Paperless Pipeline Security

Last Modified on 11/10/2026 12:22 pm EST

Paperless Pipeline protects your data with bank-grade encryption, isolated accounts, and PCI-certified infrastructure — with simple ways to add your own layer on top.

Introduction

People arrive at this page for one of two reasons: they're evaluating Pipeline and have to answer someone else's compliance questions about it, or something happened that made them worry about their own account. Both deserve a plain answer.

Security here has two halves, and they aren't the same job. One half is ours. It covers how your data moves, how it's stored, how one company's account is kept apart from every other company's, and how payment information is handled. Those are commitments we make and can describe to your broker, your attorney, or your state regulator without hedging. The other half is the part only your office can do: who holds a login, how strong those passwords are, and how quickly someone leaving loses access.

Knowing which half is which is most of the answer. You can hand the first half to whoever's asking without becoming an expert in it, and the second half is a short list of habits rather than a project. And if a message claiming to be from Pipeline looks wrong to you, or you find yourself shut out of your own account for no reason you can see, ask us. Both are worth checking, and neither is a bother.

How It Works

Pipeline protects your data in transit, at rest, and account-by-account.

Encryption in Transit

All web-based communication with Pipeline — including uploading and downloading documents — uses industry-standard SSL encryption, which protects your data as it moves between your device and our servers.

Encryption at Rest

Pipeline stores documents on Amazon Web Services (AWS), which includes built-in encryption for stored data. Your files stay protected while they sit in Pipeline, not just while they travel to it.

Account Data Isolation

Every company's account operates within its own distinct, secure environment. Actions in one account stay isolated and never touch the data in another, which prevents any cross-account compromise.

PCI Compliance

Paperless Pipeline complies with the Payment Card Industry Data Security Standard (PCI DSS) and holds a PCI Compliance Certificate from SecurityMetrics.

Email Security

Emails you send from Pipeline go out through our email service, SendGrid, which communicates with the recipient's mail server using TLS encryption whenever that server supports it — an extra layer of protection on your outgoing messages.

To keep documents encrypted on the way in, upload them directly with the Upload Doc feature rather than emailing them to a Maildrop address. Pipeline can't process an encrypted email sent *in* to a Maildrop address, because it can't extract attachments from one.

Password Requirements

Pipeline's password rules follow current guidelines from the National Institute of Standards and Technology (NIST):

- A minimum of 8 characters, because length matters more than complexity.
- Pipeline blocks common, easily guessable phrases.
- Pipeline doesn't force an arbitrary mix of uppercase, numbers, and symbols — rules like that tend to push people toward weaker, more predictable passwords.

Ways to Strengthen Your Account Security

Pipeline does its part; here's how your team adds to it:

- **Require two-factor authentication.** Admins can require a security code at login for everyone, with the option to remember trusted devices for 30 days.
- **Set company-wide security policies.** Ask everyone to use strong passwords, a VPN on unsecured networks, and up-to-date browsers and devices.
- **Use a strong, unique password.** A long, unique password is one of the simplest protections against unauthorized access.
- **Secure your network.** A VPN encrypts your traffic, which matters most on public or unsecured WiFi.
- **Stay updated.** Keeping devices, operating systems, and browsers current pulls in the latest security patches.

Add the Second Step at Login

The first item on that list is the one with a switch behind it. It's a company-level decision rather than a personal preference — a master admin turns it on for the whole account, then opts out anyone who genuinely has to be opted out.

Two-factor authentication adds a second step when you log in on a device Pipeline doesn't recognize: an email to finish logging in, with a link to click or a code to type.

See Two-factor Authentication

Our Commitments

Our Terms of Service and Privacy Policy spell out how we collect, use, and safeguard your information. Both are linked in the footer at paperlesspipeline.com. Together they cover your rights and responsibilities and our

commitment to your privacy and data security.

Frequently Asked Questions

Is my data encrypted?

Yes — in transit and at rest. All web-based communication with Pipeline uses industry-standard SSL encryption, and documents are stored on Amazon Web Services (AWS) with built-in encryption for stored data.

Is Paperless Pipeline PCI compliant?

Yes. Pipeline complies with the Payment Card Industry Data Security Standard (PCI DSS) and holds a PCI Compliance Certificate from SecurityMetrics.

Is my account's data separated from other companies' data?

Yes. Each company's account runs in its own distinct, secure environment. Actions in one account stay isolated and never affect another account's data.

Are emails I send from Pipeline secure?

They're encrypted in transit when the recipient supports it. Outgoing email goes through SendGrid, which uses TLS encryption to communicate with the recipient's mail server as long as that server supports encryption.

Can I send a password-protected or encrypted email from Pipeline?

No — there's no end-to-end or password protection on the message itself. Emails use TLS encryption in transit when the recipient's server supports it, but the document can't be individually password-protected.

Can I email encrypted documents to my Maildrop address?

No. Pipeline can't extract attachments from encrypted incoming emails. To keep documents encrypted on the way in, upload them directly with the Upload Doc feature instead.