PROFILE

Security & Software FAQ

Describe your organization's business background and ownership structure, including all parent and subsidiary relationships.

Profile, LLC, is an Indiana based sole proprietorship established in February of 2014 by Chad Q. Brown, the sole owner, founder, and president. The headquarters is located at 128 North 3rd St. Lafayette, IN 47901. We are a boutique software HR assessment organization, we own proprietary software that facilitates behavioral data to sports and corporate organizations based on the DISC behavioral theory that was founded in 1928 at Harvard University by Dr. William Marston. DISC is a leading personality assessment tool popular within Fortune 500 companies, military groups, and organizations all over the world. It is a globally utilized tool provided in 27 different languages.

Describe how long your organization has conducted business in this product area.

Profile, LLC has conducted business for over 6 years in the behavioral assessment consulting space.

Describe how you perform security assessments of third party companies with which you share data (i.e. hosting providers, cloud services, PaaS, IaaS, SaaS, etc.). Provide a summary of your practices that assures that the third party will be subject to the appropriate standards regarding security, service recoverability, and confidentiality.

We only work with select IaaS and SaaS providers based on their reputation as industry leaders and their commitment to quality of service. We evaluate various metrics for providers including average downtime, how they handle incidents, support response time, best practices (use of modern security protocols), quality of API wrappers, and more.

Define what controls are in place to secure their remote environment and connection to our organization's data.

SSH keys are required for any connection and regular security checkups are in place to ensure latest antivirus definitions, OS updates, etc.

Have you or any third party you contract with that may have access or allow access to our organization's data experienced a breach?

No, we have not had a third-party that we have a contract with, inform us of a security breach that impacted our services.

Are databases used in the system segregated from front-end systems? (e.g. web and application servers)

Yes, Profile uses a detached client and server architecture with two databases. One database is dedicated to storing redundant assessment results on the "assessment scoring API server". The other database stores users, general applicant data, and other data required for the application to function.

Describe or provide a reference to all web-enabled features and functionality of the system (i.e. accessed via a web-based interface).

Users can join and create a organization account, login, purchase assessment credits, create job postings, edit job postings, delete job postings, view job postings, send assessment links associated with a job posting to applicants, view applicant reports, generate batch reports with multiple applicants, save reports as pdfs, edit applicant information, add additional assessments to an applicant, archive an applicant, view archived applicants, add new sub accounts, distribute credits to sub accounts, add new sub account users, edit sub account users, delete sub account users, upload files, edit sub account access to uploaded files, download uploaded files, delete uploaded files, edit branding for account portals, generate API key pairs, delete API key pairs, and view API documentation.

Describe or provide a reference to any OS and/or web-browser combinations that are not currently supported.

Profile is supported by all OS's and web browsers.

Describe or provide a reference to the facilities available in the system to provide separation of duties between security administration and system administration functions.

Security administration is not performed via the software. There is no "admin panel" or control for security administration. Security administration is performed by the development team via their own utilities.

Describe or provide a reference that details how administrator access is handled (e.g. provisioning, principle of least privilege, deprovisioning, etc.)

Administrator access is manually granted by Profile staff for security purposes. We do not allow clients to self-serve the type of account provided to educational institutions.

Does the system provide data input validation and error messages?

Yes, we do client and server side form validation. We are not susceptible to classic SQL injection attacks because we do not use a SQL database. All user input is sanitized.

Do you employ a single-tenant or multi-tenant environment?

Multi-tenant. Although instances of the application may be branched for load balancing purposes, all clients connect to a single running instance of the application. We use Node.js for our backend server, so instances are further broken down by available processing cores.

Describe or provide references explaining how tertiary services are redundant (i.e. DNS, ISP, etc…).

All of our server instances are hosted with IaaS providers which allow for seamless rollover to other data centers. We also use Cloudflare to cache DNS requests and static asset delivery. We store answers to assessment questions as answered to protect data in the event of an outage. In most cases, assessment results can be rescued even if our API services go down for a period of time.

Describe or provide a reference to the system capability to log security/authorization changes as well as user and administrator security (physical or electronic) events (e.g., login failures, access denied, changes accepted), and all requirements necessary to implement logging and monitoring on the system. Include information about SIEM/log collector usage.

