FitnessGram® IT FAQs

GENERAL

Q) How do I access the software?

A) The new URL for all hosted FitnessGram® customers is https://myhealthyzone.fitnessgram.net.

Q) Are file uploads secure?

A) When a user uploads a file via the FitnessGram® 2015 application it is a two-step process:

1) The user transfers the file to the FitnessGram® VM via HTTPS (443)
2) The application transfers that file to our processing VM via FTPS port 989 or 990

Q) What is your backup/retention policy?

A) Point in time restore capability is up to 35 days, so a deleted student would be available on point in time restore for up to 35 days. Full archives are performed every 7 days and retained for 90 days so deleted data is available offline for up to 97 days. After 97 days, deleted data is completely removed from all backup/DR instances.

Q) Who owns the content of data stored in FitnessGram®?

A) You retain all rights and ownership of your Content. "Content" means the information and data, provided by you concerning your students, assessments, schools, and operations. The Cooper Institute® does not claim any ownership to your Content. Ownership of all information entered into the software remains with the School/District and can be accessed and/or exported by the School/District at any time.

Q) What is the availability of the website and data?

A) The data will be available 7 days a week, 24 hours a day, unless an outage has been communicated beforehand. A system notification will be posted in advance of any planned maintenance.

Q) In what format is the data stored at the host site?

A) The content is held within an encrypted Microsoft Azure® SQL database.

Q) Where is the live data actually stored? Where are the backups stored? (Are all sites within the continental US?)

A) Data is stored in a Microsoft Azure® data center on the US East Coast. For continuity and recovery purposes, all data is also mirrored into a separate Microsoft Azure® data center on the US West Coast.

Q) What method is used for encryption of data both in transit and at rest?

A) Data is encrypted in transit via HTTPS and at rest via TLS. Data entered via the front-end is encrypted during transport and remains encrypted in the database. When data files are uploaded into the system, they are immediately encrypted upon receipt. The transmission is via a secure connection.

Q) Can the school district access its own data? In what format will this data be retrieved?

A) School/District data and can be accessed and/or exported by the School/District at any time with a research extract. This extract is provided in a CSV (comma-separated-values) format, and should be readable by ISD applications.

Q) Are companies involved in the delivery of FitnessGram® FERPA compliant?

A) The vendor complies with the requirements of The Family Educational Rights and Privacy Act (FERPA) (20 U.S.C. § 1232g; 34 CFR Part 99); the Federal law that protects the privacy of student education records.

Q) Q) Are companies involved in the delivery of FitnessGram® Web Content Accessibility Guidelines (WACG) compliant?

A) Yes.

Q) How do you handle Information Requests or Disclosures?

A) We may access or disclose information about you, or your use of the Services (a) when it is required by law (such as when we receive a valid subpoena or search warrant); (b) to respond to your requests for customer service support; or (c) when we, in our discretion, think it is necessary to protect the rights, property, or personal safety of us, our users, or the public. Currently the system does not have a way to specifically retain information to hold data for litigation or other purposes. In the event that such a necessity arises, a backup of the data can be taken and explicitly retained.

Q) Do you perform Security Audits? Are the results publically available?

A) Security audits are performed twice a year, and for security purposes the test results are confidential.

Q) What would happen in the event of Service Discontinuation?

A) We may modify or discontinue the Services, FitnessGram® Software, or any portions or features thereof at any time without liability to you or anyone else. However, we will make reasonable effort to notify you before we make the change. If we discontinue a Service in its entirety, we will also allow you a reasonable time to download your Content, and we will provide you with a pro rata refund for any unused fees for that Service that you may have prepaid.

Q) Will the staff at the companies involved in the delivery of FitnessGram® be accessing school data?

A) We will not access, or view any of your Content, except as reasonably necessary to perform the Services. Actions reasonably necessary to perform the Services may include (but are not limited to) (a) responding to support requests; (b) detecting, preventing or otherwise addressing fraud, security, unlawful, or technical issues; and (c) enforcing our terms of use.

