IDS, and IPS systems?*

ANSWER Yes

ADDITIONAL INFORMATION Provider console changes are captured in the providers' audit logs; application-level network configuration is version controlled with full history.

FIDP-06 Is authority for firewall change approval documented? Please list approver names or titles in Additional Info.

ANSWER Yes

ADDITIONAL INFORMATION Matt Acevedo, Founder: sole authority for production configuration changes.

FIDP-07 Have you implemented an intrusion prevention system (network-based)?

ANSWER Yes

ADDITIONAL INFORMATION Platform-layer protections including managed DDoS mitigation and firewall rules at the edge.

FIDP-08 Do you employ host-based intrusion prevention?

ANSWER NA

ADDITIONAL INFORMATION See FIDP-04.

FIDP-09 Are you employing any next-generation persistent threat (NGPT) monitoring?

ANSWER No

FIDP-10 Is intrusion monitoring performed internally or by a third-party service?

ANSWER Yes

ADDITIONAL INFORMATION Infrastructure intrusion monitoring is performed by the platform providers as part of their managed service. Application-layer monitoring is internal: error and anomaly monitoring with alerting (credentials stripped), platform firewall telemetry, and audit logging, reviewed by the operator.

FIDP-11 Do you monitor for intrusions on a 24 × 7 × 365 basis?

ANSWER No

ADDITIONAL INFORMATION Provider infrastructure is monitored continuously by the platform vendors. TRIOPilot's own application alert response is single-operator and not staffed around the clock; alerting notifies the founder immediately.

Incident Handling

HFIH-01 Do you have a formal incident response plan?

ANSWER No

ADDITIONAL INFORMATION A formal written incident response plan (severity model, contact tree, notification templates, annual tabletop) is in progress on the security roadmap. Current practice: monitoring alerts notify the operator, incidents are investigated immediately, remediated at root cause, and written up. A recent availability incident was investigated and remediated within the hour with a documented postmortem.

HFIH-02 Do you either have an internal incident response team or retain an external team?

ANSWER Yes

ADDITIONAL INFORMATION Internal: the founder is the incident responder, with escalation paths to the platform providers' support and status channels.

HFIH-03 Do you have the capability to respond to incidents on a 24 × 7 × 365 basis?

ANSWER No

ADDITIONAL INFORMATION Single-operator company; alerting is continuous and reaches the founder immediately, but a staffed around-the-clock response rotation does not exist.

HFIH-04 Do you carry cyber-risk insurance to protect against unforeseen service outages, data that is lost or stolen, and security incidents?

ANSWER No

ADDITIONAL INFORMATION Cyber liability insurance is not currently carried; it is under evaluation and can be discussed as part of contracting.

Vulnerability Management

VULN-01 Are your systems and applications scanned with an authenticated user account for vulnerabilities (that are remediated) prior to new releases?*

ANSWER No

ADDITIONAL INFORMATION Dedicated authenticated vulnerability scanning is not yet in place; it is planned alongside an independent penetration test. Compensating controls today: continuous dependency vulnerability monitoring with prompt remediation, a required pre-release automated test run, staging verification, and recurring internal adversarial security audits of the high-risk paths (authentication, tenant isolation, public intake, exports, storage).

VULN-02 Will you provide results of application and system vulnerability scans to the institution?*

ANSWER Yes

ADDITIONAL INFORMATION Dependency scan status and internal security audit summaries are available now; results of future application scans and penetration tests will be shared with customers under NDA.

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?*

ANSWER Yes

ADDITIONAL INFORMATION Yes, at a mutually agreed time and scope.

VULN-04 Have your systems and applications had a third-party security assessment completed in the last year?

ANSWER No

ADDITIONAL INFORMATION Not yet; an independent penetration test is a roadmap commitment. Internal audits with written reports have been performed (data loss, supply chain and malicious code, authentication architecture).

VULN-05 Do you regularly scan for common web application security vulnerabilities (e.g., SQL injection, XSS, XSRF, etc.)?

