ActiveXchange Data Security Fact Sheet

Intended Audience

This document is intended for integration partners and clients who are looking to familiarize themselves with the data security processes and standards in place at ActiveXchange when working with the ActiveXchange platform. Typically, this information would be of interest to Information Security / Compliance / Risk Management roles within these organizations.

Architectural Overview

ActiveXchange is a cloud-native SaaS application delivered securely to our customers through a web-browser interface requiring no on-premise installation or support. The application consists of an Angular SPA front-end with a secure REST Web API developed in .NET 5 leveraging other Microsoft Azure (backend) services.

Our product stack is built entirely within Microsoft Azure, and we utilize the following services to deliver the application:

1. Azure App Services / Azure Static Apps / Azure Functions
2. Azure SQL Database / Azure Data Factory / Azure Databricks
3. Azure Service Bus
4. Azure Key Vault
5. Azure Blob Storage
6. Microsoft Defender for Cloud

Information Security

Answers to frequently asked questions around information security.

Q. **Which IT operational, security, privacy related standards, certification, and/or regulations do you comply with? (ISO-27001, HIPAA, PCI, ISO-22307, CoBIT, etc.)?**

A. As a company we are working towards ISO-27001 internally and hope to achieve certification by Q4 2024. Microsoft Azure compliance disclosures can be found at https://docs.microsoft.com/en-us/azure/compliance/offerings/.

Q. **How do you handle PII (Personally Identifiable Information)?**

A. Our core subscription offering does not request typical PII such as name, phone or email address of individuals. We do, however, require a date of birth (can be obfuscated to an accuracy of a year) and a physical address (can be obfuscated to a postal code). Both of these pieces of information are discarded permanently during our ETL process (within minutes of receiving data) and are never used or displayed within any user-facing element of our product. During the ETL process, this data is used for the following purposes:

1. Date of Birth (accuracy of a year) allows us to attribute an individual to an age bracket for statistical purposes. The bracket size may vary, typically no smaller than five years.
2. Physical address (postal code) is immediately geocoded into latitude and longitude coordinates. The coordinates are then located within the smallest statistical block geography defined by the official government statistics body in the territory of

operation (e.g. Statistics Canada, US Census Bureau, etc.). These block geographies are developed to ensure anonymity and prevent the ability to use geographic information to locate an individual. Once this block assignment is completed, both address and geocoded coordinates are permanently removed from our system.

Note: Integration partners can optionally provide us with the geographic coordinates directly in place of a physical address, if capable.

Q. **How is client data isolated?**

A. Client-specific and sourced data is co-located within shared database tables and partitioned on tenant keys. Tenant isolation is assured at a code level via global query filters within our Entity Framework data access layer.

Q. **Is data encrypted in transit and at rest?**

A. All data transmission occurs over HTTPS at a minimum of TLS 1.2. Our .app domain suffix can only ever be accessed via HTTPS and enforced via HSTS at the domain level (.app controlled by Google). We utilise Microsoft's "Encryption at rest" within Azure and more information on this can be found at: https://docs.microsoft.com/en-us/azure/security/fundamentals/encryption-atrest.

Q. **How are SSL Certificates managed?**

A. Automatic renewal provisioning as part of Azure App Service. No manual handling of SSL certificates. (The exception to this rule is the certificate securing our CMS platform powering our in-app module "ActiveXchange Academy". This element contains no client content and provides CMS services to our Client Success team as part of our educational resources).

Q. **Where is data stored?**

A. Client-sourced data is stored in Microsoft Azure SQL Databases within the Azure cloud. We host elastic pools in the territories we operate within. For clients in Australia / New Zealand these are hosted in the "Australian East" data centre (NSW). For North American clients, these are located in the "Canada Central" data centre (Toronto). We aim to ensure data residency in the country of operation where Microsoft offers the ability to do so.

Q. **How often are external penetration tests performed?**

A. We are currently evaluating PTaaS (Penetration Testing as a Service) vendors and anticipate selecting a service that aligns with our product release cycle to perform a penetration test after each product release. We expect this to be in place in early 2024.