Q) In what format is FitnessGram® data stored?

A) The content is held within an encrypted Microsoft Azure® SQL database.

Q) What is the frequency of system updates and how are these handled?

A) FitnessGram® 2015 runs on Microsoft Azure® SQL in a geo-redundant high availability configuration and the database instances are automatically patched by Microsoft®. See https://azure.microsoft.com/enus/blog/patching-sql-azure. The FitnessGram® 2015 application runs on multiple geo-redundant VMs, which are automatically updated by Microsoft®.

APPLICATION SECURITY

Q) Does the software development life-cycle model used by the hosting service provider in the development of their software, incorporate features from any standards based framework models (e.g. TSP-Secure, SAMM, Microsoft® SDL, OWASP, NIST SP800-64 rev 2,)?

A) The software development life-cycle model used by the hosting service provider in the development of their software does NOT, at this time, incorporate features from any standards based framework models (e.g. TSP-Secure, SAMM, Microsoft® SDL, OWASP, NIST SP800-64 rev 2, etc.). Security components are NOT, at this time, identified and represented during each phase of the software development life cycle.

Q) Does the service provider have change management policies in place?

A) Yes, the service provider has change management policies in place.

Q) When are maintenance changes applied?

A) A pre-determined maintenance window is used to apply changes.

Q) Does the service provider have a process to test their software for anomalies when new operating system patches are applied?

A) Yes

Q) Has a technical and/or security evaluation been completed or conducted when a significant change occurred?

A) Yes

Q) Are source code audits performed by someone other than the person or team that wrote the code?

A) Yes

Q) Is access to the service provider's application restricted to encrypted channels (e.g. https)?

A) Yes

Q) What are the session management processes used by the hosted service's applications?

A) The session management processes used by the hosted service's applications can be described as follows:

FitnessGram® 2015 Software is based on *The Claims Based Identity Model*, which is fully integrated with Windows Identity Foundation .Net Framework 4.5.When a User Logs in, the user presents an identity to FG2015 application as a set of claims. The idea here is that an external identity system is configured to give the FG2015 application everything it needs to know about the user with each request s/he makes, along with cryptographic assurance that the identity data you receive comes from a trusted source as the user navigates through the FG2015 System.

FG2015 WIF Session Management:

Requests are handled by the session module after an authentication is established. While the session is in active use the authentication module is in a bypassed state. Upon time session time out (30 min) or user log out the authentication module is re-invoked.

AUTHENTICATION

Q) Are user IDs unique?

A) Each user will have a unique User ID within their jurisdiction.

Q) Are strong passwords required?

A) Strong passwords are required when manually creating or resetting, but not when importing when accounts are created automatically. Users may change their own password securely, and at that time, a strong password is required.

Q) Do passwords expire? Are the users forced to change them periodically?

A) Passwords do not currently expire so an active user is not forced to change. Accounts not currently in an active class will be inactivated, and inactive users are not allowed to log in.

Q) Are accounts locked out after a certain number of attempts?

A) No

Q) Are users automatically de-authenticated after being inactive for a certain period?

A) No, but users who are not active in a class are called “Inactive”, and Inactive users may not log in.

Q) Are passwords visible in the software?

A) No, Passwords are entered in a non-display field.

Q) Are Passwords encrypted during network transit and storage?

A) Yes, passwords are encrypted during network transit and storage.

Q) Are password attempts logged?

A) Password attempts (both successful and unsuccessful) are not logged and maintained.

Q) Does the software support two-factor authentication?

A) Two-factor authentication is not supported.

AUTHENTICATION PROTOCOL

Q) Can Service Provider authenticate with LDAP, Shibboleth/Incommon, Active Directory, CAS or any custom NetIDs program?

A) No

AUTHORIZATION

Q) Will users will be authorized by the hosting service provider's system

A) Yes

Q) Will the system restrict access within the application based on roles assigned to authorized users?

