

Security Overview

Last updated: October 2, 2026

PheedLoop provides event management software to associations, conference organizers and other event teams: registration and ticketing, event websites, the PheedLoop Go attendee app, virtual events, and on-site check-in and badge printing. This overview describes how we protect our clients' data and the practices in place as of the date above.

Our full policy set, completed security questionnaire and supporting documents are available to clients and prospects under NDA. This overview is for information only. Contractual commitments are set out in the client agreement and the PheedLoop Data Processing Addendum.

1. Security governance

Rahul Goel, CEO, is PheedLoop's Security Officer and Privacy Officer and is accountable for the security and privacy program. He delegates day-to-day security operations to the Head of Engineering.

The program is defined in a set of 20 security and privacy policies approved by the CEO and reviewed every 12 months, after any critical incident, and after any material change to our infrastructure or sub-processors.

- Every employee and contractor signs a confidentiality agreement before receiving access to company or client data.
- All employees complete a background check before receiving access to production systems or client data.
- Security awareness training is completed within 30 days of hire and every year after, delivered and tracked in our in-house learning system. Engineers also complete annual secure development training.
- Security and privacy risks are assessed at least once a year and before major architecture changes.
- Vendors that process client personal data are reviewed before onboarding and every year, and are bound by written data protection terms.

2. Infrastructure and network security

The PheedLoop platform is hosted on Amazon Web Services in the Canada (Central) region, across two availability zones, with separate staging and production environments. Physical security of the data centres is provided by AWS, which holds ISO/IEC 27001, SOC 2 and other certifications. AWS's reports are available to clients directly through AWS Artifact.

- Public traffic enters only through a web application firewall and load balancer. Application services and data stores run in private subnets with no direct internet access.
- All traffic is encrypted in transit. Public endpoints require HTTPS with TLS 1.2 or higher.
- Infrastructure is defined primarily as code, and changes are reviewed before they are applied.

3. Access control and authentication

For clients. Organizers manage their team's access with role-based permissions. Organizer accounts support two-factor authentication (TOTP), which we strongly recommend every administrator enable. Attendees can sign in with single sign-on through OpenID Connect, with magic links or one-time codes, or with a password. Passwords are stored only in salted, hashed form, and sessions expire after inactivity. Single sign-on for the organizer dashboard is not currently available.

For PheedLoop staff.

- Every person has a unique, named account, and access is granted by role on least privilege.
- Company accounts use single sign-on with multi-factor authentication. MFA is enforced on email, AWS, GitHub and our internal admin tools.
- Production access is limited to a small group of engineers. Privileged actions in AWS are logged, and privileged access is subject to quarterly review.
- Staff access to client data is limited to delivering, supporting or securing the service, and actions taken in client accounts are logged.
- All access is revoked on an employee's last working day.
- Employees must use company-provided laptops, configured with full-disk encryption, automatic screen lock and automatic updates.

4. Application security and change management

- Every code change is reviewed and approved by an engineer other than its author.
- Automated tests, including tests that check one client cannot access another client's data, run on every change. A failing test blocks the release.
- Features that affect authentication, payments, data export or tenant boundaries receive a security review during design.
- Engineers follow secure coding practices covering the OWASP Top 10.
- Application dependencies and container images are scanned automatically for known vulnerabilities.
- Production client data is never used in development or testing.
- Releases are deployed without downtime and can be rolled back. Major updates are announced to clients in advance.

5. Data protection and privacy

Encryption. Databases, file storage and backups are encrypted at rest with AES-256, with keys managed in AWS Key Management Service. Application credentials are held in a managed secrets service and never stored in code.

Tenant isolation. All clients share one platform. Every record belongs to an organization, and the application checks organization membership on every request.

Payments. Card details are entered into fields hosted by the organizer's payment processor and never touch PheedLoop's systems.

AI. The platform has no AI features, and client data is not used to train AI models.

Data location. Client data is stored in AWS Canada (Central). A limited set of sub-processors, mainly for analytics, support, error monitoring and real-time messaging, process narrower data in the United States. Our sub-processors are published at pheedloop.com/more/pheedloop-sub-processors, and clients receive 30 days' notice of changes. All PheedLoop staff are located in Canada.

Privacy. PheedLoop processes event data on behalf of our clients, who remain the controllers of that data. We support compliance with PIPEDA, Québec Law 25, the EU and UK GDPR and US state privacy laws, and we sign a Data Processing Addendum with clients that need one.

Retention. Client data is kept for the life of the account, deleted within 14 days of a verified client request, and permanently deleted 12 months after an account ends. Backups expire on a rolling 7-day cycle.

6. Vulnerability management and testing

- Vulnerabilities are rated by severity and fixed within set targets: 7 days for Critical and 30 days for High.
- Container images are rebuilt with current patches on every deployment, and AWS patches its managed services.
- PheedLoop has not yet commissioned an independent penetration test. Our first is planned for 2027, and we will share a summary of its scope and findings on request.
- Clients may run their own security testing of their account with advance notice and an agreed scope.
- We welcome reports from security researchers at security@pheedloop.com and acknowledge them within 3 business days. Our Vulnerability Disclosure Policy includes safe harbour for good-faith research.

7. Business continuity and disaster recovery

- Application services and the database run across two availability zones with automatic failover.
- The database is backed up continuously with point-in-time recovery, and backups are encrypted and kept in AWS Canada (Central).
- Our recovery targets are under 1 hour for the loss of an availability zone and 4 hours for a database restore, with no more than 5 minutes of data loss. Recovery from the loss of an entire AWS region is being addressed through a multi-region disaster recovery strategy now in development.
- Our Disaster Recovery Plan requires an annual restore test, and our Business Continuity Plan allows the whole company to operate remotely.
- Clients can follow service status at status.pheedloop.com.

8. Incident response

PheedLoop maintains a documented Incident Response Plan with defined severity levels and roles. If an incident affects a client's data, we notify that client without undue delay and no later than 72 hours after confirming it, then provide regular updates and a written report within 10 business days of closing the incident. Every serious incident receives a post-incident review.

9. Compliance and assurance

PheedLoop does not currently hold an independent security certification. Our policies are structured around the control areas in ISO/IEC 27001 and the SOC 2 Trust Services Criteria, and our infrastructure runs on AWS services covered by AWS's own independent audits.

The following are available to clients and prospects under NDA:

- Our full security and privacy policy set
- A completed SIG Lite questionnaire
- Our Data Processing Addendum
- Architecture and data flow documentation
- A management attestation on penetration testing

10. Contact

Security questions and vulnerability reports: security@pheedloop.com

Privacy questions and data requests: privacy@pheedloop.com

PheedLoop Inc., 4950 Yonge Street, Suite 2308, Toronto, Ontario M2N 6K1, Canada. Phone: +1 (888) 360-5667.