Paperless Pipeline Security

Your Paperless Pipeline account gets the same security and protection an online bank gives its customers — industry-standard encryption, isolated accounts, and an extra login barrier you can switch on anytime.

Introduction

Paperless Pipeline runs your account on a comprehensive security framework with three fronts: server security, data encryption, and login protocols. The platform handles the heavy lifting. You and your team add the layers that fit your office.

The infrastructure is Amazon Web Services (AWS). The encryption is industry-standard SSL. Every account runs in its own isolated environment, so nothing crosses between companies. On top of that baseline, your office can require Two-Factor Authentication and set policies that match how your team works.

How It Works

Security in Pipeline is layered. Pipeline secures the platform, your company adds policies and 2FA, and each user shores up their own login.

Server and infrastructure (handled for you)

Pipeline runs on Amazon Web Services (AWS) — the same world-class server infrastructure many online banks use, with the same redundancy and protections. Every account operates in its own distinct environment, so actions in one account never affect another.

Encryption everywhere

All web traffic between your browser and Pipeline uses industry-standard SSL encryption (SHA-256 with RSA). The maildrop server receives docs over encrypted channels, and outbound email uses TLS encryption whenever the recipient's mail server supports it.

Login security

Password requirements follow guidelines from the National Institute of Standards and Technology (NIST) — length over forced complexity. The minimum is 8 characters. Easily-guessable words like *password* and *pipeline* are blocked. There are no arbitrary rules about mixing uppercase, numbers, or symbols.

Two-Factor Authentication

An optional second layer at sign-in. When your company turns it on, every user enters a one-time security code (sent to their login email) along with their password. See *Two-Factor Authentication* for the full setup and how it works at login.

PCI compliance

Pipeline holds a PCI Compliance Certificate from Security Metrics — the standard for safely handling payment card data.

Terms of Service and Privacy Policy

Two documents govern how Pipeline treats you and your data. The Terms of Service set out the rules for using Pipeline — your rights and responsibilities. The Privacy Policy spells out how Pipeline collects, uses, and safeguards your personal information. Both are linked from the platform and worth a read.

Good to know

- **Length beats complexity.** A long passphrase you can remember is more secure than a short one with required symbols. NIST's modern guidance is what Pipeline follows.
- **2FA codes go to your login email.** That makes the security of your email account part of the boundary. Keep that inbox locked down too.
- **Pipeline isolates each company's data.** Nothing in one company's account can be reached from another, by design.
- **High-impact requests need master admin sign-off.** Removing a master admin, canceling the account, or other account-wide changes need to come from the master admin's login email — for security and privacy.
- **Support can pull a login report.** If you need to see who signed in when (timestamp, IP, email used), ask support from your master admin email.

Require Two-Factor Authentication for your office

Adds a one-time security code at sign-in for every user, on top of the password.

Who can do this: Master admins.

Click your name in the upper-right corner, then **[Admin / Settings]**.

Scroll to **Feature Settings**.

Check **Require Two-Factor Authentication**.

Click **[Save Settings]**.

From the next sign-in onward, every user enters a security code Pipeline emails to their login address. To opt an individual user out, see *Two-Factor Authentication*.

Strengthen your team's security

A short list of habits that close the gaps platform security can't reach. Worth setting expectations on with the whole office.

Who can do this: Anyone — admins set the policy, every user follows it on their own login.

- **Use a strong, unique password.** At least 8 characters, no common words, and not one you've used

elsewhere. If you use a password manager, let it generate one for you.

- **Use a VPN on public Wi-Fi.** Coffee shops, airports, and open networks are where credentials get exposed. A VPN encrypts your traffic so it can't be intercepted.
- **Keep browsers and operating systems updated.** Security patches ride inside those updates. An outdated browser is a known vulnerability.
- **Turn on 2FA at the company level.** With a security code required, a stolen password alone won't get anyone in.

Get a recent login history

Helpful when you're investigating suspicious activity and want to see when and where sign-ins happened.

Who can do this: Master admins. Available on request from support.

From your master admin login email, write to support and ask for a login report covering the date range you're interested in.

Support generates the report with timestamp, IP address, and the email used for each sign-in, and sends it back.

If you suspect an account is compromised, follow this up by resetting the password and turning on 2FA. See *Re-secure a compromised account* for the full sequence.