A) Yes, examples of such roles include the following:

- ✓ Teacher
- ✓ Student
- ✓ Parent
- ✓ School Administrator/District Administrator/State Administrator

Q) Are security reports that identify users and their access levels available?

A) No, but a district administrator can log in and see all users and access levels within their jurisdiction.

Q) Are accounts automatically disabled after a defined period of non-use?

A) No, but users who are inactivated, when not in an active class, are not able to log in

Q) Are service provider's security controls able to detect and report unauthorized access attempts?

A) Yes

DATA SECURITY

Q) Is all network transfer of client Restricted/Confidential Data encrypted when traversing the service provider's network and the client network or non-client networks?

A) Yes

Q) Is all network transfer of client Restricted/Confidential Data encrypted between multiple service providers' systems (e.g., Web and database servers?)

A) Yes

Q) Is all physical transfer of client Restricted/Confidential Data encrypted (e.g. backups to tape, disk, DVD)?

A) Yes

Q) Will client Restricted/Confidential Data will be stored, temporarily or otherwise, on end-user workstations, portable devices, or removable media?

A) No

Q) Since encryption is used, are there are procedures for key generation, distribution, storage, use, destruction, and archiving?

A) Yes

Q) Does the service provider's software provide appropriate controls to ensure data integrity (e.g., input validation, checksums of stored data, transaction redo logs)?

A) Yes

Q) Do the service provider's developers and systems administration staff, who have access to client Restricted/Confidential Data, have unique account IDs assigned to them?

A) Yes

Q) Are the duties of the service provider's technical staff separated to ensure least privilege and individual accountability, and are there documented job descriptions that accurately reflect assigned duties and responsibilities and that segregate duties?

A) Yes

Q) Are the activities of service provider's technical staff logged when performing system maintenance?

A) No

Q) Is user-level access to client Restricted/Confidential Data logged, monitored, and possible security violations are investigated?

A) Yes

Q) Is this log data available to the client?

A) No

Q) Does the log data does not specify the data element or data record accessed and the action taken upon the data?

A) No

INCIDENT RESPONSE

Q) Does the service provider have a documented process for reporting security incidents involving systems used to store/access/modify hosted client data to the client contact or, if appropriate, law enforcement?

A) Yes

Q) Are security incidents are monitored and tracked until resolved?

A) Yes

Q) Are incident information and common vulnerabilities or threats shared with owners of interconnected systems or data hosting customers?

A) Yes

Q) Will a third party have access to the service provider's hardware or systems that store client Confidential Data?

A) Yes

Q) Are the service provider's database and Web server access and error logs regularly reviewed for anomalies that could indicate a compromise?

A) Yes

Q) How is breach detection handled?

A) Breach detection is handled by the Microsoft Azure® security team. Microsoft® has a global, 24x7 incident response service that works to mitigate the effects of attacks and malicious activity. The incident response team follows established procedures for incident management, communication, and recovery, and uses discoverable and predictable interfaces with internal and external partners alike.

Q) In the event of a breach, will the client be notified of the breach and the extent of the data exposure?

A) Yes

Q) Will the client be notified of data requests, such as subpoenas or warrants, from a third party?

A) Yes, where feasible and allowable by law

OPERATIONAL CONTROLS

Q) Does the service provider outsource hosting of application and data storage servers to a third-party?

A) Yes

Q) Describe the physical security of the data center.

A) The service provider has taken measures to ensure the physical security of the data center(s) in which the application and data storage servers are housed, specifically

addressing access controlled and audited entry ways, temperature monitoring and control, fire prevention and suppression, and use of a backup power source.

Q) Is the service provider is currently providing hosting services for other clients?

A) Yes, multi-client access is effectively controlled to ensure users are restricted to only the data they are authorized to access.

Q) Does the service provider maintain and apply host security standards on their servers and verify them whenever changes in configuration are introduced into the system?

