Security FAQ

Explore frequently asked questions about the security measures taken to secure both the Paperless Pipeline server and account data.

How secure is the Paperless Pipeline server?

Paperless Pipeline incorporates an industry-standard security infrastructure, giving you the same data protection and redundancy as an online bank. It is built on the trusted foundation of Amazon Web Services (AWS) and employs industry-standard SSL encryption.

Learn more about Paperless Pipeline Server Security →

What type of data encryption does Paperless Pipeline use?

Paperless Pipeline employs industry-standard SSL encryption, utilizing SHA-256 with RSA encryption by GeoTrust. This ensures that every interaction between your device and our servers is protected with the highest standards of confidentiality and integrity.

View Paperless Pipeline's SSL Certificate →

What type of data encryption is used for docs and emails?

All web-based communication within Paperless Pipeline, including uploading and downloading documents, has end-to-end encryption and security.

Paperless Pipeline's email server supports encrypted channels for sending and receiving emails and any included attachments.

Learn more about Paperless Pipeline Data Security →

What certifications for data protection do you have?

Paperless Pipeline holds a PCI Compliance Certificate from Security Metrics.

Learn more about PCI Compliance →

What is your policy if your server data is hacked or breached?

Given our robust **security measures and extensive safeguards**, a security incident is highly unlikely. In the event of a data breach or hack, we will notify all affected customers, shut down Paperless Pipeline immediately, and dedicate all resources to investigating and resolving the incident.

Learn more about Paperless Pipeline's Commitments →

Do you offer two-factor authentication?

Yes, we offer two-factor authentication (2FA) as an optional extra layer of security for your Paperless Pipeline

account.

Learn more about Two-factor Authentication →

Why aren't your password requirements more stringent?

Paperless Pipeline password requirements are strategically designed to enhance your account's security by adhering to the latest guidelines recommended by the National Institute of Standards and Technology (NIST).

NIST advises against imposing arbitrary rules like requiring a specific mix of uppercase, lowercase, numbers, and symbols because they don't guarantee a strong password. In fact, ironically, stricter password requirements can lead people to create more uniform passwords to satisfy the criteria, making passwords easier to guess and harder to remember.

Instead, we encourage unique but memorable passwords by permitting you to decide which characters to use.

Learn more about Paperless Pipeline Login Security →

How can we make our login process more secure?

Admins can make accounts more secure by requiring two-factor authentication and setting company-wide security policies. At the same time, everyone can help by using strong passwords, VPNs on public networks, and up-to-date devices.

Learn Ways to Enhance Your Account Security →

Still have questions?

If you still have questions left unanswered, we're here to help! Please **contact us**.