Security and Procurement

Security review | Updated Sep 1, 2026

Everything a vendor security review asks of PFLB is written down, and most of it is on this page.

Security Officer: Svetlana Matalaeva, security@pflb.us · Trust center: pflb.trust.site · security.txt · Download this page as PDF

Attestations and coverage

SOC 2 Type II

Observation period 3 March 2025 to 25 March 2026, covering Security, Availability and Confidentiality, issued by an independent service auditor, with no exceptions noted. Report released under a mutual NDA.

Penetration test

Independent web application security assessment of pflb.us and platform.pflb.us, April 2026. All findings have been remediated. Engineer workstations are covered by the SOC 2 endpoint controls described under Who touches the system.

Insurance

Cyber liability $2M aggregate; professional liability (errors and omissions) $1M per claim and $1M aggregate, claims-made; commercial general liability $2M aggregate and $1M per occurrence. Placed with an A-rated US insurer. Certificates naming your entity are issued on request; higher limits are available for your contract.

People and geography

Named, individually screened contracted engineers working from the United States, the United Kingdom and Iceland. Every person is sanctions-screened before access; no one from a sanctioned jurisdiction touches an engagement. The named list for your engagement comes with the NDA.

If your team has shortlisted PFLB for load testing, the next step belongs to security, legal and procurement. This page is written for them: which documents exist and how to get them, where your data lives, who touches the system, how onboarding runs, and what procurement needs to open a vendor record. Most reviews can start without a signature: six policies are open now, and the SOC 2 report follows the mutual NDA.

Documents and how to get them

Six policies are open to anyone at pflb.trust.site. The rest, including the SOC 2 Type II report, open the day you countersign a mutual NDA there.

Document	What it shows	Access
Information Security Policy	How the program is governed	Open
Access Control Policy	Who gets access, and how	Open
Encryption Policy	Data in transit and at rest	Open
Incident Management Policy	What happens when something goes wrong	Open
Business Continuity & Disaster Recovery Policy	Resilience posture	Open
Data Retention Policy	How long we keep things	Open
SOC 2 Type II report	Controls tested over a full year	**Under NDA**
Full policy library (27 further policies and procedures)	Implementation detail	**Under NDA**
Certificate of insurance naming your entity	Cover, with your endorsements	**On request**
Your questionnaire, completed	Your format, returned filled	**On request**
MSA with information security exhibit	The contract terms described on this page	**Under NDA**

Where your data lives

Four deployment options. We send you the data-flow diagram for the one you pick.

Our cloud

Fastest to start. We generate load from our infrastructure and keep the results in our platform. Your data stays in the test environment you point us at.

Your cloud

Generators run in your AWS or Azure account. You own the compute, we run the control plane, and nothing about the run leaves your boundary.

Inside your perimeter

On-premise generators for systems the internet cannot reach. Common in banking, utilities and anything behind a hard network edge.

Anonymized test data

When a lower environment needs production-shaped data, we generate an anonymized set that keeps the shape and referential integrity and carries none of the real values.

Who touches the system, and from where

Named engineers, each screened before access is issued, each with a declared work location.

PFLB, Inc. is a US entity. Testing is delivered by contracted engineers rather than employees: the same named people on every engagement. They work from the United States, the United Kingdom and Iceland. Each is screened to the category your policy requires, declares where they work from before access is granted, and is bound by written confidentiality obligations that flow down from your agreement. Every person is sanctions-screened; no one from a sanctioned jurisdiction touches an engagement. If your contract requires all work inside a single jurisdiction with no access from abroad, say so on the first call and we will tell you whether we can staff it that way.

Engineer workstations are company-issued devices under endpoint management: full-disk encryption enforced by policy, anti-malware on every workstation, automatic screen lock after 15 minutes, multi-factor authentication for cloud services and remote access, and VPN for access to the platform. These are controls tested in the SOC 2 Type II report, not a description written for this page.

Subprocessors: Amazon Web Services (platform hosting), Google Workspace (email and documents), Sprinto (compliance monitoring and the trust center). Your agreement obliges us to keep this list current, to give advance notice of changes, and gives you the right to object on reasonable data-protection grounds.

How onboarding runs

1. Mutual NDA. One document, usually signed the same day. Everything behind it is already prepared.

2. Security package. We release the SOC 2 Type II report in the trust center. Send your questionnaire in whatever format you use; we return it filled.

3. Insurance to your schedule. A certificate naming your entity, with the endorsements your contract requires, including waiver of subrogation and additional insured where applicable. We issue certificates ourselves, so turnaround is measured in hours.

