FOR DISTRICTS

Data security and incident response policy

Effective September 18, 2026. This policy describes how BreathEasy Administrative Services LLC protects the data districts entrust to BreathEasy | Campus™, and what happens if something goes wrong.

CONTROLS IN PLACE

- Encryption in transit and at rest
- Least-privilege staff access
- Continuous backups and tested restores
- Documented breach notification timeline

Scope and ownership

This policy covers the BreathEasy | Campus™ application, its database, its hosting environment, and the company staff who administer it. BreathEasy Administrative Services LLC, 201 Lupin Street, Pahrump, Nevada 89048, operates the service. The company has two members, both of whom perform operational duties. One member is the designated security officer and incident commander; the other is the designated privacy officer and backup incident commander. Both members review this policy at least annually.

Data districts place in the system remains the property of the district. The company acts as a school official under FERPA and processes data only to deliver the service.

Data classification

- Restricted: student identifiers, behavior and discipline records, IEP progress, urgent incident records, guardian contact details, mandated-reporter records.
- Confidential: staff account details, sign-in and audit logs, district configuration.
- Public: marketing website content and published policy documents.

Restricted data is never used for advertising, never sold, and never used to train unrelated systems.

Encryption

- In transit: TLS 1.2 or higher for every connection, with HTTP redirected to HTTPS and modern cipher suites only.
- At rest: AES-256 encryption for the database, automated backups, and uploaded files such as referral photos.
- Secrets and API credentials are held in managed secret storage, never in source code and never in client-side code.

Access control and tenancy

- Least privilege by default. Every staff member gets the narrowest role that lets them do their job.
- Row-level security policies and role checks are used to enforce school and district access boundaries at the database and application layers.
- Unique named accounts only. Shared logins are not permitted, and roles are assigned by a district IT administrator.
- Default access uses named staff accounts with email and password or Google sign-in. Accounts lock after five failed sign-in attempts within ten minutes.
- Staff sessions end automatically after 30 minutes with no activity, on both web and handheld clients, with an on-screen warning about one minute before sign-out.
- District identity integration is available upon request and configured during onboarding. Available configurations include Google Workspace or Microsoft Entra ID through SAML or OIDC, identity-provider MFA policy enforcement, and automated account lifecycle integration where supported by the district's identity environment.
- District administrators can deactivate staff access. Manual account deprovisioning is available as the default account-lifecycle process.
- Company administrative access to production is limited to named personnel, used only for support and maintenance, and logged.

- District administrators should review staff accounts and roles at least each semester; the company reviews its own access quarterly and on every personnel change.

Application security

- Dependency and application security reviews are performed as part of release preparation. Known high-severity vulnerabilities are evaluated and resolved before affected changes are deployed.
- Input is validated on the server, and privileged actions are re-checked on the server rather than trusted from the browser.
- No production student data is copied into test, demo, or development environments. Demonstration tenants use fictional students.
- Audit records for discipline, urgent incidents, and mandated reports are append-only; corrections are added as timestamped amendments rather than edits.

Hosting, backups, and continuity

The company does not own or operate data centers. All infrastructure runs on two major cloud providers, Amazon Web Services and Cloudflare, reached through managed platforms that provision and patch those resources on our behalf.

- The web application and its server functions are served from Cloudflare's global edge network, with all data processing bound to United States regions.
- The database, authentication, and private file storage run on managed PostgreSQL hosted on Amazon Web Services in the US East (Ohio) region, us-east-2. This is where student and staff records physically reside, and they never leave United States regions.
- Both providers hold SOC 2 Type II and ISO 27001 certification for the data centers, physical storage, and network infrastructure involved. Those attestation reports are available to districts on request.
- Automated daily backups with point-in-time recovery, retained on a rolling 35-day cycle.
- Recovery time objective of 24 hours and recovery point objective of 24 hours for a full-service outage.
- Restore procedures are tested at least annually.

These infrastructure attestations apply to the providers and services they cover. BreathEasy is responsible for application design, access rules, role assignment, data handling, tenant separation, support access, and the policies governing use of the service.

Logging and monitoring

Application security events include sign-in attempts, account lockouts and unlocks, role changes, support access, and each use of an AI drafting feature, recorded with the acting user, the tool and model used, and the student record involved. Additional administrative events are captured where applicable. Records include available request and actor details, such as timestamp, IP address, user agent, affected user or record, and relevant details. The system automatically locks an account after five failed sign-in attempts within ten minutes and alerts the district security/IT contact and help@breatheasy.net.

