
**IT Security Policy**

**Last updated: January 2021**

Appendix A: Supplier details and penetration testing (SportsEye v1.0 and v1.2)
Appendix B: Summary risk assessment

This document is prepared and managed by ActiveXchange and is intended for users and system administrators and relates to the IT security standards maintained across all platforms developed by ActiveXchange.

ActiveXchange follows the standards and recommendations of ISO 27001.

General client principles and terms are available at the following:

- Data Use including privacy terms, our see Standard Data Use Agreement, which can be downloaded here: https://activexchange.org/your-data-our-commitment
- Service Level Agreement: https://activexchange.org/service-level-agreement
- Data Transfer Guidelines: https://drive.google.com/file/d/1aBPixlNBPs0CrJ6pXE4ulVdszOHgIcbR/view?usp=sharing

## Common Definitions

**Data Owner:** the Client is deemed to be owner of the Data and to own all right, title and interest in and to all of the Data and shall have sole responsibility for the legality, reliability, integrity, accuracy and quality of the Data when provided.

**Data processor:** the role of ActiveXchange. Processed data relates to the structured output created by ActiveXchange through its processing of the Data;

**Service provider:** ActiveXchange unless otherwise specified.

**Warranties:** the Service Providers represent and warrant to the Client (and Data Owner) that they will act in accordance with all applicable laws and regulations including, without limitation, the Data Privacy Act 1988, and with all reasonable skill and care in a timely and professional manner by appropriately skilled and qualified persons;

**SportsEye platform:** the primary cloud-based software through which processed data is accessed by ActiveXchange Clients.

**Offline Analysis Reports:** ActiveXchange provides a set of report products, based on predictive models, which use processed and aggregated data to inform planning and investment decisions.

**Personal data:** as defined by the Data Privacy Act 1988

**Systems:** refers to the full stack of data management and software applications.

**Users:** those who are issued outputs by ActiveXchange or provided with access to SportsEye accounts to access processed data.

**Primary purpose (of service):** the intended purpose for the sharing of data by the Data Owner and as outlined in the Data Use Agreement.

**Data Sharing Code of Practice**

1. Organisations in the Australia and New Zealand community sport and leisure sector wish to share data with ActiveXchange to:
    a. Increase participation in sports and other physical activity;
    b. Improve operational performance;
    c. Achieve better returns from financial investments in facilities;
    d. Enhance relationships between sports bodies, tiers of government and other stakeholders.

2. The scope of the data to be shared with ActiveXchange covers data on members and participants, activities and participation, facilities, membership types and status, and programs; it includes personal data for the purpose of understanding a persons activity profile. Personal data is never used to contact the individual without further enhanced permission from the Data Owner, or is it transferred to a third party. We typically do not request or require names or contact details. In addition, any personal data we receive is usually anonymised as part of the loading process. See ActiveXchange's **Data Transfer Guidelines** for the latest data fields used within each product.

3. Partners and clients agree to share data for the following Purposes:
    a. Production of processed data and reports to provide (and facilitate) improved decision making with regard site programming and investment, typically accessed via a SportsEye account.
    b. Anonymous benchmarked processed data and reports on sportsactivity, users, programmes, facilities and operational performance;
    c. Reports – structured reports on operational and financial performance relating to the operator based on the processed data.

4. ActiveXchange will use the Data only for the agreed purposes and will always respect the rights of all Data Owners. All source data provided by the Data Owner is securely deleted on written request.

## ActiveXchange's Views on Information Security

ActiveXchange is committed to ensuring the integrity of the information generated and stored within their databases and accessed via their online platforms and compliance with relevant legislation covering this area. To maintain this integrity in what can be regarded as a transient medium ActiveXchange believes that it is essential to establish and conform to clearly defined standards of operation in relation to platform-based information. To assist with this ActiveXchange has developed this IT Security Policy, which is reviewed and updated annually.

ActiveXchange also aims to make its Employees and Users of their databases and platforms aware of this Policy and also of other relevant standard practice and legislation, and how to achieve compliance with them.

## Policy Statement on Information Security

(1) ActiveXchange seeks to ensure that all information received, generated and stored within their databases and online platforms developed by the organisations is accurate and appropriately managed.

(2) All clients, partners and employees with access to the information kept within ActiveXchange platforms will conform to the IT Security Policy.

(3) All data connections to external bodies is validated to conform to the IT Security Policy.

