

## Security questionnaire answers (HECVAT-style summary)

The questions purchasing and IT security offices ask most often about Astra FP&A K-12, with short answers. **In place** means it works in the product today. **In the DPA** means it is a commitment in our Data Processing Agreement. **Not yet** means it isn't in place. A full HECVAT is available on request.

### The data we hold

| Question                                             | Answer                                                                                                                                                                                                                                                                                 | Status     |
|------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|
| <b>What data does Astra FP&amp;A K-12 hold?</b>      | Totals and summaries only, uploaded by the district's own staff: ledger and budget totals, enrollment counts, personnel cost summarized by group, and similar figures. No records about individual students or employees.                                                              | In place   |
| <b>What if a file contains personal information?</b> | Every uploaded file and document is scanned before it is stored. A file whose columns or values look like names, ID numbers, Social Security numbers, dates of birth, email addresses, phone numbers, home addresses, or bank or card numbers is refused, and nothing in it is loaded. | In place   |
| <b>Is our data used to train AI models?</b>          | No. Customer data is never used to train AI models. Under our agreement with the AI provider, it doesn't use this content to train its models either.                                                                                                                                  | In place   |
| <b>Where is data stored?</b>                         | In the United States. The provider and its subprocessors store and process customer data in the United States and won't move it outside the United States without the customer's written consent (Data Processing Agreement, section 12).                                              | In the DPA |
| <b>Who hosts Astra FP&amp;A K-12?</b>                | Production hosting is in the United States, with the provider named in the Data Processing Agreement's subprocessor list (section 7). Data is encrypted in transit with TLS, and the database and backups are encrypted at rest through the hosting provider (section 6).              | In the DPA |

## Isolation and access

| Question                                                 | Answer                                                                                                                                                                                                                                                                    | Status     |
|----------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|
| <b>How is our data kept apart from other customers'?</b> | Every data table carries the district's ID, and Postgres row-level security limits every query to one district. The policies are forced and the application's database role can't bypass them, so a mistake in application code still can't read another district's rows. | In place   |
| <b>Who in our district can see what?</b>                 | Owners invite people as owners, analysts or viewers, and choose which areas each role can open, such as personnel and salary figures. Hidden areas are blocked on the server, and the AI analyst can't read them for that person either.                                  | In place   |
| <b>Can the vendor's staff see our data?</b>              | Only to provide support you ask for, to keep the service secure, or as the law requires. Access is limited to personnel who need it, using individual accounts with two-step verification (Data Processing Agreement, sections 5 and 6).                                  | In the DPA |

## Sign-in

| Question                                                  | Answer                                                                                                                                                                                                                            | Status   |
|-----------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------|
| <b>How are passwords protected?</b>                       | Passwords must be at least 12 characters and are stored only as Argon2 hashes. Sign-in is throttled after 5 failed attempts. Session tokens are stored as hashes.                                                                 | In place |
| <b>Is two-step verification available?</b>                | Yes: passkeys (Touch ID, Face ID, Windows Hello or a security key) and authenticator-app codes, with ten one-time recovery codes stored as hashes. Authenticator secrets are encrypted at rest.                                   | In place |
| <b>Can we require two-step verification for everyone?</b> | Yes. An owner can require it for the whole district. Anyone without a passkey or authenticator is then sent to set one up before they can use anything else, and no one can remove their last method while the requirement is on. | In place |
| <b>Single sign-on (SAML or OIDC)?</b>                     | Not yet. Accounts are structured for it, but single sign-on isn't built.                                                                                                                                                          | Not yet  |

## Activity records and AI

| Question                              | Answer                                                                                                                                                                                                                                                                                                                                                                                                   | Status   |
|---------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------|
| <b>Is activity logged?</b>            | Yes. Sign-ins, uploads, restatements of closed years, role and permission changes, assumption changes and each AI analyst question are recorded with who made them and when.                                                                                                                                                                                                                             | In place |
| <b>What does the AI provider see?</b> | The AI analyst runs on Anthropic's Claude. For each question it receives the question, the page context and the results of the tools it calls on your workspace: figures calculated from your aggregated data and, if you've added your own documents, passages from them. It has no direct access to the database. Every figure in an answer comes from a calculation and links to the query behind it. | In place |

## Your data, your control

| Question                                            | Answer                                                                                                                                                                                                                                                                                    | Status     |
|-----------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|
| <b>Can we export our data?</b>                      | Yes. Owners and analysts can download a .zip of the district's own data (the loaded files as CSV, plus scenarios and settings) at any time, including after a trial ends.                                                                                                                 | In place   |
| <b>Can we delete it?</b>                            | Yes. An owner can delete the district's workspace from Settings, Plan and billing. When a subscription ends, you have 30 days to export; data is then deleted within 60 days, and from backups as they are overwritten within 35 days after that (Data Processing Agreement, section 10). | In place   |
| <b>How quickly will you tell us about a breach?</b> | Without undue delay, and in any case within 72 hours of confirming a breach affecting your data (Data Processing Agreement, section 8).                                                                                                                                                   | In the DPA |
| <b>Are there backups?</b>                           | Automated database backups, with the ability to restore them (Data Processing Agreement, section 6).                                                                                                                                                                                      | In the DPA |
| <b>FERPA</b>                                        | Astra FP&A K-12 is built not to receive education records. If any personally identifiable information from education records reached it, the provider acts as a school official under FERPA and won't re-disclose it (Data Processing Agreement, section 4).                              | In the DPA |

## Reviews and reports

| Question                                | Answer                                                                                                                                                                                                                         | Status     |
|-----------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|
| <b>SOC 2 report?</b>                    | Not yet.                                                                                                                                                                                                                       | Not yet    |
| <b>Independent penetration test?</b>    | No report yet. The Data Processing Agreement commits to independent testing at least yearly, and the most recent report is shared under confidentiality when available (sections 6 and 11).                                    | Not yet    |
| <b>HECVAT or our own questionnaire?</b> | Available on request. We complete the full HECVAT, or your own security questionnaire, once a year and after a security incident (Data Processing Agreement, section 11). This summary answers the questions asked most often. | On request |

Questions about these answers: [to be completed]. The Data Processing Agreement is published at <https://astra-fpa.ai/dpa>.