COMPANY DOCUMENT | SEPTEMBER 2026

Security Overview

How 1099FIRE protects the SSNs, TINs and financial details you trust us with, and what our independent SOC 2 Type 2 audit covers.

> **About this document.** This is a plain-English summary of our security program, written by National Software, Inc. for customers and prospective customers. It is not our SOC 2 report. That report is a separate, restricted-use document issued by our auditor, Sensiba LLP.

OUR SOC 2 TYPE 2 AUDIT AT A GLANCE

REPORT	**SOC 2 Type 2**
AUDITOR	**Sensiba LLP, independent CPA firm**
LATEST REPORT	**June 1 to November 30, 2025, issued December 18, 2025**
RESULT	**Clean opinion, no exceptions noted**
CRITERIA COVERED	**Security, Availability, Confidentiality**
CURRENT OBSERVATION PERIOD	**December 1, 2025 to November 30, 2026, report expected December 2026**

WHAT IS INSIDE

1 The SOC 2 Type 2 audit
2 How your data moves
3 How we protect your data
4 Standards we follow
5 Data retention
6 Security FAQ
7 Other documents
8 Contact

National Software, Inc., operating as 1099FIRE | PO Box 93001, Phoenix, Arizona 85070 | (480) 706-6474 | info@1099fire.com
Last reviewed September 2026. The current version of this document is always at 1099fire.com/security.

SECTION 1

The SOC 2 Type 2 audit

A SOC 2 audit is done by an independent CPA firm. It checks whether a company has the right controls in place to protect customer data.

Type 2 is the tougher version. Instead of looking at our controls on a single day, the auditor tested whether they actually worked across six months. They did, with no exceptions.

The testing didn't stop there. Our current observation period started December 1, 2025, the day after the last one ended, and runs through November 30, 2026. Sensiba LLP expects to issue that report in December 2026, so an outside firm has been auditing how we protect your data since June 2025 without a break.

What the audit covers

Three of the AICPA Trust Services Criteria:

Security

Systems and data are protected against unauthorized access, inside and out.

Availability

The service runs when you need it, with backups and a tested recovery plan behind it.

Confidentiality

Information meant to stay private stays private, and is disposed of properly when it's no longer needed.

PERIOD	STATUS
Jun 1 to Nov 30, 2025	Tested by Sensiba LLP. Report issued December 18, 2025 with no exceptions.
Dec 1, 2025 to Nov 30, 2026	Current observation period, under way. It started the day after the last one ended, so there is no gap.
December 2026	Next report expected.

The SOC 2 report itself is issued by Sensiba LLP and is a restricted-use document. This overview is our own summary of the program those reports examine.

SECTION 2

How your data moves

From the moment you upload a file to the moment your returns reach the IRS, your data is protected at every step.

> **Your files**
> You upload them through your secure client portal.

> **Encrypted in transit**
>
> TLS 1.2 or higher protects the file on its way to us.
>
> **1099FIRE systems**
>
> Encrypted storage with AES-256, daily backups and multi-zone cloud hosting.
>
> **The IRS**
>
> Returns are transmitted to the IRS electronically and encrypted, through A2A.

Along the way, only 1099FIRE staff whose job requires it can reach your data, and they sign in with multi-factor authentication to do it.

SECTION 3

How we protect your data

Every safeguard below was tested by Sensiba LLP as part of our SOC 2 Type 2 audit.

Encryption everywhere

AES-256 for stored data, TLS 1.2 or higher for data in transit, and full-disk encryption on staff computers.

Multi-factor sign-in

Staff need multi-factor authentication to reach sensitive systems, and every person has their own login.

Daily backups

Production systems are backed up every day. We test our disaster recovery plan at least once a year against internal recovery time and recovery point targets.

Screened, trained team

Background checks for new hires, security training every year, and confidentiality agreements for all staff.

Need-to-know access

Access is granted by role and kept to the minimum each job requires. We review it every quarter.

Resilient hosting

Our systems run on Render and Supabase across multiple availability zones, so one data center outage doesn't stop us.

Always monitored

Drata watches our controls around the clock. Automated alerts flag suspicious traffic, and we scan for vulnerabilities.

Reviewed changes

Every software change is reviewed and tested by a second person, in a separate environment, before it goes live.

SECTION 4

Standards we follow

AICPA	**SOC 2 Trust Services Criteria** Our program is built around the Security, Availability and Confidentiality criteria, and audited against them every year.
IRS	**Publication 4557** We align with the IRS guide to Safeguarding Taxpayer Data.
IRS	**A2A approved** 1099FIRE is approved by the IRS for A2A filing. Returns are transmitted electronically and encrypted.
Insurance	**Coverage in place** Cyber Liability, Technology Errors & Omissions, and Commercial General Liability.