## General principles of Implementation

### Scope

The IT Security Policy covers all online platforms developed by ActiveXchange and use of processed data for offline analysis reports. All new systems must have their security controls agreed by ActiveXchange's Cyber Security Director, or a nominee.

The IT Security Policy may be changed at any time in order to maintain currency as technology changes or as new threats emerge. Users are informed appropriately.

### Conditions

- All systems within the company and connections to outside bodies must conform to this Policy. ActiveXchange will ensure that the Policy is put into practice.
- ActiveXchange reserves the right to isolate any system or network that represents a potential or actual breach of security.
- ActiveXchange reserves the right to monitor information sent over its networks.

### Access Control

- All databases and platforms, except those designed for public open access, are required, at their point of entry, to have an auditable sign-on procedure with a unique, traceable Identifier and Password.
- A multi factor authentication required to access the Azure database (ActiveXchange's data warehouse)
- All access to databases and platforms is audited to ensure traceability and responsibility.

- Access and connection to selected wider networks is restricted to authorised Users only.
- ActiveXchange reserves the right to deny systems access to users.

**ActiveXchange System Administration**

Assigning administrative responsibilities for ActiveXchange's systems is absolutely necessary in order to maintain security.

The System Administrator holds the following:

- The responsibility for the Administration of the computer system, including security administration, is assigned to knowledgeable individuals and authorised by ActiveXchange's Chief Information Officer (who reports to the Executive).
- The Administrator is aware of his/her responsibilities regarding administration of the computer system as well as the security and integrity of the data and information stored and processed on the computer system.
- System Administrators is provided with the proper training, including training on security issues where required.
- System Administration takes place on secure workstations using secure IDs assigned to individual administrators as per the system administration rules.
- System Administrators are aware that operational shortcuts can lead to errors and reduce effectiveness of safeguards or even negate them.

**Security Breach Handling**

ActiveXchange, or a party designated by it, is responsible for and/or deal with:

- All incidents that affect, or could affect, information security.
- The monitoring of security breaches.
- Maintaining the IT Security Policy document.
- Communicating security breaches to all affected Data Owners.

**Data Protection**

Users and Data Owners who provide data, or input data on to ActiveXchange's online platforms, are responsible for ensuring that they comply with the requirements of the Data Privacy Act 1988.

ActiveXchange commits to complying with the Act at all times in how data is handled. This this end:

- open and transparent management of personal information (outlined in this Policy and our Data Use terms);
- anonymity and pseudonymity (ActiveXchange endeavour to anonymise as much information is possible);
- collection of solicited personal information (ActiveXchange works with Data Owners to ensure use of data is for a relevant and defined purpose);

- dealing with unsolicited personal information (ActiveXchange securely destroys records we do identify as unnecessary for the purpose of ActiveXchange services and also notifies the Data Owner if unnecessary or irrelevant data is transferred);
- notification of the collection of personal information (as the data processor, ActiveXchange supports the Data Owner to ensure the necessary terms around data collection are in place to align with the purpose of ActiveXchange services);
- use or disclosure of personal information (ActiveXchange uses information for its primary purpose as outlined in the Data Use Agreement);
- direct marketing (ActiveXchange does not undertake direct marketing unless part of the primary purpose of services and explicitly authroised by the Data Owner);
- cross-border disclosure of personal information (no personal information ever leaves Australia/ New Zealand);
- adoption, use or disclosure of government related identifiers
- Integrity of personal information (ActiveXchange has a set of tools and processes to review and continually support improve the integrity of data);
- security of personal information (ActiveXchange only holds data required for the fulfillment of the primary purpose as stipulated with the Data Owner. Removal of information from ActiveXchange systems is through and secure)
- access to personal information (ActiveXchange maintains systematic audit of records held to allow for ease of access and removal of any specific individuals data)
- correction of personal information (any updates to improve the integrity of data are proactively taken).

