SECURITY OVERVIEW

How We Protect Your Data.

The controls behind the Generator Labs platform, and the documents your security review will ask for.

DOCUMENT	Security Overview
SERVICE	Generator Labs (all products)
PUBLISHED	November 2026
CONTACT	legal@generatorlabs.com · generatorlabs.com/security

Generator Labs monitors internet infrastructure for its customers. This overview describes how we protect the data you trust us with.

Our security program is modeled on ISO 27001 and the SOC 2 Trust Services Criteria. We don't hold a formal certification, so we make our controls easy to review: our completed CAIQ-Lite questionnaire and our Data Processing Addendum are at generatorlabs.com/security.

TLS 1.2+	AES-256	72 h
WEBSITE, PORTAL, API, AND INTERNAL DATA	ENCRYPTION AT REST	INCIDENT NOTIFICATION

01

Infrastructure

The Service runs on Amazon Web Services in the United States, with DNS lookup infrastructure in Canada. Databases and internal services run in private networks that can't be reached from the internet. AWS provides network-level DDoS protection, and a web application firewall filters traffic to the website, portal, and API.

02

Encryption

- TLS 1.2 or 1.3 for all traffic to the website, portal, and API, and for connections that carry customer data inside our private networks.
- AES-256 at rest on every storage volume and bucket.
- Passwords are stored as bcrypt hashes.
- API tokens are stored hashed and shown only when created or rotated, so a copy of our database cluster can't be used to call the API.

03

Access

Your account: multi-factor authentication, role-based permissions, and a login history for account administrators. Account owners can require MFA across their team and choose how their users sign in, including through supported third-party sign-in providers.

Our staff: administrative access requires MFA, is limited to people who need it, is reviewed every quarter, and is removed the same day a person leaves or changes role.

04 Monitoring and Detection

Automated monitoring alerts on-call staff around the clock, as does Amazon GuardDuty, which watches our cloud account for threats such as unusual API activity, compromised credentials, and malicious network traffic. Every administrative action in our cloud account goes to a tamper-evident audit log kept for one year, and every read of that log is logged too.

05 Backups and Recovery

- Our database cluster spans multiple availability zones and fails over automatically if a server fails.
- Daily backups are kept for 30 days. All backups are encrypted and stored separately from the servers they protect, with copies in a second AWS region.
- A full restore is tested automatically every month, and our database cluster can be restored to any point in the last 30 days.
- Recovery targets, for the loss of a server, database, or availability zone: at most 5 minutes of database changes lost, and the portal and API restored within 8 hours.

06 Patching and Testing

Containers are rebuilt with current OS updates on every release, and servers are patched on a regular schedule. Critical security updates are applied within 7 days of release, and high-severity updates within 30 days.

Container images are scanned for vulnerabilities on every build and weekly, and servers are scanned continuously. AWS Security Agent, a third-party penetration testing service, tests the Service at least once a year.

07 People and Payments

Everyone with access to customer data is bound by confidentiality and completes security and privacy training on joining and every quarter after.

Stripe and PayPal handle card payments; we never see or store card numbers.

08 Privacy and Compliance

- Our Data Processing Addendum supports your GDPR, UK GDPR, Swiss FADP, PIPEDA, and CCPA obligations, with the Standard Contractual Clauses built in.
- Data is processed in the United States and Canada. Checks also query third-party sources and the endpoints you monitor, wherever they're located.
- We notify you within 72 hours of becoming aware of a security incident affecting your data.
- You get 30 days' notice before a new subprocessor processes your data.
- Your data is deleted within 30 days of your account closing, and backups expire within a further 30 days.

09 Documents

At generatorlabs.com/security: Data Processing Addendum, subprocessor list, Service Level Agreement (99.9% monthly uptime for all paid plans), CAIQ-Lite questionnaire, and our live status page.

On request from legal@generatorlabs.com: a summary of our latest penetration test. The full report and our security policies are available under NDA.

10 Vulnerability Disclosure

Found a security issue? Email abuse@generatorlabs.com with a description, steps to reproduce, the impact, and how to reach you. We'll acknowledge your report within 2 business days, keep you updated, and tell you when it's fixed. Good-faith research that follows our policy at generatorlabs.com/security is authorized.



Questions About Our Security?

Our Data Processing Addendum, subprocessors, and CAIQ-Lite questionnaire are on our security page. For our penetration test summary or anything this overview doesn't answer, email legal@generatorlabs.com.

generatorlabs.com/security

© 2026 GENERATOR LABS · ALL RIGHTS RESERVED · GENERATORLABS.COM