District IT admins, district admins, and the platform owner can review and export these events from the Security panel in the admin console. Operational logs are retained for 18 months. This automated monitoring covers application-level activity; it does not replace district network, endpoint, or identity-provider logging, which remain the district's responsibility.

Personnel

- Background checks before any access to production systems.
- Signed confidentiality and data-handling agreements.
- Annual security awareness and FERPA training.
- Access is revoked the same day a role ends.

Incident response

Incidents are classified by severity and handled on the following timeline.

- Severity 1, confirmed or suspected exposure of restricted data: acknowledged immediately, containment target of 4 hours.
- Severity 2, service outage or degraded availability with no data exposure: acknowledged within 1 hour during school hours, resolution target of 8 hours.
- Severity 3, isolated defect: triaged within one business day.

The response follows a fixed sequence: detect, contain, eradicate, recover, notify, and review.

- Districts are notified without unreasonable delay and no later than 72 hours after the company confirms a breach involving their student or staff data, including what happened, what data was involved, and what is being done.
- A written post-incident report follows within 15 business days, covering root cause, remediation, and preventive changes.
- The company cooperates with the district's own notification duties under state breach-notification law and its contractual obligations, and will not notify parents directly unless the district asks it to.

- For a confirmed breach originating on infrastructure the company controls, the company bears the reasonable cost of forensic investigation of its own systems, and of parent and staff notification and credit monitoring where those costs are attributable to that breach. Final allocation is set in the signed agreement.
- Report a suspected incident to help@breatheasy.net with 'SECURITY' in the subject line. Reports are monitored continuously.

Vendor and sub-processor management

Every third party that touches district data, what it handles, and where it sits:

Sub-processor	Role	Region	Compliance posture
Application hosting (Lovable, managed platform)	Serves the web application and its server functions	Cloudflare global edge network, United States processing	Cloudflare holds SOC 2 Type II and ISO 27001
Database, authentication, and file storage (Supabase, managed platform)	Managed PostgreSQL database, authentication, and private file storage for attachments	Amazon Web Services, US East (Ohio), us-east-2	Supabase holds SOC 2 Type II; AWS data centers hold SOC 2 Type II and ISO 27001
Transactional email (Lovable messaging, managed platform)	Delivers report cards, discipline notices, account email, and security alerts	United States	SOC 2 Type II certified infrastructure

No advertising networks, analytics vendors, or data brokers receive any data from the application. Each sub-processor is bound by terms at least as restrictive as the agreement with the district, and none may use district data for its own purposes. New sub-processors are reviewed for security and privacy posture before use, and districts are notified before a change affecting student data.

Retention and secure deletion

Default retention periods are published in the privacy policy (/privacy) and may be shortened or extended by written agreement. On written request or at the end of a contract, the district receives a full export, live data is permanently deleted within 30 days, and backup copies age out on the normal 35-day cycle. Deletion is confirmed in writing.

Audit rights and current attestations

Districts may request this policy, the sub-processor list, and a summary of the most recent security review at any time, and may include audit rights in their agreement.

BreathEasy Administrative Services LLC does not currently hold its own SOC 2 report. The underlying data centers, physical storage, and network infrastructure operate within provider environments holding SOC 2 Type II and ISO 27001 certifications. Provider attestations are available upon request and apply only to the controls and services covered by those reports. Completed CAIQ v4.1 and HECVAT 4.1.6 self-assessments are included in the district packet at /district-documents (/district-documents). District identity integration is configured during onboarding when included in the written district scope. Optional facial lookup is disabled by default at the district level and appears only after a district asks for it to be enabled.

An independent third-party penetration test of the application has not been performed. A gray-box test would cover the application endpoints, authentication and session handling, role enforcement, and multi-tenant separation.

Cyber-risk and technology errors and omissions coverage is carried through Hiscox with a $250,000 aggregate limit, policy period through February 24, 2027. A certificate of insurance, including a certificate naming the district, is issued on request.

A completed NDPA-style data privacy exhibit, the line-item schedule of data, and any state-specific addendum are published at /district-addendum (/district-addendum) and available for district counsel from help@breatheasy.net.

Contact

BreathEasy Administrative Services LLC
201 Lupin Street, Pahrump, Nevada 89048
Security and privacy: help@breatheasy.net
Sales and contracts: sales@breatheasy.net

Document version

Data security and incident response policy version 1.4, effective September 18, 2026. A current copy of this document, plus downloadable PDFs, are available at /district-documents (/district-documents).