We have access to log streams for the application logging all events. However, we do not currently store these logs on behalf of our clients.

Describe or provide a reference to the retention period for those logs, how logs are protected, and whether they are accessible to the customer (and if so, how).

Our 3rd-party logging service gives us 30 days of retention to any logs if we need to access them.

How and when will our organization be notified of major changes to your environment that could impact our security posture?

The Profile software has a change log prominently displayed in the main navigation of the software. Please refer to this for all new features.

Do clients have the option to not participate in or postpone an upgrade to a new release?

Yes, major feature releases are typically flagged on a per-account basis. Any new feature will be opt-in only. All performance, security patches and general improvements will be rolled out to all accounts without notice.

Describe or provide a reference to your solution support strategy in relation to maintaining software currency. (i.e. how many concurrent versions are you willing to run and support?)

Profile only deploys and supports a single version of the software. We handle client customization through account feature flags not version independence.

How does your organization ensure that only application software verifiable as authorized, tested, and approved for production, and having met all other requirements and reviews necessary for commissioning, is placed into production?

We perform CI testing and require all pull requests be checked by another software developer before merging into the production codebase.

Describe or provide a reference to your release schedule for product security updates.

We do not have a predefined release schedule for security updates. As updates are needed, they are released for immediate availability. Releases are typically done on a weekly basis.

Provide a brief summary of how critical patches are applied to all systems and applications.

All software deployments are automatic and instant.

Describe or provide a reference to how security risks are mitigated until patches can be applied.

Once a vulnerability is discovered, the profile team will evaluate the risk and possibly affected areas of the platform and react accordingly. There is no one case-fits-all protocol on how we address security vulnerabilities and patching.

Are upgrades or system changes installed during off-peak hours or in a manner that does not impact the customer?

Yes, feature upgrades, general fixes, performance improvements, etc are all performed during non-peak hours. From time to time, we may need to perform emergency maintenance in a way that impacts our customers, but we do our best to provide advance notice.

Do procedures exist to provide that emergency changes are documented and authorized (including after the fact approval)?

Yes, just in the sense that our engineering staff documents and agrees upon the action. From time to time, we may need to perform emergency maintenance in a way that impacts our customers, but we do our best to provide advance notice.

Describe or provide a reference to how institution data is physically and logically separated from that of other customers.

Profile uses an authorization check system on all requested resources to ensure the user with a given access key in fact has permissions to access the requested resource. All protected routes check this behavior on the server to prevent unauthorized access.

Is sensitive data encrypted in transport?

Yes. We use SSL/TLS for all connections.

Is sensitive data encrypted in storage (e.g. disk encryption, at-rest)?

Yes. Our 3rd party database provider encrypts all data stores and backups.

Describe or provide a reference to the encryption technology and strategy you employ for transmitting sensitive information over TCP/IP networks (e.g., SSH, SSL/TLS, VPN).

We use SSL/TLS to secure all connections and transmission of data.

List all locations (i.e. city + datacenter name) where our organization's data will be stored?

We host data with several IaaS providers with datacenter locations across the US. Please reference Heroku, MongoDB Atlas and Azure US data center regions.

Can our organization extract a full backup of data?

Yes, upon request.

Are ownership rights to all data, inputs, outputs, and metadata retained by our organization?

No. Your organization will be granted a non-exclusive rights license to the collected applicant data. Individual applicants are able to individually request deletion of data, therefore we cannot fully transfer ownership of the data.

Describe or provide a reference to the backup processes for the servers on which the service and/or data resides.

All data is backed up daily and encrypted.

Are backup copies made according to predefined schedules and securely stored and protected?

Yes. Backup copies are made on a daily schedule and securely stored.

How long are data backups stored?

6 months on a rolling basis.

Are you encrypting your backups?

Yes. All data is backed up daily and encrypted

Summarize the encryption algorithm/strategy you are using to secure the backups.

MongoDB does not provide us the exact algorithm/strategy for their encryption for security reasons.

