

BudgetUp security overview

For IT security, information governance and procurement teams

Version 0.1 · 8 October 2026 · Tamsar Global Ltd (trading as BudgetUp), company 17371733 · Security contact: hello@budgetup.uk (subject "Security report") · Privacy: privacy@budgetup.uk

How to read this. We describe what is in place today, and say plainly where something is **planned** or **in progress**. Tamsar Global Ltd is certified to ISO/IEC 27001; the certificate is available on request. Our parent company, Tamsar, Inc., holds Cyber Essentials (IASME, valid to July 2027); certification in Tamsar Global Ltd's own name is planned. We have not yet had an independent penetration test.

1. Summary

Area	Position today
Hosting	Hetzner Online GmbH, Germany (EU). Docker containers behind a Cloudflare Tunnel; no public ports on the origin
Tenant isolation	PostgreSQL row-level security (RLS), app role cannot bypass it, automated RLS tests on every change
Encryption in transit	TLS 1.2+ at the Cloudflare edge, HSTS (2 years, preload), encrypted tunnel to the origin
Encryption at rest	Special-category fields AES-256-GCM at the application layer; backups encrypted before upload. Full-disk encryption of the database server: planned (dedicated server build)
Backups	Nightly, encrypted, off-site in Cloudflare R2 (EU jurisdiction), 30 days; 7 days on the server; alerting if stale
Identity	Passwordless sign-in (email links), Google sign-in, institution SSO: SAML 2.0 (UKAMF / Shibboleth, ADFS, Entra, OpenAthens), Microsoft Entra ID and Google Workspace (OIDC), SCIM 2.0 provisioning, LTI 1.3
Logging	Append-only audit log; structured application logs; error tracking (EU)
Certifications	ISO/IEC 27001 (Tamsar Global Ltd; certificate on request). Cyber Essentials held by parent Tamsar, Inc. Others planned

2. Architecture and hosting

- **Application:** Next.js (Node.js) web app and a background worker, built as container images, running with Docker Compose.
- **Database:** PostgreSQL 17 in a container on a private Docker network with no published port.
- **Edge:** Cloudflare (DNS, TLS, DDoS protection) and a Cloudflare Tunnel. The web container listens only on the server's loopback interface; traffic reaches it only through the tunnel.

- **Location:** Hetzner, Germany. EU hosting is covered by the UK adequacy regulations. The deployment is portable, so we can move to a UK host if a buyer requires UK-only residency.
- **Interim shared host (disclosure).** Until we have paying customers, production runs on a Hetzner server that also hosts another Tamsar product. BudgetUp has its own Docker network, its own database container and volume, its own secrets file (root-only) and memory limits; the two products share no database, network or credentials. The target architecture is a dedicated database server (LUKS full-disk encryption, pgBackRest with point-in-time recovery, a streaming replica) and separate web servers. Infrastructure code for it is in our repository, and a pgBackRest restore drill has been run on it locally (17/17 migrations, RLS on, identical row counts on 90 tables, point-in-time replay confirmed), but it is not yet in production.

3. Tenant isolation: row-level security, with tests

- Every institution-scoped table has PostgreSQL **row-level security** enabled and **forced**. Each request sets a context (learner, institution staff, or system job) and the policies filter rows to that context.
- **Three database roles:**
 - the application role, which is `NOBYPASSRLS`, so a bug in a query cannot read another institution's rows;
 - an authentication role, which can bypass RLS but is granted only the four sign-in tables;
 - the owner role, used only by migrations, content sync and backups, never by the running app.
- **Owner-only data:** AI coach conversations and optional equality information can be read only by the learner (and audited system jobs). No institution staff role has a read path.
- **Tests:** RLS test suites run as the restricted app role against a real PostgreSQL database in continuous integration on every change: core tenant isolation, audit log, billing, campaigns and branding, AI coach, integration APIs (SCIM, LTI, xAPI), outcomes reporting and small-number suppression. A schema check also fails if migrations drift from the schema.
- **Reporting:** institution reports are computed live and suppress any group under 10 learners.