ANSWER No

ADDITIONAL INFORMATION No scheduled automated web-vulnerability scanning yet (planned). The architecture mitigates the common classes by construction: all data access is parameterized through the database API (no string-built SQL), the framework escapes output by default, authorization is enforced at the database layer, and internal security audits explicitly hunt injection, cross-site scripting, and authorization flaws.

VULN-06 Are your systems and applications regularly scanned externally for vulnerabilities?

ANSWER No

ADDITIONAL INFORMATION Planned; see VULN-01.

IT Accessibility

IT Accessibility

ITAC-01 Solution Provider Accessibility Contact Name

ANSWER Matt Acevedo

ITAC-02 Solution Provider Accessibility Contact Title

ANSWER Founder

ITAC-03 Solution Provider Accessibility Contact Email

ANSWER hello@triopilot.com

ITAC-04 Solution Provider Accessibility Contact Phone Number

ANSWER 305-204-1204

ITAC-05 Web Link to Accessibility Statement or VPAT

ANSWER Not yet published

ADDITIONAL INFORMATION An accessibility statement and VPAT/ACR have not yet been published; see ITAC-06.

ITAC-06 Has a VPAT or ACR been created or updated for the solution and version under consideration within the past 12 months?*

ANSWER No

ADDITIONAL INFORMATION A VPAT/ACR has not yet been produced. The product is built mobile-first with accessibility-conscious engineering (semantic HTML, labeled controls, keyboard paths for complex interactions); a formal WCAG evaluation and ACR are planned.

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?*

ANSWER No

ADDITIONAL INFORMATION We are not yet in a position to contractually warrant WCAG 2.1 AA because a formal conformance evaluation has not been performed. We are open to discussing a contractual accessibility roadmap commitment with the institution.

ITAC-08 Does the solution substantially conform to WCAG 2.1 AA?*

ANSWER No

ADDITIONAL INFORMATION Substantial conformance has not been formally verified. Engineering practice targets accessible patterns (keyboard operability including keyboard alternatives to drag-and-drop features, focus management for dialogs and menus, form labels, color contrast); a formal audit is planned.

ITAC-09 Do you have a documented and implemented process for reporting and tracking accessibility issues?*

ANSWER No

ADDITIONAL INFORMATION Accessibility issues are received through the in-product Share Feedback channel and email and are triaged into the engineering task list like defects; a dedicated documented accessibility reporting and tracking process is not yet in place.

ITAC-10 Do you have documentation to support the accessibility features of your solution?

ANSWER No

ADDITIONAL INFORMATION The product aims to be accessible in its default state with no special configuration; dedicated accessibility documentation has not yet been written.

ITAC-11 Has a third-party expert conducted an audit of the most recent version of your solution?

ANSWER No

ITAC-12 Do you have a documented and implemented process for verifying accessibility conformance?

ANSWER No

ADDITIONAL INFORMATION Not yet; verification is currently by engineering practice and review rather than a documented conformance process.

ITAC-13 Have you adopted a technical or legal standard of conformance for the solution?

ANSWER No

ADDITIONAL INFORMATION A formal standard has not yet been adopted; WCAG 2.1 AA is the working target.

ITAC-14 Can you provide a current, detailed accessibility roadmap with delivery timelines?

ANSWER No

ADDITIONAL INFORMATION A prioritized accessibility roadmap can be produced with the institution; a standing published roadmap does not yet exist.

ITAC-15 Do you expect your staff to maintain a current skill set in IT accessibility?

ANSWER Yes

ADDITIONAL INFORMATION The developer maintains current knowledge of accessibility practice and implements keyboard and assistive-technology paths as part of feature work.

ITAC-16 Do you have documented processes and procedures for implementing accessibility into your development lifecycle?

ANSWER No

ADDITIONAL INFORMATION Accessibility is considered during design and implementation (keyboard alternatives are required for pointer-driven features, and focus management is part of component review), but a formally documented lifecycle process does not yet exist; it is planned with the VPAT work.

ITAC-17 Can all functions of the application or service be performed using only the keyboard?

ANSWER Yes

ADDITIONAL INFORMATION Keyboard operability is an engineering requirement; complex pointer interactions (for example drag-and-drop configuration screens) ship with equivalent keyboard controls. A formal full-product keyboard audit will accompany the planned VPAT.

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?