Describe or provide a reference to your cryptographic key management process (generation, exchange, storage, safeguards, use, vetting, and replacement) of all system components (e.g. database, system, web, etc.).

All data encryption is handled by IaaS partners.

Do current backups include all operating system software, utilities, security software, application software and data files necessary for recovery?

Yes. Our stack runs on containers that can be replicated very quickly in the event of a backup situation.

Are you utilizing a web application firewall (WAF)?

Yes. We use Cloudflare to implement WAF and traffic rules.

Are you utilizing a stateful packet inspection (SPI) firewall?

No. We currently do not have any plans to implement this due to the nature of our hosting environment with Heroku.

State and describe who has the authority to change firewall rules?

Only our CTO has the authority to change the firewall rules.

Do you have a documented policy for firewall change requests?

Yes. All requests go to our CTO for final approval and implementation.

Describe or provide a reference to any other safeguards used to monitor for attacks?

We record logs of traffic and traffic sources to detect types of attacks such as SQL injection attacks, DDoS attacks, and etc.

Do you monitor for intrusions on a 24x7x365 basis?

Yes. We use several logging services to monitor connections as well as individual resource requests to flag for nefarious activity. Logs do not contain identifiable user information.

Describe or provide a reference to physical safeguards that are placed on facilities housing our organization's data (e.g., video monitoring, restricted access areas, man traps, card access controls, etc.)?

We rely on IaaS providers and cannot comment on their datacenter practices.

Are employees allowed to take home customer data in any form?

No.

Have your developers been trained in secure coding techniques?

Yes. Our developers regularly review each other's work, participate in online webinars, read articles and attend "boot camps" to stay up to date.

Was your application developed using secure coding techniques?

Yes. We always provide the best possible solution to any development feature making sure to escape user input, look for possible vulnerabilities, and etc.

Do you subject your code to Static Code Analysis and/or Static Application Security Testing prior to release? If so, what tool(s) do you use?

Yes. https://snyk.io/

Describe testing processes that are established and followed (e.g., development of test plans, personnel involved in the testing process, and authorized individuals accountable for approval and certification of test results)?

We perform peer review testing on all merged code. Our staff also tests features as a part of continued quality assurance. Our software development team runs automated test suites on all merged code.

Are information security principles designed into the product life cycle?

Yes. We take all reasonable measures to secure our application from a design perspective.

Describe or provide a reference to your system development life cycle methodology including your environments, version control, and change management (if not already covered in the Change Management section).

Local development environments run automated test suites before integration. All software is checked into version control and deployed using automated hooks to container environments after passing CI.

Will you comply with applicable Breach Notification Laws?

Yes. Once our team becomes aware of a breach, we will notify affected parties within 30 business days.

Will you comply with our organization's IT policies with regards to user privacy and data protection?

Yes.

Is your company subject to US laws and regulations?

Yes.

Do you require new employees to fill out agreements and review policies?

Yes.

Do you have a documented information security policy?

Yes. Available upon request.

Do you have an information security awareness program?

Yes. All employees/contractors are required to attend internal workshops reviewing security best practices to keep awareness high.

Is the security awareness training mandatory for all employees?

Yes.

Describe or provide a reference to your Internal Audit processes and procedures.

We audit our internal systems and procedures on a semi-annual basis with the development team. This internal audit mostly includes evaluating packages and 3rd parties as internal software packages and dependencies are all audited for vulnerabilities on every release cycle.

Do you incorporate customer feedback into security feature requests?

Yes, via email to the Profile representative that is handling your account.

Can you provide an evaluation site to our organization for testing?

Yes. A demo portal can be provided to various teams within your organization for testing purposes.

Provide a general summary of your Quality Assurance program.

Profile regularly performs disparate impact, validity and other studies on it's assessment catalog (through our assessment publishing partner) to ensure the highest quality behavioral index report possible. Profile also regularly tests new software features with 3rd party groups to provide the best possible online experience for our clients. Profile can customize our software or solutions to your needs for an additionally scoped development cost.

Will your company provide quality and performance metrics in relation to the scope of services and performance expectations for the services you are offering?

Yes. Upon request, we can provide quality metrics in relation to the scope of services and performance expectations we are offering.