Security questionnaire answers

Answers in the format of the HECVAT Lite used by colleges and universities, version 1.1, November 12, 2026.

> This document answers the topics of the HECVAT Lite in our own words. It is not the EDUCAUSE workbook itself. If your institution uses the official HECVAT workbook or its own questionnaire, email support@outcomespath.com and we will complete it. Answers describe the service as of the date above and are confirmed in the contract.

Company and product

#	Question	Answer	Details
1	Name of the product and the company that provides it	**See details**	OutcomesPath, a case management and outcome tracking service, provided by OutcomesPath LLC, 347 5th Ave Ste 1402-405, New York NY 10016. Contact: support@outcomespath.com.
2	Is the product delivered as software as a service in a web browser?	**Yes**	Staff app at app.outcomespath.com, participant and partner portals in the same app, public website at www.outcomespath.com. Nothing is installed on campus or agency computers.
3	Does the product store or process personally identifiable information?	**Yes**	Participant names, contact details, program status, intake details, demographics the organization chooses to collect, notes, referrals, outcomes such as credentials, employment and wages, uploaded documents, and signed forms.
4	Can the product hold education records covered by FERPA?	**Yes**	Colleges and schools can record student enrollment, credentials and outcomes. OutcomesPath acts as a school official under the institution's direct control and uses records only to provide the service. See the sample data privacy agreement.
5	Does the vendor sell customer data or use it for advertising?	**No**	Never. Participant information is not sold, not used for advertising, and not used to train artificial intelligence models.

Documentation and assurance

#	Question	Answer	Details
1	Has the vendor completed a SOC 2 Type II examination of its own service?	**No**	Not yet. Controls are mapped to the SOC 2 Trust Services Criteria and NIST SP 800-53 Moderate. The infrastructure providers (Supabase on AWS, Netlify) hold SOC 2 Type II reports, and AWS holds ISO 27001.

2	Has an independent firm performed a penetration test?	**No**	Not yet. Every release passes a written security gate based on the OWASP Developer Guide web application checklist, including tests of row-level security with hostile accounts from other organizations and every role. A summary of the latest internal review is available on request.
3	Are security policies documented?	**Yes**	The public Security page states hosting, access control, encryption, audit, backups, availability, incident response, retention, deletion and subprocessors. The control matrix, system description and policies are available to prospective customers on request.
4	Is there an accessibility conformance report (VPAT)?	**Yes**	An Accessibility Conformance Report in the VPAT 2.5 WCAG format is on the procurement page.
5	Can the vendor provide proof of cyber liability insurance and a W-9?	**On request**	Email support@outcomespath.com.

Hosting and data location

#	Question	Answer	Details
1	Where is customer data stored?	**United States**	In the United States. The database is a managed PostgreSQL service from Supabase hosted on AWS in the United States. Web pages are served by Netlify.
2	Is customer data kept separate from other customers?	**Yes**	Every organization is a separate tenant. Row-level security in the database enforces the boundary for every query, not only the screens.
3	Is data encrypted in transit?	**Yes**	HTTPS everywhere with HSTS. A content security policy limits scripts, frames and connections to named services.
4	Is data encrypted at rest?	**Yes**	By the database and storage provider.
5	Are uploaded files kept private?	**Yes**	Case documents are in private storage. A file opens only for staff who can see that case file and for the participant, through a signed link that expires in two minutes. File types are limited to PDF, images and Word, up to 10 MB.

Authentication and access

#	Question	Answer	Details
1	Does the product support single sign-on?	**Yes**	Sign in with Google or Microsoft. On Enterprise plans, SAML 2.0 single sign-on with the institution's identity provider (for example Microsoft Entra ID, Okta or Google Workspace), set up with the institution's IT team.

2	Is multi-factor authentication available?	**Yes**	Authenticator-app two-factor sign-in for every staff account. An organization can require it for all staff; the database then returns no records to a session that has not verified a code. New organizations require it by default.
3	Is access role based?	**Yes**	Owner, admin, caseworker, viewer, participant, referral partner and employer. Admins set caseworker permissions, including limiting a caseworker to assigned participants, enforced in the database. Permission groups apply the same permissions to a team.
4	Do sessions time out?	**Yes**	Staff after 30 minutes of inactivity by default (each organization can set 15 minutes to 2 hours); participants and partners after 60 minutes.
5	Can vendor staff see customer records?	**Partly**	Only when an owner or admin grants read-only support access for 1 hour to 3 days. Support cannot change, export or delete records, every screen opened is logged, and access ends on its own or when the organization ends it. Support never asks for passwords.
6	Is there a periodic access review?	**Yes**	Owners and admins run a one-click access review listing every staff, partner and employer login with role, permissions, two-factor status and last sign-in.