ANSWER No

ADDITIONAL INFORMATION Single interface for all users; no overlay, lite mode, or AI-based alternate interface.

AI

AI Qualifying Questions

AIQU-01 Does your solution leverage machine learning (ML) or do you plan to do so in the next 12 months?

ANSWER No

ADDITIONAL INFORMATION TRIOPilot does not train or operate machine learning models of its own; the assistant calls a commercial large language model API. See AIQU-02.

AIQU-02 Does your solution leverage a large language model (LLM) or do you plan to do so in the next 12 months?

ANSWER Yes

ADDITIONAL INFORMATION The staff assistant uses a commercial large language model (Anthropic Claude) over Anthropic's official API.

General AI Questions

AIGN-01 Does your solution have an AI risk model when developing or implementing your solution's AI model?*

ANSWER Yes

ADDITIONAL INFORMATION The assistant's design is explicitly threat-modeled against LLM risk classes, aligned with the OWASP Top 10 for LLM applications: least-privilege tools, no write path inside the model loop, prompt-injection containment by construction, and per-tenant usage caps. The design document is available for review.

AIGN-02 Can your solution's AI features be disabled by tenant and/or user?*

ANSWER Yes

ADDITIONAL INFORMATION Per-tenant enable switch, default OFF; the institution's administrator controls it. A platform-level kill switch (revoking the provider key) hard-disables the feature everywhere, failing closed.

AIGN-03 Have your staff completed responsible AI training?*

ANSWER NA

ADDITIONAL INFORMATION No staff beyond the founder, who designed the feature's responsible-use constraints; responsible AI training will accompany the first hire.

AIGN-04 Please describe the capabilities of your solution's AI features.

ANSWER An optional, staff-only chat assistant for program staff: it looks up students the signed-in user is already authorized to see, counts and groups them, prepares filtered lists and CSV exports through the product's existing reporting machinery, answers questions from the help center, and drafts contact log entries and text messages. It cannot write data or send a message itself: a person reviews each draft and clicks to save a contact log entry, or presses Send on a text draft card, which posts to the same Bulk Texts route with the same permission checks as the Bulk Texts screen. It never computes federal APR numbers and never generates database queries; it calls a fixed set of thirteen tools that wrap existing authorization-scoped product code, so row level security and role permissions apply identically to assistant use and direct use. Status: generally available; disabled by default for every program, and each program's administrators decide whether to turn it on. Each program's AI traffic can run under its own API credential and spend limit, which TRIOPilot can revoke for that program alone. A program's own credential is encrypted with AES-256-GCM under a key used for nothing else, and a credential that cannot be used turns the assistant off for that program rather than falling back to TRIOPilot's. Provider data handling is governed by Anthropic's commercial terms, which incorporate the Anthropic Data Processing Addendum, prohibit training on customer content, and automatically delete API inputs and outputs within 30 days.

AIGN-05 Does your solution support business rules to protect sensitive data from being ingested by the AI model?

ANSWER Yes

ADDITIONAL INFORMATION The assistant can reach data only through fixed, parameterized tools that enforce the signed-in user's own role and tenant permissions at the database layer; there is no free-form data ingestion, and conversations are ephemeral (not stored).

AI Policy

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?*

ANSWER No

ADDITIONAL INFORMATION Customer documentation is published in the help center (Use the AI Assistant). A separate AI policy document is not yet published. The internal design specification documenting the risk decisions exists and is available for review.

AIPL-02 Have you identified and measured AI risks?*

ANSWER Yes

ADDITIONAL INFORMATION Documented in the design specification: FERPA exposure, prompt injection, over-privilege, and cost abuse, each with a structural mitigation (draft-then-confirm writes, a fixed tool allowlist, session-scoped authorization, and per-tenant metered caps).

AIPL-03 In the event of an incident, can your solution's AI features be disabled in a timely manner?*

ANSWER Yes

ADDITIONAL INFORMATION Immediate: the institution's administrator can switch the feature off per tenant at any time, and the platform operator can disable it globally within minutes by revoking the provider key (the feature fails closed without it).