A) Yes

Q) Does the service provider have, and exercise a process, to maintain current patch levels of software running on their systems?

A) Yes

Q) Does the service provider implement anti-malware controls on servers?

A) Yes

Q) Does the service provider have an information security audit or evaluation program for their operation?

A) Yes

Q) Does the service provider have an effective procedure for timely termination of access of their staff and Client users (upon notification) who no longer need access to the service provider's system?

A) Yes

Q) Can clients request and receive special administrative access to the hosted service on vendor systems?

A) No administrative access to hosted service on vendor systems will be granted to clients other than what is provided by the standard GUI.

Q) Are tests and examinations of key controls routinely made ? (e.g., network scans, analyses of router and switch settings, penetration testing?

A) Yes

Q) How does the service provider ensure the expertise of employees who have access to client Restricted/Confidential Data?

A) All staff with access to data undergoes a background check at hire. Anyone with direct database access has passed an interview process and has more than 1 year working with the program. Direct access to the live database is very limited.

Q) How is remote access for staff handled?

A) For service provider staff with remote access to systems that store client Restricted/Confidential Data, any remote access is username/password/IP restricted.

Q) What is the backup/retention policy?

A) Upon direction from Client data will be deleted from the host systems. Per the backup retention policy, data will persist in backups for 97 days, after which it is completely removed.

PURPOSE OF SYSTEM

Q) What is the purpose of the FitnessGram® software?

A) FitnessGram® 2015 will be used for the collection and assessment and reporting of personal fitness information.

RECOVERABILITY

Q) Is there an exit strategy in the event the client cancels the contract?

A) Yes

Q) What is the format of the data collected?

A) The format of collected data to be made available to the client will be Excel, CSV and PDF.

TESTING AND VALIDATION

Q) Are risk assessments performed and documented on a regular basis or whenever the system, facilities, or other conditions change?

A) FitnessGram® 2015 resides on the Microsoft Azure® platform and no such changes are anticipated. If we were to change the platform a risk assessment would be performed.

Q) Is a testing application environment available?

A) Hosting service provider can make available a test evaluation instance of their service or application that can be used by Client IT security staff to validate the information security assertions made by the vendor (e.g. Sandbox). Client may have access to all levels of the front end necessary, but client will not have access into the back end database.

CONTENT OWNERSHIP AND ERROR CORRECTION

Q) Who can edit or delete data in the system?

A) Within the system, pupil-generated content is editable by both the pupil and by school administration (may vary by specific module) and presiding teacher. While a pupil does not have the capability to fully remove their content, the administration does maintain that capability.

Q) How are data errors noticed by parents rectified?

A) Parents can log in and see all data for their pupils. If some information is in error, parent must contact the pupil's physical education teacher to correct the discrepancy in the system. In the event the erroneous information was provided to FitnessGram® via an update from another system, the physical education teacher will need to alert the appropriate administrators of that system to ensure the erroneous information is corrected at the source.

** These IT FAQs may be modified/updated at any time to remain current with industry standards and regulations and as required by law.*

IT ACRONYM KEY

CAS: Central Authentication Service

CSV: Comma-Separated Values file format

FAQ: Frequently Asked Question

FTPS: File Transfer Protocol Secure

GUI: Graphical User Interface

HTTPS: Hypertext Transfer Protocol Secure

IIS: Internet Information Services

IT: Information Technology

LDAP: Lightweight Directory Access Protocol

Microsoft® SDL: MICROSOFT Security Development Lifecycle

NIST: National Institute of Standards and Technology

OpenSAMM: Open Software Assurance Maturity Model

OWASP: Open Web Application Security Program

PDF: Portable Document Format

SDLC: System Development Life Cycle

SQL: Structured Query Language

TLS: Transport Layer Security

TSP-Secure: Software Engineering Institute's Team Software Process-Secure

URL: Uniform Resource Locator

VM: Virtual Machine

WIF: Windows Identity Foundation