4. Encryption

In transit. HTTPS only. Cloudflare terminates TLS 1.2 or higher at the edge. HTTP Strict Transport Security is sent with a two-year max-age, `includeSubDomains` and `preload`. The edge-to-origin hop runs inside the encrypted Cloudflare Tunnel. Outbound calls to sub-processors (email, error tracking, AI) use TLS.

At rest.

- Optional special-category and equality information: AES-256-GCM at the application layer, with a dedicated 32-byte key held in the server's secrets file, not in the database. Production refuses to start without it.
- Backups: encrypted on the server with `rcrypt` before upload to Cloudflare R2. Cloudflare also encrypts R2 objects at rest.
- Database volume: on the interim shared host, the database volume is **not** full-disk encrypted by us. LUKS full-disk encryption is part of the dedicated database server build (**planned**).

5. Secrets handling

- Production secrets (database role passwords, session signing secret, special-category key, LTI, SAML and badge signing keys, job secret, API keys) are generated **on the server** by a script that refuses to overwrite an existing file. They live in a single root-owned file with mode 600 and have never been copied off the server, except for the recovery copies below.
- Each container receives only the secrets it needs (for example, only the migration job gets the owner database URL, and only the worker gets the job secret).
- Recovery copies of the special-category key and the backup encryption password are kept in the owner's password manager, so backups remain usable if the server is lost.
- No secrets are kept in source control. Continuous integration uses throwaway, CI-only database credentials.
- Public build-time identifiers (for example analytics project keys) are not secrets and are treated as public.
- **Planned:** automated secret scanning (gitleaks) in continuous integration, and SOPS / age-encrypted secrets for the dedicated deployment.

6. Backups and recovery

- **Nightly** logical backup (`pg_dump`, compressed) at 03:47 UTC.
- **7 days** kept on the server; **30 days** kept **off-site** in Cloudflare R2 under the **EU jurisdiction, encrypted** on the server before upload.
- A watchdog alerts by email if the newest local dump or the last successful off-site copy is more than 26 hours old.
- A documented restore procedure covers restoring onto the same host or a new host. Backups age out within 35 days of data being deleted from the live database.
- **Targets (indicative, not yet contractual):** recovery point objective 24 hours; recovery time objective one working day on the interim host. The dedicated build adds continuous WAL archiving for point-in-time recovery.
- **Gap:** a dated restore test of the R2 off-site copy on the interim host should be recorded (the local pgBackRest drill above covers the dedicated build only).

7. Access control and single sign-on

Learners and staff signing in to BudgetUp

- **No passwords are stored.** Sign-in is by single-use email link (valid 15 minutes), "Continue with Google", or the institution's own identity provider. Sessions last up to 30 days from last use, in `HttpOnly`, `Secure`, `SameSite=Lax` cookies, and can be revoked by signing out everywhere.
- **Institution single sign-on (built and tested):**
 - **SAML 2.0**, one service provider entity per institution, for Shibboleth, ADFS, Entra (SAML mode) and OpenAthens Keystone, with **UK Access Management Federation (UKAMF)** metadata support: federation metadata signatures are verified and tampered metadata is rejected. SAML single logout is supported.
 - **Microsoft Entra ID (OIDC)**, through a multi-tenant app registration; your IT admin consents once.
 - **Google Workspace (OIDC)**, with the domain checked against Google's verification.
 - OIDC back-channel logout.
- **Provisioning: SCIM 2.0** (Microsoft Entra ID, Okta): users, groups to cohorts, and deprovisioning of leavers. The Microsoft Entra SCIM validator reported 24/24 checks passed.
- **LMS: LTI 1.3 Advantage** (dynamic registration, launch, deep linking, grade passback) tested end to end in Moodle 4.5.
- **Roles:** learner; institution administrator; institution analyst (read-only). Staff consoles show suppressed aggregates only.
- **UKAMF note:** on the interim host the scheduled federation metadata refresh is switched off for memory reasons; it runs on the dedicated build. Our UKAMF registration is being prepared.