**Environmental Security**

- ActiveXchange's primary premises considered are data centres (see section below on suppliers), head office, employees working from home, and employees during travel. ActiveXchange puts in measures to ensure information assets can only be accessed by authorised users within each of these environments. This includes:
    - Entry controls to the office (and process for visitors). At least two barriers to the office. Each staff member has their own access card to monitor access. Any locally stored data is locked away if held on the premise. In addition, ActiveXchange implements the following procedures:
        - A restricted awareness of the location and function of secure areas;
        - Restrictions on the use of recording equipment within secure areas;
        - Restriction on unsupervised working within secure areas wherever possible;
        - In and out monitoring and logging.
    - In relation to equipment, ActiveXchange implements the following:
        - Information processing facilities (laptops, desktops etc) handling sensitive data should be positioned and the viewing angle restricted to reduce the risk of information being viewed by unauthorised persons during their use.
        - Storage facilities are secured to avoid unauthorised access with keys held by authorised key holders.
        - Food and drink should be kept away from ICT equipment.

        - Wireless routers, shared printers etc should be positioned to allow easy access when required and not distract anyone from working or have information left on the printer that should not be there.
        - Information processing facilities like laptops are sited so they are securely stored when not in use and easily accessed when required.
        - Home workers also need to carefully consider their siting and positioning of equipment to avoid risks similar to those addressed for workers in at the offices as well as unintentional use or access by family & friends.
- Where appropriate ActiveXchange also monitors the following, with a dedicated member of staff responsible for the related processes and checks:
    - Supporting utilities
    - Cabling security
    - Equipment maintenance
    - Removal of assets (a register of all assets are recorded against individuals and before any equipment is removed all access and information is password protected)
    - Secure disposal of equipment
    - Clear desk and screen policy

**Human resources security**

- ActiveXchange appreciates that staff are critical to high levels of information security. The following are therefore undertaken:
    - A background reference check is undertaken for all employees and contractors
    - Terms of employment (referencing this policy and other relevant legislation)
    - As part of the onboarding, those staff with access to sensitive data are fully trained and monitored by a line manager on a rolling basis.
    - A process for employment termination, ensuring all sensitive information is always protected.
- ActiveXchange has a disciplinary process to reinforce processes.

**Asset management**

- ActiveXchange implements the following best practice measures:
    - Inventory of assets, considering levels of risk and importance
    - Ownership of assets, ensuring a suitably qualified and experience member of staff has responsibility
    - Defining acceptable use of assets, ensuring this is documented
    - Return of assets, and any issues logged as incidents.

**Information classification and labelling**

- As part of ActiveXchange's asset/inventory management process the following classification is appended to data by the Data Owner, following a set of guidelines that are reviewed by the Executive Team:
    - Confidential (only senior management have access)
    - Restricted (most employees within the Data Team have monitored access)
    - Internal (all employees have access)
    - Public information (everyone has access).
- In addition ActiveXchange has a consistent approach to labelling data and files to track and manage edits and roles.

- Handling of assets is aligned with their classification and also relates to environmental security measures in place.

**Information systems acquisition, development and maintenance**

- ActiveXchange general only use global systems that have extensive security measures in place (see Appendix A)
- A risk assessment is undertake on each system before it is acquired to ensure it has adequate security controls
- When transferring data we ensure a suitable network and procedures are deployed. Data extract and transfer options are detailed in our **Data Transfer Guidance** document. Typically any data shared must be done through password protected files (and encrypted where required) and transferred over a dedicated FTP server or through dedicated and monitored APIs.
- Any applications development by ActiveXchange must follow a set of information security requirements and is subsequently tested at each stage of the development lifecycle.
- System change control procedures to avoid unnecessary vulnerabilities
- Secure testing environment is always used for any new developments
- ActiveXchange typically undertakes all development work internally. Any contractors used are supervised to ensure compliance
- System security and acceptance testing is completed

**Incident management**

- As a general principle, security incidents and events are reported through suitable management channels as soon as possible.
- Employees and contractors are aware of their obligations, covered as part of the training protocols. This may include ineffective security controls; assumed breaches of information integrity or confidentiality, or availability issues e.g. not being able to access a service.
- Weaknesses should be reported to then agree a suitable testing process
- Action take aims to minimise any compromise of the availability, integrity or confidentiality of information and prevent against further incidents.
- The following are undertaken and as a Company we commit to a continuous improvement process:
    - collecting evidence as soon as possible after the occurrence;
    - conducting an information security forensics analysis (grand term but at least being clear on root cause and related aspects or what happened and who was involved, why etc);
    - escalation, if required, for example to relevant regulators;
    - ensuring all that all involved response activities are properly logged for later analysis;
    - communicating the existence of the information security incident or any relevant details to the leadership for them to be further communicated to various individuals or organisations on a need-to-know basis; and
    - dealing with information security weaknesses found to cause or contribute to the incident.
- To ensure business continuity

**Business continuity management**

- We verify the established and implemented information security continuity controls at regular intervals in order to ensure that they are valid and effective during potential situations.
- We consider how information processing facilities are implemented with redundancy sufficiency to meet availability requirements. Redundancy refers to implementing, typically, duplicate hardware to ensure availability of information processing systems.
- Either ActiveXchange or our suppliers test redundancy regularly to ensure it is adequate.
- Redundant components of our systems (or those provided by suppliers) are to have the same levels of security.