We also comply with applicable privacy laws, including CCPA, GDPR and HIPAA where they apply.

> **Security questionnaires.** We don't complete third-party or custom security questionnaires, including HECVAT. Our SOC 2 Type 2 examination and the safeguards in this document are what we provide instead. An independent CPA firm has already tested these controls, which is stronger assurance than a self-reported questionnaire.

SECTION 5

Data retention

WHAT	HOW LONG
Client data files	Not retained. The file you send is used to prepare and transmit your returns, and is removed shortly after processing is complete.
Filing records	7 years. The record of what was filed, with submission receipts and confirmations, in line with IRS requirements.
System logs	12 months.

When data reaches the end of its retention period, it is erased using a defined secure disposal process. Because we don't hold your source files, keep your own copy of the data used for filing in case corrections or proof of filing are needed later.

SECTION 6

Security FAQ

THE SOC 2 AUDIT

Is 1099FIRE SOC 2 audited?

Yes. National Software, Inc., the company behind 1099FIRE, has completed a SOC 2 Type 2 examination by Sensiba LLP, an independent CPA firm.

Our most recent report covers June 1 to November 30, 2025 and was issued on December 18, 2025. Sensiba tested our controls across that whole period and noted no exceptions.

The audit is ongoing. Our current observation period runs from December 1, 2025 to November 30, 2026, and Sensiba expects to issue that report in December 2026.

What's the difference between SOC 2 Type 1 and Type 2?

A Type 1 report is a snapshot. It checks that the right controls are designed and in place on one specific day.

A Type 2 report is more like a recording. The auditor tests whether those controls actually worked, day after day, over several months. Most businesses and their auditors ask vendors for a Type 2. That's the one we have.

What do Security, Availability and Confidentiality cover?

They're Trust Services Criteria set by the AICPA, the organization behind SOC 2. Our audit covered all three:

- Security: systems and data are protected against unauthorized access.
- Availability: the system is up when you need it, with backups and recovery plans if something goes wrong.
- Confidentiality: private information stays private, and it's securely disposed of when it's no longer needed.

Is SOC 2 a certification?

Not exactly, which is why you'll see us say "audited" instead of "certified." No agency hands out a SOC 2 certificate. An independent CPA firm examines a company's controls and issues a formal opinion in a report. That report is what you'd ask a vendor for.

Is the audit a one-time thing?

No. Each audit period starts the day after the last one ends, so there's no gap in coverage.

- June 1 to November 30, 2025: tested, report issued December 18, 2025.
- December 1, 2025 to November 30, 2026: observation period under way, report expected December 2026.

After that, a new 12-month period begins.

Your latest report ends in November 2025. How do I know your controls still work?

Auditors ask this a lot, and here's what covers the time since the last report:

- Our current SOC 2 Type 2 observation period has been running since December 1, 2025.
- Sensiba issued a letter on July 16, 2026 confirming that audit is under way.
- Between audits, Drata monitors our controls continuously and alerts us if anything falls out of line.

YOUR DATA

Is my data encrypted?

Yes, both while it's moving and while it's stored.

- In transit: data traveling between you and our system is encrypted with TLS 1.2 or higher.
- At rest: the databases that hold customer data are encrypted with AES-256.
- On our computers: staff workstations use full-disk encryption, which protects anything stored locally if a device is lost.

Where is my data stored?

The 1099FIRE system runs on established cloud providers. Render hosts the application and Supabase hosts the databases.

Both run across multiple availability zones, so if one data center has an outage, the system can fail over to another. Physical security at those data centers is handled by the providers, and we review their own audit reports as part of our vendor oversight.

How is my data backed up?

All production systems and databases are backed up every day, and those backups are monitored.

Backups only matter if you can restore from them, so we also run a business continuity and disaster recovery test at least once a year. Our written recovery plan spells out who does what to bring critical systems back, and it sets internal recovery time and recovery point targets.

How long do you keep my data, and how is it deleted?

There's an important split here.

- Your data files are not kept. We use the file you send to prepare and transmit your returns, and it's removed shortly after processing is finished. Our Data Services Terms say the same: we don't retain the Excel file you provide or the text file created for upload.
- Filing records are kept for 7 years. That means the record of what was filed, along with submission receipts and confirmations, which matches IRS requirements.
- System logs are kept for 12 months.

When data reaches the end of its retention period, it's erased using a defined secure disposal process. Because we don't hold your source files, keep your own copy of the data used for filing in case corrections or proof of filing are needed later.

How is my data used?

Only to deliver the services you've contracted with us for. Access to it is logged and monitored. Our Privacy Policy explains exactly what we do and don't share.

How should I send SSNs, TINs and other sensitive data?

Through your secure client portal, which we set up once payment is received.

Please don't send SSNs, TINs or card numbers by email, even to us. Email gets copied to multiple servers, can be forwarded by mistake, and can be read if an account is ever compromised. The portal avoids all of that.

