Sortly Security and Compliance FAQ

Who is your Cloud Hosting Provider?

We use Amazon Web Services (AWS).

In what geographic location is the Cloud Service hosted including backups?

We host in the us-west-2 (Oregon) region.

What certifications does Sortly hold?

We have no certifications at this time.

Is data encrypted while stored and in transit?

Data in transit uses SHA-256 with RSA, and AES-256 at rest.

Will the customer retain ownership of all company data?

Data is the property of its owner. companies can export their company data at any time and will be completely deleted from Sortly's servers on request.

Which authentication methods are used for the applications?

Our application is authenticated by default using OAuth2 for both our login and our API. We offer optional SSO with our Enterprise Plan which allows the client to configure an identity provider using OAuth2 or SAML v2 authentication standards.

Does Sortly utilize two-factor authentication and what methods are supported?

Our internal authentication method does not, though we do optionally offer SSO for customers on our Enterprise Plan, and external identity providers can be set up to use two-factor authentication.

Does Sortly use automated Intrusion detection or prevention systems?

Not at this time.

Who will have administrative access to Sortly?

Administration for the service as a whole is performed by Sortly, Inc. employees only.

Who retains information ownership and retrieval rights?

Customers own their content; Sortly cannot use or extract customer data without express permission.

Does Sortly utilize an antivirus solution and provider?

Antivirus protection is part of the AWS EC2 instances we use for Sortly.

Do you have a documented Privacy Policy and if so please provide policy?

Yes. https://www.sortly.com/privacy-policy

Does Sortly have a documented information breach management and notification process and if so please provide documentation?

We have internal protocols regarding immediate announcement if a breach occurs and a plan for maintaining integrity.

Do you have a documented Business Continuity Plan?

Not at this time.

Does Sortly backup data on a regular basis?

We backup the database every 24 hours and retain backup images for 35 days.

Are there documented procedures and APIs for importing and exporting data to/from the Cloud?

Sortly provides an in-product import/export feature as well as an API.

Has Sortly been penetration tested by an independent 3rd Party?

Not at this time.

How is malware fought?

All service images are scanned regularly and are hosted in a limited AWS VPC. Our REST endpoints are throttled and monitored for usage to detect malicious intent.

How is software updated?

Our software is updated weekly on Wednesdays with hotfixes as necessary in between. We regularly update our stack and libraries to keep on top of security patches.

How can data recovery be ensured?

Our data retrieval process is intended for disaster recovery with daily backups held for 35 days.

What measures are used for HW/SW (e.g. mirroring or maintenance)?

We replicate our data over three database instances.

Are there defined user roles?

We have three roles defined in our software. Owners have access to all folders and settings; Admins have access to all folders but cannot add/manage users or update billing information. Member roles can be limited to access specific item groups with read-only or edit permissions.

How are the operations performed in the applications logged?

We log operations on our server and client; all logs are stored for 30 days on our DataDog instance for monitoring and debugging. Transactions performed by a company's users are stored and available through an Activity History report for one year.

How is personal data archived (long term storage, e.g. in other systems)?

Personal data only resides in our relational database and our ElasticSearch instance for search. It is not stored anywhere else besides backup; logging only uses IDs and not personally identifiable data.

How is it ensured that the recorded data can be made available to data subjects?

Customers have access to all data for their company; you may export data in CSV, XLS, or PDF.

How is personal data processed in the test and development system?

We do not use our customer's data in test and development environments.