**Policy Responsibility**

- Responsibility for compliance with the policy is delegated to the Director of ActiveXchange, who seeks advice and sign-off from our Cyber Security Advisor.
- Individuals are responsible for their own actions and usage of their assigned Personal Identifier, and are trained accordingly.
- Individuals are responsible for ensuring that they comply with all the requirements of the IT Security Policy.

All User queries and notifications relating to the contents of this document should be addressed to ActiveXchange Customer Support by email to info@ActiveXchange.org

**Responsibility for Review**

The ActiveXchange Board is responsible for the maintenance and annual review of this Policy, with roles delegated to the Executive team and Advisory Board as required.

## Appendix A

Data *security of* primary system suppliers

ActiveXchange ensures all systems it procures meet the standards of this Policy. ActiveXchange adapts its procedures where necessary to insure the integration and maintenance of the full technology stack is secure at all times. The primary systems are listed below.

ActiveXchange uses AWS to power v1.0 of the SportsEye product suite. From August 2021 all products will be built on the Microsoft stack. AWS provides the following data security.

*AWS CloudFront*

CloudFront offers the most advanced security capabilities, including field level encryption and HTTPS support, seamlessly integrated with AWS Shield, AWS Web Application Firewall and Route 53 to protect against multiple types of attacks including network and application layer DDoS attacks. These services co-reside at edge networking locations – globally scaled and connected via the AWS network backbone – providing a more secure, performant, and available experience for your users.

**Amazon Web Services (supplier used to power the front end application)**

*AWS Lambda and Lambda Edge functions*

These two services provide the following:

- DNS zone walking via Amazon Route 53 Hosted Zones
- Denial of Service (DoS), Distributed Denial of Service (DDoS), Simulated DoS, Simulated DDoS (These are subject to the DDoS Simulation Testing policy)
- Port flooding
- Protocol flooding
- Request flooding (login request flooding, API request flooding)

**Microsoft (Azure back end database)**

ActiveXchange uses Australian based cloud servers powered by Microsoft (Azure) for data processing. Full details on security procedures and certification can be found at: https://www.microsoft.com/en-us/trustcenter/security/azure-security and https://docs.microsoft.com/en-us/azure/security/azure-security

**Google (general internal file management)**

ActiveXchange also uses Australian based cloud servers provided by Google Cloud (the "Provider") for temporary storage of data models and outputs. All of Provider's data centres have been certified by national and/or international security standards.

The security guidelines below are taken from the Security Policy of the Provider and can also be found at https://cloud.google.com/security/compliance/

## Appendix B: ActiveXchange – IT Risk Assessment - January 2021

This following two tables covers the types of information received by ActiveXchange, and how this is then classified and handled.

| Categrory | Processess | Risks | Risk Rating | Likelihood | Operational Procedures |
|---|---|---|---|---|---|
| Transfer | Sensitive Information (PII data) sent by mail | Data leak | Medium | Highly likely | Having a Data Owner who keeps track of flow of data (Having the responsibility of storing data at a central location and making sure that everyone deletes PII information after use) |
| Transfer | Sensitive Information (PII data) sent by google drive | Data leak | Low | Highly likely | Having a Data Owner who keeps track of flow of data |
| Transfer | Sensitive Information (PII data) being downloaded into local system | Data leak | High | Highly likely | Having a Data Owner who keeps track of flow of data |
| Storage | Local system | Data leak | High | Highly likely | Deleting PII as soon as it is downloaded to the system |
| Storage | Microsoft Azure database | Data leak | low/none | low probability | Access control system in place (4 users added and access monitored) |
| Storage | sFTP | Data leak | low/none | low probability | Access control system in place (3 users to be added) |
| Technology (operations) | Unauthorized Access | AX core service disrupted/ Data leak/Data privacy issues | High | Low | All users would be asked to reset their passwords |
| Technology (operations) | Security of the site (attack on the site) | AX core service disrupted/Data privacy issues | High | Low | All users would be asked to reset their passwords<br>Contact the host server |
| Technology (operations) | De-activation of users/remove user previliges | Data leak/Data privacy | High | Low | User removed within 6 hours of notifying ActiveXchange |