AIPL-04 If disabled because of an incident, can your solution's AI features be re-enabled in a timely manner?*

ANSWER Yes

ADDITIONAL INFORMATION Re-enabling is the same switch; restoration is immediate once an incident is resolved.

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)?

ANSWER No

ADDITIONAL INFORMATION Formal NIST AI RMF process documentation does not yet exist. The feature's documented design constraints (human confirmation of all writes, least privilege, no aggregate or eligibility computation by the model) address the practical harm classes for this use case.

AI Data Security

AISC-01 If sensitive data is introduced to your solution's AI model, can the data be removed from the AI model by request?*

ANSWER Yes

ADDITIONAL INFORMATION Institutional data never enters the model itself: the provider is contractually barred from training on customer content, so there is nothing in the model to remove. TRIOPilot stores no conversations, and the provider automatically deletes API inputs and outputs within 30 days under its commercial terms. A provider zero data retention configuration (removing even that 30 day window) is under evaluation.

AISC-02 Is user input data used to influence your solution's AI model?*

ANSWER No

ADDITIONAL INFORMATION The commercial API is contractually barred from training on customer inputs or outputs (Anthropic commercial terms), and the product exposes no feedback mechanism that would opt any conversation into training. Prompts and responses are used only to generate the answer and are automatically deleted by the provider within 30 days.

AISC-03 Do you provide logging for your solution's AI feature(s) that includes user, date, and action taken?*

ANSWER Yes

ADDITIONAL INFORMATION Any data change the assistant drafts is committed only by a human through the standard product paths, which are fully captured in the tenant-visible audit log (actor, timestamp, action). Assistant usage is metered per tenant. Conversations themselves are deliberately ephemeral and not stored.

AISC-04 Please describe how you validate user inputs.

ANSWER Assistant requests require an authenticated product session. Tool calls are schema validated with typed parameters; every tool executes through the same server-side authorization (role capabilities plus database row level security) as the equivalent screen in the product; the loop is bounded, with per-tenant usage caps; and the write path requires human review and confirmation outside the model loop, which structurally contains prompt injection.

AISC-05 Do you plan for and mitigate supply-chain risk related to your AI features?

ANSWER Yes

ADDITIONAL INFORMATION The AI surface is a single first-party provider (Anthropic) over its official SDK; no model artifacts or third-party plugins are used. The dependency is covered by the same lockfile integrity and audit controls as the rest of the application.

AI Large Language Model (LLM)

AILM-01 Do you limit your solution's LLM privileges by default?*

ANSWER Yes

ADDITIONAL INFORMATION The model has no privileges of its own: it can only invoke thirteen read or draft tools that execute under the signed-in user's session and permissions. There is no commit path inside the loop and no service-role database access anywhere in the feature.

AILM-02 Is your LLM training data vetted, validated, and verified before training the solution's AI model?*

ANSWER NA

ADDITIONAL INFORMATION TRIOPilot does not train or tune the model; it uses the provider's commercial model as-is.

AILM-03 Do any actions taken by your solution's LLM features or plugins require human intervention?*

ANSWER Yes

ADDITIONAL INFORMATION Structurally: the assistant can only draft changes (for example a contact log entry); a human must review and click to save. The save endpoint is not callable from inside the model loop.

AILM-04 Do you limit multiple LLM model plugins being called as part of a single input?*

ANSWER Yes

ADDITIONAL INFORMATION The tool loop is bounded (limited tool calls per turn) with a fixed first-party tool set of thirteen; there are no third-party plugins.

AILM-05 Do you limit your solution's LLM resource use per request, per step, and per action?

ANSWER Yes

ADDITIONAL INFORMATION Bounded loop per request plus per-tenant monthly usage caps with atomic reservation, with visibility and warnings at 80 percent of the cap.

AILM-06 Do you leverage LLM model tuning or other model validation mechanisms?

ANSWER No

ADDITIONAL INFORMATION No fine-tuning. Output reliability comes from constrained tools and mandatory human confirmation before any data changes.

Privacy

General Privacy

PRGN-01 Does your solution process FERPA-related data?

ANSWER Yes

ADDITIONAL INFORMATION Student education records are the core data. TRIOPilot operates as a school official under FERPA per its agreement with each institution.