Our own staff

- Production access is limited to the company owner, by SSH key to the server. Platform-operator functions in the app (privacy request queue, billing operations) are limited to a named allow-list of accounts and audit-logged.
- **Gaps to close:** multi-factor authentication confirmed and enforced on every administrative account (Hetzner, Cloudflare, Google Cloud, Stripe, Brevo, GitHub, the password manager); a written access-control and joiners-and-leavers policy. These are also Cyber Essentials requirements.

8. Logging and audit

- **Audit log:** append-only (the app role has no `UPDATE`, `DELETE` or `TRUNCATE` on it), isolated per institution by RLS. It records security and data-rights events: sign-in method changes, data exports, corrections, account deletions, data-rights requests, retention runs, role and

setting changes (for example switching the AI coach on), subscription events. It holds account ids, never names or email addresses. Kept up to 6 years.

- **Application logs:** structured JSON lines, capped in size on the server.
- **Error tracking:** server errors go to PostHog EU (Frankfurt) with no user, session, cookie, IP, header or request body attached; browser errors only with analytics consent and never in under-18 mode.
- **Monitoring:** an external uptime check every 5 minutes (Cloudflare Worker) and a server watchdog every 5 minutes (service health, disk, memory, backup freshness, tunnel), both alerting by email.

9. Application security

- Security headers on every page: a strict Content Security Policy listing each allowed host, `X-Frame-Options: SAMEORIGIN`, `X-Content-Type-Options: nosniff`, `Referrer-Policy: strict-origin-when-cross-origin`, and a restrictive `Permissions-Policy` (no camera, microphone, geolocation, payment or USB).
- Rate limiting on sign-in, data export, feedback, the AI coach and other sensitive endpoints, using hashed keys (no emails or IP addresses stored).
- Input validation with typed schemas on API routes.
- Production refuses to boot without its required security configuration (checked in continuous integration).
- No user-generated public content, chat or direct messages, which removes a large class of abuse and moderation risk.

10. Vulnerability management

In place

- Dependencies are pinned with a lockfile and installed with `--frozen-lockfile` in CI.
- Every change runs typecheck, unit tests and database RLS tests in CI, and a container build and boot test.
- A vulnerability disclosure route on the trust centre: email hello@budgetup.uk with "Security report" in the subject. We will not take action against good-faith research that avoids harming users or data.

Planned

- Automated dependency vulnerability alerts and scanning, and a monthly patch routine for the host OS and images (patch high and critical issues within 14 days, a Cyber Essentials requirement).
- Secret scanning (gitleaks) and OWASP ZAP baseline scans in CI.
- `security.txt` (RFC 9116).

- An independent CREST-accredited penetration test before public launch, then yearly and before major releases.

11. Incident response

1. **Detect:** monitoring alerts, error tracking, reports to the security inbox, or notice from a sub-processor.
2. **Triage and contain** (target: start within 4 working hours of awareness): assess scope, revoke sessions or keys, isolate affected services, preserve logs.
3. **Notify institutions:** where institution data is affected, we notify the controller **without undue delay and within 24 hours** of becoming aware, as in our DPA, with what we know and update as we learn more.
4. **Notify the ICO and individuals:** where we are the controller (direct sign-ups), within 72 hours where required; for institution data, we support the institution's own notification.
5. **Recover:** restore from backup if needed, rotate secrets, fix the cause.
6. **Review:** a written post-incident review with actions, shared with affected institutions.

A written incident response plan with named roles and a yearly tabletop exercise is **planned** alongside Cyber Essentials.

12. Assurance roadmap

Item	Status
ISO/IEC 27001 (Tamsar Global Ltd)	Certified; certificate available on request
Cyber Essentials	Held by parent Tamsar, Inc. (IASME, to July 2027); Tamsar Global Ltd's own planned
Cyber Essentials Plus	Planned
HECVAT 4	Planned (a lite answer set is available now)
CREST penetration test	Planned, before public launch
NCSC Cloud Security Principles mapping	Planned
ICO registration (Tamsar Global Ltd)	In progress

Related documents: data processing agreement template, DPIA summary, security questionnaire answers, accessibility conformance report. All at <https://budgetup.uk/trust> or on request.