Security FAQ

Paperless Pipeline secures your account with industry-standard encryption, isolated accounts, and login protocols you can layer on. These are the questions readers ask most often about how it all works.

What kind of encryption does Pipeline use?

All web traffic between your browser and Pipeline uses industry-standard SSL encryption (SHA-256 with RSA). The maildrop server receives emailed docs over encrypted channels. Outbound email uses TLS encryption whenever the recipient's mail server supports it. Together, these cover the path your data takes in and out of Pipeline.

Is Pipeline's infrastructure secure?

Yes. Pipeline runs on Amazon Web Services (AWS) — the same enterprise-grade server infrastructure many online banks use, with the redundancy and protections that come with it. Every company's account runs in its own isolated environment, so nothing in one account can be reached from another.

Is Pipeline PCI compliant?

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

Why doesn't Pipeline require special characters in passwords?

Because length beats complexity. Pipeline's password rules follow guidelines from the National Institute of Standards and Technology (NIST), which favors length over forced character-class rules. NIST research shows that mandatory symbol-and-number mixes tend to push people toward more uniform passwords — easier to guess, not harder. Long passphrases beat short complex passwords. Pipeline requires at least 8 characters and blocks easily-guessable common words.

Does Pipeline send 2FA codes by text message or by an authenticator app?

By email. When 2FA is on, Pipeline emails a one-time security code to your Pipeline login email at sign-in. That's the only delivery channel right now — so make sure the email account on your Pipeline profile is one you can actually access.

What should I do if I think someone got into a Pipeline account?

Change the affected user's Pipeline password and their email password right away. Turn on Two-Factor Authentication for your company. Then write to support — we can generate a login report (timestamp, IP, email used) to help you confirm what happened, and we can delete any unauthorized messages with admin approval. See *Re-secure a compromised account* for the full sequence.