This document is part of the data protection risk assessment toolkit. It should be used along with the data protection risk assessment table.

| No | Question | Actions |
|---|---|---|
| ***How risky is your information?*** | | |
| 1. | What information about people does your area have? Examples include personal information, attendance data and facility performance data | List types of data in the data protection risk self-assessment table<br><br>Does your area have any information that is unnecessary or disproportionate to the task?<br>**If yes**, stop collecting and using this. Dispose of the information that you already hold. |
| 2. | Are these different types of information high, medium or low risk? | Classify your area's information into these three risk categories.<br><br>You must implement stricter measures and take greater care when dealing with high and medium risk information. |
| 3. | Do affected individuals/ companies know:<br><br>• What information you hold about them?<br>• What you do with that information?<br>• Whether you disclose the information to other organisations? | If you use information about people/ companies for purposes they would not expect (for example marketing), you must tell them about these uses.<br>Write a statement explaining what you do with the information you hold about people/ companies, and ensure they see it.<br><br>Have a procedure in place for responding quickly and appropriately if anyone objects to you using information about them. |
| ***What do you do with this information?*** | | |
| 4. | Where and in what formats do you keep personal data? Examples include paper files, databases, electronic files, laptops and portable devices. | Add these details to the data protection risk assessment table |
| 5. | How do you store the information? | Add these details to the data protection risk assessment table.<br>For each, ensure that the security measures you have in place are appropriate to the format and risk category. For example, password-protect spreadsheets containing personal or commercially sensitive details. Ensure any cloud/ database storage solutions have suitable security standards. |

| | | |
|---|---|---|
| 6. | Do you use an IT system or application to process information about people? | **If yes:**<br>• See AX IT Security Policy (and code of practice) |
| 7. | Do staff ever work away from the office?<br>Do staff use smartphones or laptops for work? | **If yes**, you can limit the need to take information home by using remote access facilities.<br>All staff (including mobile workers) must follow the policy on the storage, transmission and use of personal data and sensitive business information.<br>Office-based staff who occasionally work at home should follow the guidance on working at home |
| 8. | Do staff in your area know when to dispose of information?<br>Does this happen in practice? | Each area of the organisation is responsible for looking after and disposing of the information it holds.<br>Develop a records retention schedule, which sets out when and how to dispose of different types of information, and ensure it is implemented. |
| 9. | How do staff dispose of paper information? | Low risk information can be disposed of through normal waste procedures, for example, using recycling facilities.<br>**High and medium risk** information must be disposed of using confidential waste facilities. |
| 10. | How do staff dispose of electronic records or computing equipment? | Delete information held on servers or shared drives as part of your everyday computer use – ultimate deletion is the responsibility of your local IT support/ database provider.<br><br>You must either ensure that any **high or medium risk** information stored on hard drives or other portable devices is no longer available when you dispose of the computing equipment or ask your local IT support to do so. This can involve wiping the hard drive or destroying the computer or device completely. |
| ***Who can access and update this information?*** | | |
| 11. | Is it clear which members of staff are responsible for accessing and updating information? | Establish procedures which set out these responsibilities, and limit access and amendment privileges. For each information type, limit these privileges to |

| | | |
|---|---|---|
| | | staff that need the information to do their jobs. |
| 12. | Are people with access to sensitive business data or personal information aware of their responsibilities towards it? | Staff, temporary workers, volunteers or other parties with access should agree a user statement or confidentiality agreement which sets out these responsibilities. This is built into all employee contracts and all staff are regularly briefed. |
| 14. | Do you outsource any services where personal data is transferred to a third-party supplier?<br>Examples include outsourcing database cleansing or using a mailing house to send out publications. | **If yes,** you must have a written agreement that protects the personal data. |
| 15. | Do you share information about people/ companies with other organisation, either on a regular or one- off basis? | **If yes,** AX will always require in place a written agreement from the Data Owner. |
| 16. | What training or advice is available for staff with access to information about people? | Ensure staff know what they should and should not do when working with information about people. Incorporate this into your training, for example, during your staff induction program. |