Security FAQ

Security FAQ

Q: How secure is your server? What type of data encryption is used?

A: Utilizing industry standard SSL encryption and the world-class server infrastructure of Amazon Web Services (AWS), Paperless Pipeline ensures the security of our users' data. Paperless Pipeline incorporates an industry standard security infrastructure, giving you the same level of data protection and redundancy as an online bank.

Further security information is available here →
SSL certificate information about Paperless Pipeline's application may be found here →

Q: If we are using our link on your site to upload documents which would be an email from our email to your designated email address, would this be supported by the SSL technology also?

A: Emails are only as secure as your email server and any internal email relay servers (such as your ISPs email servers) through which they make it to Paperless Pipeline's email server. Our email server supports an encrypted channel for receiving documents sent to through the maildrop system. But you will need to check with your ISP and local network tech support to ensure that their sending servers also use encryption.

Q: Are the emails that are sent out from the Paperless Pipeline encrypted? If not, is this something that is being reviewed as a possibility?

A: Our email servers communicate with the recipient's email servers using TLS encryption as long as the recipient server supports encryption. You can find more details on SendGrid here → (the email sending service that Paperless Pipeline uses for sending out all emails from Pipeline).

We don't have plans to support encrypted emails to Pipeline's maildrop system because Pipeline would be unable to extract attached documents from them. If

you'd like to ensure that the documents submitted to Pipeline are encrypted during transmission, you should instruct your team to upload them directly into Pipeline using Pipeline's Upload Doc →feature instead of emailing them to their maildrop addresses. All web-based communication with Pipeline (including upload and download of files) has end-to-end encryption and security.

Q: What certifications for data protection do you have?

A: PCI Compliance Certificate from Security Metrics

Q: How do you isolate and safeguard my data from that of other clients?

A: Through a well-designed database and software system where each entity is isolated per client account.

Q: If one of your other clients gets hacked how does that affect us?

A: Because of the aforementioned per-client data isolation, compromise of one client's data will not affect that of another client.

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

A: We will notify all affected customers immediately upon the discovery of a data breach or hack. We will shutdown Pipeline immediately and dedicate all resources to investigating the incident and fixing it.

Q: What liability do you have or how do you help with that breach?

A: Our Terms of Service and Privacy Policy may be downloaded from here:

Terms of Service →
Privacy Policy →

Q: Do you have any 2 factor login process?

A: We do not offer 2-factor login.

Q: How can we make our login process more secure?

A: Require your users to select hard-to-guess unique passwords. Require your users to change their passwords at least twice a year. Require your users to use a standard VPN service when connecting through public, unknown, or insecure WiFi networks.