Security

Secure Maildrop System

Paperless Pipeline's email server utilizes encrypted channels for receiving documents sent via Maildrop Addresses.

However, emails sent to Paperless Pipeline are only as secure as your email server and any internal email relay servers through which they reach Paperless Pipeline's email server.

To ensure your sending server also uses encryption, check with your Internet Service Provider (ISP) or local network tech support.

TLS Encrypted Emails

When you send an email from Paperless Pipeline, our email-sending service, Sendgrid, communicates with your recipient's email servers using TLS encryption as long as the recipient's server supports encryption. This adds an extra layer of security to your communication.

Learn more from Sendgrid →

Account Data Isolation

Paperless Pipeline utilizes thoughtful software architecture and meticulous database management to isolate the data of each company's account. Every account operates within its own distinct and secure environment.

This ensures any actions taken within one account stay isolated and do not affect data in another account. It also prevents any potential data compromise across multiple accounts.

PCI Compliance Certification

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

Learn more about PCI Compliance →

Login Security

Password Requirements

Paperless Pipeline's password requirements were designed according to the latest guidelines recommended by the National Institute of Standards and Technology (NIST), a globally recognized authority in cybersecurity.

Here are some ways Paperless Pipeline implements NIST guidelines for password requirements:

- We require a minimum of 8 characters to encourage longer passwords. NIST emphasizes the importance of password length over complexity. Longer passwords are typically more secure and easier to remember.
- We prohibit the use of easily guessable phrases. NIST recommends blocking easily guessable phrases by maintaining a list of known, weak passwords that cannot be used.
- We do not impose arbitrary rules like requiring a specific mix of uppercase, lowercase, numbers, and symbols. NIST advises against more stringent password composition rules 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

Learn more about NIST's Password Guidelines →

Two-factor Authentication

As an optional extra layer of defense, Paperless Pipeline offerstwo-factor authentication (2FA). When an account turns on 2FA, users who remain opted-in must provide a unique security code in addition to their password to access their account.

2FA, as an additional step, significantly enhances your account security by adding an extra barrier against unauthorized access.

Learn more about Two-factor Authentication →

Ways to Enhance Account Security

Admins

Here are some ways admins can contribute to a more secure login process and enhanced account security:

- **Require Users to Authenticate Their Device:** If your company requirestwo-factor authentication, users must enter a security code sent to their login email to gain access. The system can remember devices for 30 days, and admins can opt-out for any individual user. Learn more about Two-factor Authentication →
- **Set Company-wide Security Policies:** Establish company-wide security policies that require

everyone to do their part. For example, mandating the use of strong passwords, VPN usage on unsecured networks, regular browser updates, and device updates can significantly boost login security.

Everyone

Here are some ways everyone can contribute to a more secure login process and enhanced account security:

- **Use A Strong Password:** Choosing a strong, lengthy, and unique password helps protect your online accounts from unauthorized access.
- **Secure Your Network:** Use a Virtual Private Network (VPN) service (likeExpressVPN →), especially when connecting to public or unsecured WiFi networks. A VPN encrypts your internet traffic, shielding your data and enhancing your online privacy.
- **Stay Updated:** Keep your devices, operating systems, and web browsers up to date. Updates frequently include security patches that shore up vulnerabilities and protect against cyber threats. Staying updated also ensures optimal performance, access to new features, and better compatibility with various platforms and applications, including Paperless Pipeline.

Our Commitments

Terms of Service

Paperless Pipeline's Terms of Service outline the guidelines and obligations governing your use of the service. By accessing and using Paperless Pipeline, you agree to abide by these terms, ensuring a mutually beneficial and secure environment for all users.

View our Terms of Service → to understand your rights and responsibilities.

Privacy Policy

Paperless Pipeline's Privacy Policy details how we collect, use, and safeguard your personal information.

View our Privacy Policy →to learn more about our commitment to your privacy and data security.