PRGN-02 Does your solution process GDPR-related or PIPL-related data?

ANSWER No

ADDITIONAL INFORMATION The service is offered to United States institutions; there is no EEA or China collection or processing.

PRGN-03 Does your solution process personal data regulated by state law(s) (e.g., CCPA)?

ANSWER Yes

ADDITIONAL INFORMATION Personal data of state residents is processed on the institution's behalf; applicable state education records and breach notification laws are honored under the FERPA school-official model and the service agreement.

PRGN-04 Does your solution process user-provided data that may contain regulated information?

ANSWER Yes

ADDITIONAL INFORMATION Free-text fields (advisor notes, comments) may contain regulated information entered by staff; they are protected identically to structured student data.

PRGN-05 Web Link to Product/Service Privacy Notice

ANSWER <https://triopilot.com/privacy>

Privacy-Specific Company Details

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?*

ANSWER No

ADDITIONAL INFORMATION No personal data breach has occurred.

PCOM-02 Use this area to share information about your privacy practices that will assist those who are assessing your company data privacy program.*

ANSWER Data minimization is a design rule: the platform stores no Social Security numbers (they are structurally excluded, including from legacy data imports), collects only fields needed for program operations and federal APR reporting, and strips credentials from error telemetry before it leaves the platform (error monitoring runs under Sentry's data processing agreement, signed 2026-09-18). The institution controls collection through its own configurable application form, controls which optional features (SMS, student portal, AI assistant) are enabled, and sees a complete audit trail of staff actions on records. Access is passwordless and role scoped, with database-level row security as the isolation backstop. All processing is in the United States, and the subprocessor list is deliberately short (see Organization THRD-02).

PCOM-03 Have you had any data privacy policy or law violations in the past 36 months?

ANSWER No

PCOM-04 Do you have a dedicated data privacy staff or office?

ANSWER No

ADDITIONAL INFORMATION No dedicated privacy office; the founder (named Security Owner) is accountable for privacy. External counsel is engaged as needed for FERPA contract terms.

Privacy-Specific Documentation

PDOC-01 If you have completed a SOC 2 audit, does it include the Privacy Trust Service Principle?

ANSWER NA

ADDITIONAL INFORMATION No SOC 2 audit has been performed yet; see Organization DOCU-03.

PDOC-02 Do you conform with a specific industry-standard privacy framework (e.g., NIST Privacy Framework, GDPR, ISO 27701)?

ANSWER No

ADDITIONAL INFORMATION No formal certification. Practices follow the FERPA school-official model with a documented data inventory, classification, and minimization rules.

PDOC-03 Does your employee onboarding and offboarding policy include training of employees on information security and data privacy?

ANSWER NA

ADDITIONAL INFORMATION No employees to onboard; security and privacy training obligations will accompany the first hire.

Privacy of Third Parties

PTHP-01 Do you have contractual agreements with third parties that require them to maintain standards and to comply with all regulatory requirements?*

ANSWER Yes

ADDITIONAL INFORMATION Each subprocessor operates under its published data processing agreement and terms committing it to security and regulatory compliance; the complete list with purposes is in Organization THRD-02.

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?

ANSWER No

ADDITIONAL INFORMATION Formal privacy impact assessments of vendors are not yet performed; vendor selection reviews security attestations and data processing terms, and the subprocessor list is deliberately short with documented data flows for each.

Privacy Change Management

PCHG-01 Does your change management process include privacy review and approval?

ANSWER Yes

ADDITIONAL INFORMATION Privacy impact is an explicit consideration in review of any change touching student data; FERPA-relevant surfaces (what students see, what staff see, what leaves the platform) receive dedicated review, and credential stripping in telemetry is regression tested.

PCHG-02 Do you have policy and procedure, currently implemented, guiding how privacy risks are mitigated until they can be resolved?

ANSWER Yes

ADDITIONAL INFORMATION Identified privacy risks are mitigated with structural controls before features ship (features default off, data is withheld rather than exposed when uncertain, credentials are stripped from telemetry); interim mitigations are documented in the engineering record until root-cause resolution.