4. Contract with a security exhibit. Our MSA carries an information security exhibit: breach notice without undue delay and no later than 72 hours, background checks, return or destruction of data within 30 days with written certification, audit rights including an on-site right following a security incident, and a subprocessor list with notice of changes.

5. Screening and access. Background checks per person to the category your policy requires, declared work locations, and any security training your side mandates, completed before access is issued.

Procurement and vendor onboarding

Legal entity

PFLB, Inc., a Delaware corporation, is the entity you contract with and the entity that invoices you. It was incorporated in 2022; the PFLB group has operated since 2008. D-U-N-S 119210793. W-9 and business registration are provided on request.

Registered and operating office

651 N Broad St, Suite 201, Middletown, DE 19709, US.

Remit-to

PFLB, Inc., 2810 N Church St # 729811, Wilmington, DE 19802-4447, US.

Certificates of insurance

Issued on request, naming your entity, with the endorsements your contract requires. Cyber liability $2M; higher limits are available for your contract.

Send your questionnaire with the RFP. A questionnaire that arrives after selection lands in the middle of legal review and adds weeks.

Security contact: Svetlana Matalaeva, Security Officer, security@pflb.us. These descriptions are informational; the executed agreement governs.

Reporting a vulnerability

If you believe you have found a security issue in pflb.us, platform.pflb.us or our services, email security@pflb.us with the steps to reproduce it. We acknowledge reports within three business days, keep you informed until the issue is resolved, and do not take legal action against researchers who act in good faith, keep data confidential and avoid service disruption. We do not run a bounty program. The same contact is published at /.well-known/security.txt.

Security questions we get asked

Can our review start before anything is signed?

Yes. The deployment options, the data-handling model and the contract structure are on this page and need no NDA. Six security policies are open in the trust center, and the SOC 2 Type II report follows the mutual NDA.

Do you have SOC 2?

Yes. A SOC 2 Type II report for the observation period 3 March 2025 to 25 March 2026, covering Security, Availability and Confidentiality, issued by an independent service auditor, with no exceptions noted. Released under a mutual NDA.

Do you have ISO 27001?

No. PFLB holds a SOC 2 Type II report covering the same control families. The two attest different things: ISO 27001 certifies that a management system exists and is designed correctly; a Type II report is an independent auditor testing whether the controls operated, on real samples, across a stated period. If your policy names ISO 27001 specifically and cannot accept an equivalent attestation, raise it on the first call rather than at contract stage.

Where are your engineers located?

In the United States, the United Kingdom and Iceland. PFLB, Inc. is a US entity; testing is delivered by named, individually screened contracted engineers who declare their work location before access is granted and are sanctions-screened. If your contract requires a single jurisdiction with no access from abroad, raise it on the first call and we will say whether we can staff it.

What insurance do you carry?

Cyber liability at $2M aggregate; professional liability (errors and omissions) at $1M per claim and $1M aggregate; workers' compensation; and commercial general liability at $2M aggregate and $1M per occurrence. Cover is placed with an A-rated US insurer. Higher limits are available for your contract. We issue a certificate naming your entity with the endorsements your contract requires, including waiver of subrogation and additional insured where applicable.

Will you complete our security questionnaire?

Yes. Send it with the RFP, in whatever format you use, and we return it filled.

Do you run background checks?

Yes, per person, to the category your policy requires. We declare which countries each person has previously worked in when your screening has to cover them. If someone declines screening, they do not join the engagement.

How are your engineers' workstations secured?

Company-issued devices under endpoint management: full-disk encryption, anti-malware, automatic screen lock after 15 minutes, multi-factor authentication for cloud and remote access, and VPN for access to the platform. These controls were tested in the SOC 2 Type II examination.

What happens to our data when the engagement ends?

Return or destruction within 30 days, with written certification on request. The obligation is a clause in the MSA.

Can you test without production data?

Usually yes. When a realistic test needs production-shaped data, we generate an anonymized set that keeps the shape and referential integrity and carries none of the real values.

Do you sign a DPA?

Our MSA carries an information security exhibit with breach notice, data return and destruction, audit rights and subprocessor list. It is released under NDA. Load testing runs on test environments and anonymized data, so most customers do not need a separate data processing agreement. If your policy requires one, send us your template and we return it reviewed.

Who else touches our systems?

Three subprocessors: Amazon Web Services for platform hosting, Google Workspace for email and documents,