How do I pay without sharing my card number by email or phone?

We'll send you a payment authorization form. Fill it out and upload it with the secure upload link we provide. Your card details never have to go through email or be read out over the phone.

What if I already emailed something sensitive?

Don't worry, it happens. Give us a call at (480) 706-6474 and we'll get you set up to send it the secure way going forward. It's also a good idea to delete the message from your Sent folder.

PEOPLE AND ACCESS

Who at 1099FIRE can see my data?

Only the people whose job requires it. Access is granted by role, kept to the minimum needed, and approved before anyone gets it.

Every person has their own login, so activity can be traced to an individual. We review who has access to critical systems every quarter, and when someone leaves the company, their access is removed promptly.

Do you use multi-factor authentication?

Yes. Multi-factor authentication is required for access to our sensitive internal systems, on top of strong password requirements. A stolen password alone isn't enough to get in.

Are your employees background checked and trained?

Yes. New hires go through a background check before they start. Everyone completes security awareness training at least once a year and signs off on our security policies.

Employment agreements also include a confidentiality agreement that covers client information.

Will I talk to a real person?

Yes. Our support team is based in the U.S., and you'll speak directly with someone who knows the product. That matters for security too. You always know who you're dealing with.

MONITORING AND RESPONSE

How do you watch for threats?

Several ways, and they run all the time.

- Drata monitors our security controls continuously and alerts us when something falls out of line.
- Our infrastructure logs web traffic and automatically flags suspicious activity.
- We scan for technical vulnerabilities and fix what we find.
- Staff computers run antivirus software and are managed centrally.

What happens if there's a security incident?

We follow a written incident response plan. It spells out who does what, how an incident is logged, classified and tracked to resolution, and how we communicate along the way.

Every security incident is reviewed by our Chief Information Security Officer. Afterward we document what we learned and put changes in place to prevent a repeat.

How do you keep software updates from causing problems?

Every code change is reviewed and tested by someone other than the person who wrote it. Testing happens in a separate environment from the live system, and only authorized staff can release changes to production.

All changes are tracked in version control, so we can roll back quickly if we ever need to.

How do you vet your own vendors?

We keep a register of the vendors we rely on, with written agreements and a risk rating for each. High-risk vendors get a security and compliance review, and we reassess vendor risk every year.

For our hosting providers, we also review their own independent audit reports.

Do you carry insurance?

Yes. We maintain Cyber Liability, Technology Errors & Omissions, and Commercial General Liability coverage.

WORKING WITH US

Is 1099FIRE authorized to file with the IRS?

Yes. 1099FIRE is IRS A2A approved, which means our system transmits information returns to the IRS electronically, and those transmissions are encrypted.

Which security standards do you follow?

Our program is built around the AICPA's SOC 2 Trust Services Criteria for Security, Availability and Confidentiality. It also aligns with IRS Publication 4557, Safeguarding Taxpayer Data.

We comply with applicable privacy laws as well, including CCPA, GDPR and HIPAA where they apply.

Can you complete our security questionnaire or HECVAT?

We don't complete third-party or custom security questionnaires, including HECVAT.

Our SOC 2 Type 2 examination and the safeguards described on this page are what we provide instead. An independent CPA firm has already tested these controls, which is stronger assurance than a self-reported questionnaire, and it's the same evidence your auditors would ask us for.

If something you need isn't answered here, call or email us and we'll talk it through.

What should my team do on our end?

Security works best when both sides do their part. On your side, we recommend you:

- Keep track of who on your team has access, and remove people when they leave.
- Use strong passwords, and turn on multi-factor authentication wherever it's offered.
- Send sensitive files only through the secure portal.
- Have your own backup plan in case any outside service is unavailable for a while.

Who do I contact about a security concern?

Email support@1099fire.com with "Security" in the subject line, or call (480) 706-6474. Please don't include SSNs, TINs or card numbers in your message.

SECTION 7

Other documents

Privacy Policy	How we collect, use, store and protect the information you share with us, your privacy rights, and the sub-processors we use. 1099fire.com/privacy-policy
Data Services Terms and Conditions	The agreement for our filing and processing services, covering responsibilities, data handling, confidentiality and retention. 1099fire.com/data-services-terms
Website Terms and Conditions	The terms covering your use of 1099fire.com itself. 1099fire.com/terms-conditions

SECTION 8

Contact

Report a security concern

If you think you've found a security issue, or something about your account doesn't look right, tell us right away.

support@1099fire.com | (480) 706-6474

Please don't include SSNs, TINs or card numbers in your email.

This document is a printed version of 1099fire.com/security. It is for informational purposes only and does not constitute legal or security advice. National Software, Inc., PO Box 93001, Phoenix, Arizona 85070.