Privacy of Sensitive Data

PDAT-01 Do you collect, process, or store demographic information?*

ANSWER Yes

ADDITIONAL INFORMATION As required for Federal TRIO program operations and the Department of Education Annual Performance Report: race and ethnicity, sex, eligibility, and educational status, entered by the institution or its applicants and reported only to the institution.

PDAT-02 Do you capture or create genetic, biometric, or biometric information (e.g., facial recognition or fingerprints)?*

ANSWER No

ADDITIONAL INFORMATION No biometric identification. The application form can capture a drawn signature image as part of a standard e-signature; it is stored as a document image and never used for recognition.

PDAT-03 Do you combine institutional data (including "de-identified," "anonymized," or otherwise masked data) with personal data from any other sources?*

ANSWER No

ADDITIONAL INFORMATION Institutional data is never combined with outside sources, sold, or used beyond providing the service to that institution.

PDAT-04 Is institutional data coming into or going out of the United States at any point during collection, processing, storage, or archiving?

ANSWER No

ADDITIONAL INFORMATION Student records, documents and backups are collected, processed and stored in United States regions (AWS us-east-1). The rate limiting service keeps short-lived counter keys (IP addresses, user ids and sign-in email addresses) in its primary region, also AWS us-east-1. The service is offered to United States institutions only.

PDAT-05 Do you capture device information (e.g., IP address, MAC address)?

ANSWER Yes

ADDITIONAL INFORMATION Standard web telemetry: IP addresses appear in transient platform request logs and authentication logs for security purposes, and the bot-protection service evaluates interaction signals on the public form. No device fingerprinting for tracking.

PDAT-06 Does any part of this service/project involve a web/app tracking component (e.g., use of web-tracking pixels, cookies)?

ANSWER Yes

ADDITIONAL INFORMATION Essential cookies only (authentication session, active-program selection). Hosting analytics (Vercel Web Analytics and Speed Insights) receive redacted page paths and timings only, with no cookies and no identifiers. No Google Analytics, no advertising, and no cross-site tracking. Google reCAPTCHA v3 runs on the public application form for bot protection.

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?

ANSWER Yes

ADDITIONAL INFORMATION See Product DATA-17: operator support access exists, is minimal and deliberate, and staff-level record actions are audit logged. Subprocessor access is limited to the flows in Organization THRD-02.

PDAT-08 Will you handle personal data in a manner compliant with all relevant laws, regulations, and applicable institution policies?

ANSWER Yes

ADDITIONAL INFORMATION FERPA (school-official model), applicable state education records and breach notification laws, and institutional policies incorporated into the service agreement.

Privacy Policies and Procedures

PRPO-01 Do you have a documented privacy management process?

ANSWER No

ADDITIONAL INFORMATION A formal privacy management process document is in progress. In place today: a published privacy policy, a documented data inventory with classification, data minimization rules enforced in code, and named accountability (Security Owner).

PRPO-02 Are privacy principles designed into the product lifecycle (i.e., privacy-by-design)?

ANSWER Yes

ADDITIONAL INFORMATION Demonstrably: a structural no-SSN rule, ephemeral AI conversations, default-off feature flags, student-visibility decisions that default to withholding, credential-stripped telemetry, and per-year data scoping.

PRPO-03 Will you comply with applicable breach notification laws?

ANSWER Yes

PRPO-04 Will you comply with the institution's policies regarding user privacy and data protection?

ANSWER Yes

PRPO-05 Is your company subject to the laws and regulations of the institution's geographic region?

ANSWER Yes

ADDITIONAL INFORMATION United States (a Wyoming limited liability company, operating from Florida): the same jurisdiction as the institution.

PRPO-06 Do you have a privacy awareness/training program?*

ANSWER No

ADDITIONAL INFORMATION No employees; the founder maintains working FERPA knowledge. A privacy training program accompanies the first hire.

PRPO-07 Is privacy awareness training mandatory for all employees?

ANSWER NA

ADDITIONAL INFORMATION See PRPO-06.

PRPO-08 Is AI privacy and ethics awareness/training required for all employees who work with AI?

ANSWER NA

ADDITIONAL INFORMATION See PRPO-06; it will be required for any future staff working with the AI features.