Logging and monitoring

#	Question	Answer	Details
1	Are user actions logged?	**Yes**	Logins, logouts, messages, record changes, status and outcome changes, exports, document uploads and views, signed forms, settings and permission changes, written by the database with who, when and from what browser. Admins can filter and export the log.
2	Is there security monitoring?	**Yes**	An hourly watch checks that live app and website files match the release, that every table keeps row-level security, and looks for new admins, two-factor turned off, unusual exports or deletions, and request floods, and emails alerts to the security inbox.

Application security

#	Question	Answer	Details
1	Is input validated on the server?	**Yes**	Database checks and triggers validate every write, including public form answers against the form's own questions and signature rules. The app never builds SQL from text.
2	Are third-party libraries tracked and updated?	**Yes**	Libraries are copied onto our own servers at known versions and reviewed each release for published vulnerabilities.

3	Are AI features optional?	**Yes**	Owners and admins turn every AI feature off with one switch. The help assistant never receives participant names, emails, phone numbers or what is typed into fields. The AI provider's API terms state data is not used for training.
4	Does the service offer an API?	**Yes**	A read-only data API (v3.29). Only an owner creates a key; it is shown once and only its SHA-256 fingerprint is stored. Each key reads only its own organization and only the kinds of data the owner chose, never notes, messages, documents, enrollment answers or demographics. Keys expire (two years at most), are limited to 120 requests a minute, can be turned off at once, and their use is logged.
5	Can customer data leave the customer's organization?	**Only when the customer chooses**	Funder share links show totals only, hide any count from 1 to 4, show demographics only for groups of 10 or more, expire, and can be turned off. Referrals to another organization through the OutcomesPath Network carry only the person's name, contact details, need and the caseworker's note, and only after the person agrees; the agreement is recorded. Email notices never name the person.
6	Is the AI note assistant optional?	**Yes**	Off until an owner or admin turns it on, and always off when AI is off for the organization. The participant's name is replaced before the text is sent, emails and phone numbers are removed again on the server, and nothing is saved until staff add the note.

Business continuity and incidents

#	Question	Answer	Details
1	Are backups taken?	**Yes**	Daily by the database provider, with point-in-time recovery available. Recovery time objective: 8 hours for the application, 24 hours for a full database restore. Recovery point objective: 24 hours (2 minutes with point-in-time recovery).
2	What is the availability target?	**99.5 percent**	99.5 percent monthly, excluding announced maintenance, which is scheduled outside 7 a.m. to 7 p.m. Eastern on weekdays with 48 hours' notice.
3	Will the vendor notify customers of a breach?	**Yes**	The organization's owner and security contact are notified by email within 72 hours of confirmation, sooner where law or contract requires, with a written summary of cause and steps taken.

Data lifecycle

#	Question	Answer	Details

1	Can the customer export all of its data?	**Yes**	Any time, in Excel or CSV, by staff with the export permission.
2	Is there a retention schedule?	**Yes**	Each organization sets how long closed cases are kept (one to ten years, seven by default). A weekly job removes cases past that period with their documents and writes the count to the activity log.
3	Is data deleted at the end of the contract?	**Yes**	30 days to export at no cost, with a full export on request, then deletion from the live service, and from backups within 30 days after that, except records the law requires to be kept.
4	Are subprocessors disclosed?	**Yes**	Supabase, Netlify, Resend, Twilio (only when texting is on), Stripe, Anthropic (AI features, which can be turned off) and Google Fonts (career tool pages only). Customers get 30 days' notice of a new subprocessor.

Accessibility

#	Question	Answer	Details
1	Does the product conform to WCAG 2.2 Level AA?	**Partly**	Built and tested to WCAG 2.2 AA with automated testing on every screen and keyboard testing. Exceptions are listed in the Accessibility Conformance Report.
2	Is the participant portal available in Spanish?	**Yes**	The portal screens switch to Spanish with one tap. The career tools and short courses are in English for now.