AccessGrid

Security Questionnaire & Responses

AccessGrid, Inc.

Updated June 2026 · Version 1.0

Consolidated answers to the security and privacy questions we are most frequently asked. For supporting documentation — penetration test report, Stripe Attestation of Compliance, subprocessor list, or a completed copy of your own questionnaire — contact **support@accessgrid.com**.

01 Company & Security Program

Is there a formal Information Security program with documented policies?

Yes. AccessGrid maintains a formal Information Security Program documenting scope, roles, and exceptions, with supporting policies covering access control & account management, data handling, secure development & change management, incident response, and vulnerability disclosure.

Has the company experienced a security incident or data breach?

No. AccessGrid has had no data breaches in the history of the company.

Are employees and contractors required to complete security training?

Yes. All employees and recurring contractors complete role-specific security training covering cybersecurity for remote work, data privacy, and emerging threats.

Is any work outsourced or subcontracted to outside parties?

No. Only full-time employees work on the core product.

Who is the point of contact for security issues?

support@accessgrid.com — also the channel for vulnerability and security reports.

02 Data Handling & Privacy

What data is stored, and does it include PII?

For customers (account holders): name, email, phone number, password (encrypted), and IP address. For end users (credential holders): name, and optionally title, email, and phone number. We also process access-event metadata (timestamps, device/reader identifiers, template IDs) generated during credential issuance and use. No payment card data, no SSN, and no health data.

What data is received or processed from the customer?

The same data we store. The customer transmits end-user enrollment data (name; optional email/phone/title) and credential configuration to AccessGrid via our REST API. We also receive — but do not store — browser information used to route the user to the best credential install flow.

Do you maintain a data-flow diagram for sensitive data?

Yes. We maintain an up-to-date diagram of how sensitive data reaches and is stored in our systems. It is maintained internally and not shared externally. A formal catalog of sensitive data types is on our roadmap.

What is the data retention policy?

Database backups are retained 30 days and server logs 90 days. Credentials are deleted within one month of a customer request (delayed only because the credentials may still be active). Audit logs are retained for the life of the customer relationship to support audit access.

How can a customer have their data removed completely, and how long does it take?

Email support@accessgrid.com to cancel service. Deletion completes within 30 calendar days; the customer receives an email confirmation on completion.

Are you GDPR/CCPA compliant, and do you publish a subprocessor list?

AccessGrid does not operate in the EU and is not formally GDPR/CCPA certified. We do not currently publish a public GDPR/CCPA subprocessor list, but we maintain a list of third parties with access to customer data and provide it on request.

Is media sanitization (NIST SP 800-88 or equivalent) implemented?

Not yet; planned for 2026. Current practice is logical deletion within the retention windows above.

03 Encryption

How is data protected in transit?

All transport is TLS 1.2+ over HTTPS, enforced at the application layer with HSTS. Inside our environment, traffic between the application tier and managed datastores runs over TLS provided by the managed service. Outbound webhook delivery is HTTPS-only, with mTLS supported where the customer provides a client certificate.

How is data protected at rest?

Database volumes are encrypted at rest by our managed Postgres provider (AES-256). In addition, sensitive application-level fields are encrypted before being written to the database — including API keys, webhook client-certificate keys, third-party integration credentials (usernames, passwords, OAuth tokens, provider settings), credential-profile key material, and wallet signing keys (Apple JWT private/transport keys, Google SmartTap keys). User passwords are encrypted. File artifacts (card-template artwork) are stored in DigitalOcean Spaces (S3-compatible object storage), which encrypts objects at rest.

Do you encrypt data prior to insertion into the database (column-level)?

Yes. We use column/field-level encryption (AES-256-GCM) that stores ciphertext in the database separate from the key.

04 Authentication & Access Control

Do you support single sign-on (SAML / Okta / OIDC)?

Yes — Okta via OIDC. SAML is not currently supported. SSO is available to enterprise and partner customers.

What is the password policy when password authentication is used?

Passwords are 6–128 characters with no character-composition requirements (long passphrases, including 64+ characters, are fully supported). Secret questions are never used. Password resets are performed through an emailed, single-use token; reset requests do not reveal whether an account exists. Passwords are stored salted and hashed with bcrypt (an adaptive, CPU-hard one-way function) at a work factor of 12. Accounts lock after 5 failed attempts to limit brute-force attacks, and no default passwords are issued.

Is multi-factor authentication required?

MFA is not currently required for AccessGrid account logins. Enterprise and partner customers who connect via Okta (OIDC SSO) can enforce MFA through their own identity provider. Separately, customers can optionally enable a one-time-passcode step (via Twilio Verify) on credential-install landing pages to add a second factor for end users.

How is access control managed in your system?

Customers manage granular, role-based permissions in the AccessGrid console — per-team control over teams, users, pass templates, payment, API keys, and more. Access decisions are made by the customer.

What logical access controls are in place?

Sensitive-data access is limited to users with a legitimate need and authorized by the data owner; redundant accounts and expired grants are deactivated promptly; and access is reviewed regularly. Production access is restricted to authorized personnel.

What physical access controls protect production facilities?

Production infrastructure runs on managed cloud providers whose facilities provide layered perimeter and interior controls, managed key access, entry/exit logging, and response plans for unauthorized access.

05 Application Security

Is the application HTTPS-only?

Yes. HTTP (port 80) is redirected to HTTPS (port 443); HSTS is set with a long max-age; authentication cookies are marked Secure; and TLS is terminated at Cloudflare, which continuously manages and scans the TLS configuration.

Which security headers are applied?

