Paperwise Security Practices

Effective January 1, 2019

paperwise

Security Practices

We take the security of your data seriously at Paperwise. Transparency is one of the principles on which our company is built. As such, we aim to be clear and open about the way we handle your security.

To that end, this document outlines our internal process for protecting your corporate information and the security restrictions that come standard in our solutions. If you have any additional questions, please email them to info@paperwise.com.

Confidentiality

We are committed to ensuring that your information is not seen by anyone who should not have access to it. We place strict controls over our employees' access to the data you and your users make available via the Paperwise services—more specifically defined in your agreement with Paperwise covering the use of Paperwise ("Customer Data"). The operation of Paperwise requires that some employees have access to the systems that store and process Customer Data.

For example, in order to diagnose a problem, we may need to access your Customer Data. These employees are prohibited from using these permissions to view Customer Data unless it is absolutely necessary. We also have technical controls and audit policies in place to ensure that any access to Customer Data is logged.

All of our employees and contract personnel are bound to our policies regarding Customer Data and we treat these issues as matters of the highest importance within our company. Additionally, they are all required to attend security trainings while employed with Paperwise.

Personnel Practices

All employees are required to read and sign our comprehensive information security policy covering the security, availability and confidentiality of Paperwise services.

Compliance

The environment that hosts the Paperwise services maintains multiple certifications for its data centers including ISO 27001 compliance, PCI Certification and SOC reports. For more information about their certification and compliance, please visit the TierPoint Security website and the TierPoint Compliance website.

Security Features for Users & Administrators

In addition to the work we do at the infrastructure level, we provide your administrators with additional tools to enable their own users to protect their Customer Data.

Access Logging

Detailed access logs are available both to users and administrators. We log every time an account signs in, noting the type of device.

Administrators and owners of paid accounts have access to log files. We make it easy for administrators to terminate all connections and sign out all devices authenticated to the Paperwise services at any time.

User-Wide Two-Factor Authentication

All user profile security is managed through two-factor authentication and authorization on their accounts. This applies to both initial setup and forgotten passwords. Instructions for doing this are available on our Help Center.

Data Retention

Owners of paid Paperwise accounts can configure retention policies. Setting a custom duration for retention means that information or files older than the duration you set will be deleted on a nightly basis.

Deletion of Customer Data

Paperwise provides the option for Users to delete Customer Data at any time during a subscription term. Within 24 hours of an administrator initiated deletion, Paperwise hard deletes all information from currently-running production systems (excluding users, participants and search terms embedded in URLs in web server access logs). Paperwise services backups are destroyed within 14 days.

Return of Customer Data

The Paperwise services include the following export capabilities:

- Standard Exports: During a subscription term, administrators of any Paperwise services plan can export Customer Data
- Data Encryption in Transit and At Rest

The Paperwise services support the latest recommended secure cipher suites and protocols to encrypt all traffic in transit.

We monitor the changing cryptographic landscape closely; upgrade the service to respond to new cryptographic weaknesses as they are discovered; and implement best practices as they evolve. For encryption in transit, we do this while also balancing the need for compatibility for older clients.

Availability

We understand that you rely on your Paperwise systems to work. We're committed to making Paperwise a highly-available service that you can count on. Our infrastructure runs on systems that are fault tolerant, for failures of individual servers and data centers. Our operations team tests disaster-recovery, measures regularly and staffs an around-the-clock, on-call team to quickly resolve unexpected incidents.

Data Protection

Our document viewers can be configured to eliminate or restrict the ability to copy and paste data.

Documents are stored and transmitted using DoD level encryption.

Disaster Recovery

Customer Data is stored redundantly at multiple locations in our hosting provider's data centers to ensure availability. We have well-tested backup and restoration procedures that allow recovery from a major disaster. Customer Data and our source code are automatically backed up nightly. The Operations team is alerted in case of a failure with this system. Backups are fully tested at least every 90 days to confirm that our processes and tools work as expected.

Network Protection

In addition to sophisticated system monitoring and logging, we have implemented two-factor authentication for all server access across our production environment. Firewalls are configured according to industry best practices and unnecessary ports are blocked by configuration with TierPoint Security Groups.

Data Streaming

All data is streamed to the browser, eliminating the need or possibility of having any data at rest.

Host Management

We perform automated vulnerability scans on our production hosts and remediate any findings that present a risk to our environment.

All information including any unstructured data, such as images or files, are stored in a Microsoft SQL Filestream at the Host level.

Encryption

The communication from the user's browser session and the server or Host system is encrypted via TLS/SSL and handed over an HTTPs connection.

Logging

Paperwise maintains an extensive, centralized logging environment in its production environment that contains information pertaining to security, monitoring, availability, access and other metrics about the Paperwise services. These logs are analyzed for security events via automated monitoring software, which is overseen by our security team.

Incident Management & Response

In the event of a security breach, Paperwise will promptly notify you of any unauthorized access to your Customer Data.

Product Security Practices

New features, functionality and design changes go through a security review process facilitated by our security team. In addition, our code is audited with automated static analysis software, tested and manually peer-reviewed prior to being deployed. Our security team works closely with development teams to resolve any additional security concerns that may arise during development.

paperwise

ABOUT PAPERWISE

Paperwise is a midwest-based software development company that specializes in data and process management. For 30 years, we've worked with trucking companies across the U.S. and Canada to create solutions that let business owners focus on the future of their business.

Interested in finding out more about our services? Give us a call or find us online!

(888) 828-7505

sales@paperwise.com

www.paperwise.com/trucking

3171 E Sunshine Springfield, MO 65804