PRPO-09 Do you have any decision-making processes that are completely automated (i.e., there is no human involvement)?

ANSWER No

ADDITIONAL INFORMATION No fully automated decisions about individuals. Program staff make all participant decisions; automated record-status derivations merely apply the federal reporting definitions the institution configures, and staff can override them.

PRPO-10 Do you have a documented process for managing automated processing, including validations, monitoring, and data subject requests?

ANSWER NA

ADDITIONAL INFORMATION No automated decision-making in scope; see PRPO-09.

PRPO-11 Do you have a documented policy for sharing information with law enforcement?

ANSWER No

ADDITIONAL INFORMATION Not yet documented. Position: institutional data is disclosed only under legally valid compulsory process, and the institution is notified unless legally prohibited. This will be formalized in the policy set.

PRPO-12 Do you share any institutional data with law enforcement without a valid warrant?*

ANSWER No

PRPO-13 Does your incident response team include a privacy analyst/officer?

ANSWER No

ADDITIONAL INFORMATION Single-operator company: the founder acts as both incident responder and privacy owner.

International Privacy

INTL-01 Will data be collected from or processed in or stored in the European Economic Area (EEA)?

ANSWER No

INTL-02 Do you have a data protection officer (DPO)?

ANSWER No

ADDITIONAL INFORMATION Privacy accountability is held by the founder as Security Owner; a DPO is not required for this United States service.

INTL-03 Will you sign appropriate GDPR Standard Contractual Clauses (SCCs) with the institution?

ANSWER NA

ADDITIONAL INFORMATION No EEA data is processed, so SCCs are not applicable; we will review if circumstances change.

INTL-04 Will data be collected from or processed in or stored in China?

ANSWER No

INTL-05 Do you comply with PIPL security, privacy, and data localization requirements?

ANSWER NA

ADDITIONAL INFORMATION No China data processing.

Data Privacy

DRPV-01 Have you performed a Data Privacy Impact Assessment for the solution/project?

ANSWER No

ADDITIONAL INFORMATION A formal DPIA document has not been produced; a documented data inventory, classification, and risk register cover the same ground and are available for review.

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?

ANSWER Yes

ADDITIONAL INFORMATION <https://triopilot.com/privacy>, plus consent and FERPA language presented on the student application itself, configurable by the institution.

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?

ANSWER Yes

ADDITIONAL INFORMATION Applicants complete the institution's application voluntarily with notice; SMS messaging requires explicit opt-in consent with STOP and START honored automatically; the optional student portal requires the student to verify their identity to activate it.

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?

ANSWER Yes

ADDITIONAL INFORMATION Data is collected and used solely to operate the service for the institution; there is no secondary use, advertising, or sale.

DRPV-05 Do you have a documented list of personal data your service maintains?

ANSWER Yes

ADDITIONAL INFORMATION A documented data inventory lists every store of personal data with classification and purpose.

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?

ANSWER Yes

ADDITIONAL INFORMATION Data is retained for the life of the service agreement and returned then deleted at offboarding (see Product DATA-09). Formal per-category retention schedules are being added to the policy set. The institution can also delete individual records in-product, with recoverable tombstones guarding against accidental destruction.

DRPV-07 Do you provide individuals with access to their personal information for review and update (i.e., data subject rights)?

ANSWER Yes

ADDITIONAL INFORMATION Under FERPA the institution is the point of access for its students; the product supports this with complete record views and exports. An optional read-only student portal (off by default, institution controlled) lets a verified student see their own record.

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?

ANSWER Yes

ADDITIONAL INFORMATION Disclosure is limited to the subprocessors necessary to run the service (Organization THRD-02); nothing is shared for any other purpose.

DRPV-09 Do you protect personal information against unauthorized access (both physical and logical)?

ANSWER Yes

ADDITIONAL INFORMATION Logical: passwordless authentication, role-based access control, database row level security, TLS, encryption at rest. Physical: SOC 2 attested provider data centers; no company facilities hold data.

DRPV-10 Do you maintain accurate, complete, and relevant personal information for the purposes identified in the privacy notice?

