Frequently Asked Questions on Data Security

No	Question	Response
1	What infrastructure is used for hosting the application and the website?	TimeSolv is hosted by a state-of-the-art data center provided by Amazon Web Services (AWS). Highly encrypted 256-bit SSL is used for data transmission between your browser and our data center. AWS maintains SSAE-16 (formerly SAS 70) compliance with Service Organization Control (SOC) comprising SOC 1, SOC2, and SOC 3 compliance reports, as well as being ISO 9001 certified. Add that we're PCI DSS compliant to the mix, and you can rest assured your data is completely protected. For redundancy, the public facing website and support site is hosted with https://wpengine.com, a high availability hosting provider.
2	Is TimeSolv PCI (Payment Card Industry Data Security Standard) compliant?	TimeSolv is PCI compliant with security audit and compliance certified by SecurityMetrics, https://securitymetrics.com .
3	What mechanisms are in place to ensure that only authorized personnel will be able to access your data?	All passwords are encrypted and TimeSolv employees do not have access to passwords to access production data.
4	Does the contract address confidentiality?	Yes, the customer contract includes terms of service agreement addressing confidentiality of customers' information. See TimeSolv's Privacy Statement at https://www.timesolv.com/privacy-statement/
5	How frequently are back-ups performed?	Onsite backups are performed in real-time with maximum delay of 5 minutes on a redundant database server. In addition, TimeSolv provides automated daily backup via

No	Question	Response
		the Automatic Data Export services.
6	Is data backed up to more than one server? Where are the respective servers located? Will data always stay within the boundaries of the United States?	Amazon AWS Data centers are built in clusters in various global regions. All data centers are online and serving customers; no data center is "cold." In case of failure, automated processes move customer data traffic away from the affected area. Core applications are deployed in an N+1 configuration, so that in the event of a data center failure, there is sufficient capacity to enable traffic to be load-balanced to the remaining sites. Learn more https://d0.awsstatic.com/whitepapers/aws-security-whitepaper.pdf All data is kept within the United States.
7	How secure are the data centers where the servers are housed?	AWS's data centers are state of the art, utilizing innovative architectural and engineering approaches. Amazon has many years of experience in designing, constructing, and operating large-scale data centers. This experience has been applied to the AWS platform and infrastructure. AWS data centers are housed in nondescript facilities. Physical access is strictly controlled both at the perimeter and at building ingress points by professional security staff utilizing video surveillance, intrusion detection systems, and other electronic means. Authorized staff must pass two-factor authentication a minimum of two times to access data center floors. All visitors and contractors are required to present identification and are signed in and continually escorted by authorized staff.
8	What types of encryption methods are used and how are passwords stored? Is your data encrypted while in transit or only when in storage?	256-bit SSL for all data transmission and password storage. Data is encrypted while in transit.
9	Are there redundant	Amazon AWS Data centers are built in clusters in various global regions. All data centers

No	Question	Response
	power supplies for the servers?	are online and serving customers; no data center is “cold.” In case of failure, automated processes move customer data traffic away from the affected area. Core applications are deployed in an N+1 configuration, so that in the event of a data center failure, there is sufficient capacity to enable traffic to be load-balanced to the remaining sites. Learn more https://d0.awsstatic.com/whitepapers/aws-security-whitepaper.pdf
10	Does the contract include a guarantee of uptime? How much uptime?	TimeSolv is open to signing a guaranteed uptime and compensation due to unexpected period of downtime. TimeSolv’s historical uptime exceeds 99.95%.
11	If a natural disaster strikes one geographic region, would all data be lost? Are there geo-redundant backups?	• AWS uses multiple clusters in multiple locations. • Client can also receive copy of their data in CSV (Comma Separated Values) format via Automatic Data Export service at $19.95/month every day to backs up on their own servers
12	If there is a data breach, will you be notified?	TimeSolv has not experienced a data breach. Customers will be notified in case of data breach.
13	What rights do you have upon termination?	TimeSolv does not hold hostage any of client’s data. All data is available for download with a built-in option as CSV files. TimeSolv is open to providing a contract with specific service levels to meet client’s needs.
14	Can we back up data locally?	Each client can back up their data with an included download capability. TimeSolv doesn’t hold data hostage to resolve billing disputes. Client can also receive copy of their data in CSV (Comma Separated Values) format via Automatic Data Export service at $19.95/month every day to backs up on their own servers.
15	Code Generation Security	TimeSolv uses state of the art Code Generation, Optimization and Compilation from The OutSystems Platform. It generates, optimizes and compiles C# code using secure code patterns, as well as introducing the enhancements to the base framework outlined below:

No	Question	Response
		• HTTPS support to prevent eavesdropping and session hijacking • Strong session identifier validation mechanisms leveraging those provided by the Java and .NET frameworks to prevent intrusion on existing sessions from multiple devices • Cross-site scripting prevention by automatically escaping the generated HTML and providing built-in functions to sanitize HTML when developers handcraft HTML code • Encrypted password for database connections to securely create and manage database accesses • SQL code injection prevention by using SQL parameterization and providing built-in functions to sanitize the strings that developers include in their queries • C# and Java code injection prevention as the generated code does not allow any type of late binding or runtime access to any pre-compiled code • Dedicated and isolated database connection pools per each pair of application / database preventing cross application and cross database access in runtime • Total runtime isolation and containment by using code generation patterns that ensure there is no way to take advantage of low level process or thread configurations • Full exception handling as all exceptions (including encryption, authentication and authorization) are handled in the generated code and logged for later auditing even when handling was not created during development – this prevents the exploitation of any vulnerability arising from specific exception or error code in the responses provided to the browser. Ref: http://www.timesolv.com/wp-content/uploads/2016/08/OutSystems-Platform-security-overview.pdf