Policies and Procedures

Answers to common process and procedure questions.

Q. **Do we have an information security policy?**

A. Yes, this policy is reviewed annually and is available on request.

Q. **Do you disclose all vulnerabilities that are discovered in your software?**

A. Our vulnerability assessment process will determine whether client-sourced data may have been compromised by the vulnerability. If so, a security advisory is issued to all clients via

email in accordance with our security policy. If the vulnerability was not capable of accessing or compromising client-sourced data, we prioritize hot fixing the vulnerability without client disclosure.

Q. **Do we have a disaster recovery plan?**

A. As an entirely cloud-native product, our DR plan leverages the scalability and availability of cloud services. Our entire stack can be redeployed within an hour globally in the event a service at a particular Azure Data Centre goes offline due to the data centre becoming unavailable. SQL Data Backups provide us with point-in-time recoverability. As we are not processing real-time data, a client account could also be fully recovered by simply ingesting their data again, if required.

Q. **How is employee access to client-sourced data governed?**

A. We follow the "least privilege" approach to data access such that only personnel who require access to the data to complete the function of their role are granted access to the underlying data. This is limited to the roles of "Data Engineers," who manage the performance and optimization of our databases and "Developer" roles (software/SQL), who build our technology stacks. Our product support personnel have product access at the same level as our "organization admin" role to assist in product support. As the account owner, you can enable/disable this access and review when it was last used.

Our product has full database table-level auditing, allowing us full transparency of data access and modification.

Q. **What is your incident management process?**

A. We follow a six-step IMP where incidents flow through the following process;

1. Log Incident (we use ClickUp as our tracking tool)
2. Prioritise Incident (Low, Medium, High) depending on the severity / impact.
3. Classify Incident – (Platform (Azure), Software, Security, Performance) work to identify which part of the technology stack is effected.
4. Resolution – data/tech teams work to resolve the issue.
5. Communication – communicate with clients affected by the incident to advise of the resolution.
6. Analysis – analyze the root cause of the issue and implement processes to mitigate similar future occurrences.

Data Structure & Schema

Answers to frequently asked questions about the types, structure, and elements of client-sourced data required.

Q. **What type of data do you require access to?**

A. Sport (products): we work with "Seasons" (Years) and request information about members, memberships, clubs, and teams for each season (year). For season (yearly) comparisons, historic seasons can be loaded into the platform.

Operator (products): we recommend ingesting the latest three years' worth of member, membership (and suspension), visit, participation, and enrollment data as the platform includes trend and forecast capabilities which require this duration of data legacy.

Movement (products): require no client-sourced data. Users are required to "name" elements created within the platform.

Infrastructure Database (products): require no client-sourced data. Users are able to contribute data related to location names, addresses, website, hours of operation, etc. of "sites", amenity details (name, size, surface, setting, etc.) of "facilities"/"spaces", and define activity usages within the platform.

Data Schema standards are available on request and detail each of the mandatory (and optional) data fields we require for you to work with ActiveXchange.

Q. **Can data be exported from your application?**

A. ActiveXchange produces client and product-specific statistical information about the client's operation and will never provide individually identifiable information about a person (member). Dashboards can be exported to PDF, and individual widgets on dashboards can be exported as PNG images for use in external presentations and documents. RAW data is never exposed.

Our Movement Pro product supports .CSV data exports of movement activity data. This data is licensed by ActiveXchange via a third-party and includes no client-sourced data.

Q. **How can data be supplied to ActiveXchange?**

A. Our preferred integration method is using our APIs to directly insert data into the platform. We are working with leading software vendors to ensure this is as seamless as possible for our shared clients and encourage them to work with their software vendors to advocate for an integration wherever possible. Larger clients may wish to build their own proxy service, and we are happy to provide technical consultation as required.

Alternatively, we allow standard .XLSX flat-file formats that clients can self-manage and upload directly within the ActiveXchange platform. For those clients who have the technical capacity internally, we recommend this be scheduled as an automated extract and delivered to your internal platform owner (e.g. Using SSRS internally to extract data at a specific schedule).