ANSWER Yes

ADDITIONAL INFORMATION The institution's staff maintain records directly; every edit is attributed and logged, and duplicate-record detection with human-reviewed merge protects record integrity.

DRPV-11 Do you have procedures to address privacy-related noncompliance complaints and disputes?

ANSWER Yes

ADDITIONAL INFORMATION Complaints and disputes are received at hello@triopilot.com and through the in-product issue channel, and are handled by the Security Owner.

DRPV-12 Do you "anonymize," "de-identify," or otherwise mask personal data?

ANSWER No

ADDITIONAL INFORMATION No anonymized or de-identified derivative datasets are produced; data is used only in identified form to operate the service.

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)?

ANSWER No

ADDITIONAL INFORMATION Institutional data is not used for advertising, profiling, resale, or unrelated analytics by us or by any subprocessor.

DRPV-14 Do you certify stop-processing requests, including any data that is processed by a third party on your behalf?

ANSWER Yes

ADDITIONAL INFORMATION A stop-processing request is honored across the platform and its subprocessors, and completion is confirmed in writing.

DRPV-15 Do you have a process to review code for ethical considerations?

ANSWER No

ADDITIONAL INFORMATION No dedicated ethics review process. Product decisions with student impact are made deliberately by the accountable owner and documented in the engineering record, and the AI feature's human-confirmation constraints reflect this.

Privacy and AI

DPAI-01 Does your service use AI for the processing of institutional data?

ANSWER Yes

ADDITIONAL INFORMATION The optional staff assistant (disabled by default for every program; each program's administrators decide whether to turn it on): when turned on, it reads data the signed-in staff member is already authorized to see, in order to answer that staff member's questions. Separately, the operator's support work, including an automated support triage routine, uses Anthropic's Claude Code under a Claude Max plan, which is governed by Anthropic's consumer terms rather than its commercial terms, so support reports and production error details (which can identify a student) are processed as model input; that account's setting to use data for model training is off. No other AI processing occurs.

DPAI-02 Is any institutional data retained in the AI processing?*

ANSWER Yes

ADDITIONAL INFORMATION Not by TRIOPilot (conversations are ephemeral and never stored) and never in any model, but the AI provider transiently retains API inputs and outputs for up to 30 days before automatic deletion under its commercial terms; abuse and legal holds can extend that in exceptional cases. A provider zero data retention configuration is under evaluation to remove the 30 day window.

DPAI-03 Do you have agreements in place with third parties or subprocessors regarding the protection of customer data and use of AI?*

ANSWER Yes

ADDITIONAL INFORMATION Yes. TRIOPilot uses the Anthropic API under Anthropic's Commercial Terms of Service, which incorporate the Anthropic Data Processing Addendum by reference and contractually prohibit training models on customer content; API inputs and outputs are automatically deleted within 30 days.

DPAI-04 Will institutional data be processed through a third party or subprocessor that also uses AI?

ANSWER No

ADDITIONAL INFORMATION The only AI subprocessor is Anthropic itself.

DPAI-05 Is AI processing limited to fully licensed commercial enterprise AI services?

ANSWER Yes

ADDITIONAL INFORMATION The in-product assistant uses Anthropic's commercial API only (Anthropic Claude). The operator's support work uses Anthropic's Claude Code under a Claude Max plan (Anthropic's consumer terms), as described in DPAI-01. No other AI tools or shared services are used.

DPAI-06 Will institutional data be used or processed by any shared AI services?

ANSWER No

ADDITIONAL INFORMATION See DPAI-05.

DPAI-07 Do you have safeguards in place to protect institutional data and data privacy from unintended AI queries or processing?

ANSWER Yes

ADDITIONAL INFORMATION The feature is off by default per tenant and hard-off platform-wide without the provider key; for the assistant, AI processing happens only when a signed-in staff member deliberately asks the assistant a question, and scoped tools prevent access beyond that user's permissions.

DPAI-08 Do you provide choice to the user to opt out of AI use?

ANSWER Yes

ADDITIONAL INFORMATION The institution opts in per tenant and can disable the feature at any time; individual staff simply do not use the assistant if they prefer, and no program data flows to the AI provider through the assistant except during a staff-initiated conversation (support work is described in DPAI-01).