A minimally permissive Content-Security-Policy, framing controls (X-Frame-Options / CSP frame-ancestors), and HSTS to reduce attack surface and limit post-exploitation.

Do you use secure frameworks/libraries to prevent injection and XSS?

Yes. We use modern, maintained frameworks that systematically escape outputs and sanitize inputs — an ORM for database access and a UI framework for DOM rendering.

Which vulnerability classes do your development guidelines guard against?

Authorization bypass, insecure session management, injections ((No)SQL, OS command, XXE, LLM/prompt), cross-site scripting, cross-site request forgery, and unsafe handling of untrusted data.

Is there an audit trail of access to data?

Yes. We keep an audit log of all account events by both customer and AccessGrid employees, available to logged-in users at /console/audit_logs. Each entry captures the user ID, IP address, timestamp, action type, and affected object, and is retained at least 30 days.

What events are logged?

Authentication events (success and failure), create/read/update/delete operations on users and objects, security-relevant configuration changes, and owner access to customer data.

06 Vulnerability & Patch Management

How often are third-party penetration tests conducted?

At least annually. Third-party penetration testing is performed against the product at least once per year; an application-component penetration test report is available on request.

Do you permit customers to test or pentest your system?

Yes. Customers or their delegates may request to test the application's security by email and will receive a response within 48 hours. Testing may run against production or a production-like environment; non-production environments do not contain production data; and reasonable testing restrictions may be defined.

What is your vulnerability and patch-management SLA?

Third-party dependencies are kept current, with security updates of medium severity or higher applied on our patching schedule and Known Exploited Vulnerabilities prioritized. Patches that materially impact security are produced and deployed within 20 business days of discovery, and actively-exploited issues are prioritized. In practice, automation-detected patches are typically deployed within one week.

Do you have a way to report vulnerabilities?

Yes. Vulnerabilities can be reported to AccessGrid (see our security page). We triage and remediate reported issues and respond within a reasonable timeframe.

How do you ensure build and release integrity?

We use a version-control system and a consistent build process that generates provenance (SLSA Build Level 1). Application credentials and tokens are stored separately from source code.

07 Incident Response

Is there a formal incident response plan, and how do you respond to a breach?

Yes — a written Incident Response policy within our Information Security Program. Severity is triaged as SEV 1 (confirmed or suspected customer-data exposure, active compromise, or widespread outage), SEV 2 (limited exposure with no evidence of ongoing compromise), or SEV 3 (low-impact or suspicious events under investigation). An Incident Lead coordinates the response. We triage to confirm the incident, then contain it (revoking access, rotating secrets — API keys, OAuth tokens, webhook mTLS keys, wallet signing keys, all AES-256-GCM encrypted so rotation is routine — blocking traffic, and revoking sessions), investigate root cause and scope using our event stream, version history, webhook-delivery logs, and platform logs, then eradicate and recover by patching the cause, restoring from point-in-time backups if needed, and validating before re-enabling. Public updates are posted to status.accessgrid.com and affected customers are notified directly. Logs and artifacts are preserved for the investigation, and access to incident materials is limited to involved personnel.

What is your breach notification timeline?

We notify relevant parties of any breach affecting sensitive information no later than 72 hours after discovery, and again as further details emerge. Notifications cover the nature of the breach, contact information, consequences, and remediation measures. Reporting to national cybersecurity agencies is considered per local guidance. A specific contractual notification SLA is negotiable.

08 Compliance & Certifications

Which certifications does AccessGrid hold (PCI, SOC 2, ISO 27001)?

PCI DSS — AccessGrid is out of scope for cardholder-data storage and processing; all card data is collected directly by our PSP (Stripe, PCI DSS Level 1) via hosted elements, and we store only Stripe customer and payment-method tokens. We are PCI DSS SAQ A eligible and maintain Stripe's Attestation of Compliance on file. SOC 2 — not currently certified; we have prioritized substantive security investments over certification at this stage, and it is not on the near-term roadmap, though we are open to discussing specific requirements. ISO 27001 — not certified and not currently planned. NIST SP 800-171 — alignment is in progress, expected complete by the end of 2026.

If no certification is in place, is there a right to audit?

Yes. While not in our standard agreement by default, we are happy to include a right-to-audit clause in the contract. Given our position on certifications, we consider direct audit rights a meaningful substitute.

Do you perform annual security self-assessments?

We perform self-assessments against a recognized baseline (MVSP). Formalizing them on a published annual cadence is on our roadmap.

09 Infrastructure & Operations

How is data backed up, and do you have disaster recovery?

All data is backed up daily to a location separate from where the application runs. Disaster-recovery plans are maintained and tested at least annually or after significant changes, in concert with incident-response planning.

Will any network interconnection (VPN, peering, reverse SSH) be required?

No. No network-level interconnection is needed. Partner systems integrate with our REST API or receive our webhooks, verifiable via basic authentication or mutual TLS.

Will administrative access to your systems be required to perform work?

No. No administrative access is required; integration is via our API and webhooks.

Is source-code escrow available?

No. AccessGrid does not place its source code in escrow, though we are open to discussing it for a long-term commitment.

10 Subprocessors & Third Parties

Do you maintain and share a list of third parties with access to customer data?

Yes. We maintain a list of third-party companies with access to customer data and make it available to clients and partners on request. Aside from our managed cloud/infrastructure providers, only Google and Apple have access to customer data, for wallet credential provisioning.

Do you assess the security of third parties annually?

We assess third parties with access to customer data. Formalizing this as an annual cadence against the latest MVSP release is on our roadmap.