Security FAQs

Servers

Where are the servers located?	Amazon: US-East (N. Virginia) and US-West (N. California)
How secure are the servers?	Amazon's infrastructure takes a world class approach to securing their servers. For details regarding Amazon's security please read the following: https://aws.amazon.com/security/
If the software requires a web server, is the web server configured to use SSL version 2 and refuse connectivity on SSLv3?	We've disabled SSLv3 and SSLv2. We currently support TLS 1, TLS1.1, TLS1.2.

Certifications

Which security certifications do you have?	Dedicated security staff with multiple security certifications. Guidebook complies with the US-EU Safe Harbor Framework. To learn more about the Safe Harbor program, and to view Guidebook's certification, please visit http://www.export.gov/safeharbor/. In the UK, we also have data protection certification from the ICO.
Are you PCI compliant?	We delegate credit card transactions to Stripe, which is a PCI Level 1 Service Provider. More about Stripe's security.
Does the software vendor possess SAS70, SOC or SSAE16 audit credentials?	At the time we do not, but AWS has these audit credentials which is where Guidebook servers are housed. More information on Amazon's compliance credentials can be found here: https://aws.amazon.com/compliance/. Additionally, we conduct vulnerability assessments against our applications on a bi-annual basis. Results of these assessments can be shared upon request.

Users' personal data

When someone sets up a Guidebook login (i.e. don't use a social log-in like Facebook, LinkedIn, etc.) what happens to that data?	That data is stored on Guidebook's servers (Amazon).

Users' personal data (continued)

When creating this log-in users need to provide an email and password. Is this used by Guidebook in any way, and for what purpose?	The email and password is used for authentication only. We also use the account for syncing schedule data and to-do items across the user's devices (phone, tablet, desktop).
Are there any user passwords stored within the software or software database?	User passwords are stored as a one-way bcrypt hash in our database (Amazon RDS), which is also encrypted at rest.
What steps will be taken to reasonably ensure that accounts cannot be compromised?	Guidebook takes a proactive and holistic approach to security. Developers write security related unit tests, administrators ensure we have properly configured security controls and we contract security vulnerability assessments and penetration tests to highly respected third-party security engineers to validate our products. To learn more about our security practices, click here.
One of the ways people can access the app is by adding their phone number so they receive a text. Where are those phone numbers stored?	Phone numbers submitted for text messages are not stored. After the message is sent, the number is discarded from memory.

Builder data

How long does the data on Guidebook remain on a user's device? After a guide has been archived, is the content still available on the person's device?	The content is available on the person's device indefinitely. If you wish to remove a guide's contents from a user's device, you can delete the content from the content management system and publish an update. The next time the user opens their guide, it will download the latest update, which will clear any content you've removed.
How long is the data stored in the content management system (Builder)? Do we just export everything at the end of the event and then close down the app?	The data is stored indefinitely on Builder unless the event organizer requests its removal. After requested removal, it is permanently removed after a 1-week period.

Builder data (continued)

Are the password strength requirements configurable?	Guidebook user accounts are not configurable. Password protected guides are configurable. If you provide Single Sign-On Access to your app, you can configure password strength requirements via your identity provider.
Do these passwords automatically expire periodically?	Guidebook user account passwords do not automatically expire.
What information is encrypted?	Guidebook encrypts all sensitive data in transit and at rest using industry-standard algorithms.

Authentication

Does the product support integration with third-party security architecture such as Active Directory (AD) and Lightweight Directory Access Protocol (LDAP) groups for user authentication and authorization? How is that managed?	If you have a SAML 2.0 compliant Identity Provider (IdP), Guidebook can act as a Service Provider (SP). Your identity provider will handle the user sign-in process and will eventually provide the authentication credentials of your users to Guidebook. Guidebook does not store your user's passwords. To learn more, read our Single Sign-On (SSO) documentation.

Other

What is our security policy framework?	Our security policy is modeled after ISO27002 and NIST 800-53.
Does the product support Web Services Security (WS-Security)?	No support.
What are the development methodologies used?	Guidebook uses Agile and Scrum.

If you have a security concern or any additional questions, please contact security@guidebook.com