ISMS Scope

Change Control

Version	Created by	Owned by	Change date	Changes/Comments	Approved by
1.0	Stephen Houston	COO	29/01/2024	Initial version	CEO
1.1	Stephen Houston	COO	27/02/2024	Reviewed by Management	CEO
1.2	Mark Kerr	COO	06/04/2025	Annual Review	CEO
2	Mark Kerr	COO	01/09/2025	27018 Update	CEO
2.1	Mark Kerr	CIO	05/03/2026	Annual Review	CEO

Table of Contents

Purpose, Scope and Users

The purpose of this document is to define rules for access to various systems, equipment, facilities and information, based on business and security requirements for access.

This document is applied to the entire Information Security Management System (ISMS) scope, i.e. to all systems, equipment, facilities and information used within the ISMS scope.

Users of this document are all employees of Concept Apps Ltd (trading as TeamFeePay).

Definition of ISMS Scope

Taking into account the legal, regulatory, contractual and other requirements, the ISMS scope is defined as specified in the following items:

Provision & Support of sports club management software and club development needs

Organisational Unit

The organisational units which are included in the scope are as follows:

1. Product
2. Sales & Marketing
3. Service
4. Operations

Locations

Concept Apps Limited Belfast office is included within the scope of this system.

Catalyst Innovation Centre

Queens Road

Belfast

BT3 9DT

Networks and IT Infrastructure

The networks and related IT Infrastructure are included in the scope.

- Heroku Infrastructure
- Microsoft 365
- Devices owned by Concept Apps Limited.

Interested Parties

Concept Apps Limited has taken into account the needs and expectations of interested parties. It is foreseen that future clients will potentially begin to require formal information security certification.

Listed below are examples of interested parties that Concept Apps Limited have reviewed when creating the information security management system:

Interested parties	**Requirements of interested parties in relation to Information security**	**How ISMS fulfils these obligations**
Information Commissioner's Office	Ensuring the security and validity of personal data. Requirement to adhere to UK Data Protection Act. **Registration number: ZB502456**	Communications Policy
Gambling Commission	Adhere to testing and standards laid out under the UK Gambling Act, inform of any breaches to those acts	Communications Policy
Business partners and suppliers	Securing connections to personal data, and security of personal data.	Incident Management Policy Confidentiality Agreements T&Cs Supplier Security
Clients & End Users	Security testing to take place if deemed required from specified clients. All clients' security requirements will be considered and met where possible. Securing connections to personal data, and security of personal data. Retain continuation of service and data security. Security compliance includes but is not limited to: Secure systems development. Evidence of implementation of security measures. Evidence of pen tests performed. Demonstrated compliance e.g. ISO27001.	Incident Management Policy Confidentiality Agreements T&Cs

Internal Staff	Ensuring all businesses operations meet security measures, assuring the protection of client and transaction data. Protection of personal data. Policies processes and procedures that are clear. Job Security.	All Policies Contracts Awareness Training
Neighbours	Ensure Concept Apps Limited does not disrupt neighbouring businesses operations.	Physical and Environmental
Landlord	Rent paid on time and premises kept tidy and damage free.	Physical and Environmental
Board of Directors, Investors & Shareholders	Sustainable business, business continuity, maximise value. Compliance with regulatory, legal, contractual and customer needs and requirements.	All ISMS policies

All of the above listed parties have expectations that reasonable steps will be taken to secure the information gathered as part of the regular operation of all Concept Apps Limited designed solutions, and that the organisation's reputation and financial stability will not be jeopardised due to poor security practices.

Leadership

The scope and associated documents have been approved by the senior leadership team as per February 2024.

Roles and Responsibilities

Management Team

The Management team responsible for the suitability, adequacy and effectiveness of the ISMS:

- CEO – Liam McStravick
- COO – Victoria Miller
- CSO – Manus Magill
- Director of Club Development – Robert Crowe
- CIO (ISO) – Mark Kerr
- CTO (ISO Co-ordinator) – Stephen Houston
- External Consultant – Tom Shields

The responsibilities of the management team are to:

- Establish the ISMS policy, objectives and plans.
- Communicate the importance of meeting the information security objectives and the need for continual improvement.
- Determine and provide resources to plan, implement, monitor, review and improve information security and management e.g. recruit appropriate staff, manage staff turnover.
- Manage risks to the organization.
- Conduct reviews of information security, at planned intervals, to ensure continuing suitability, adequacy and effectiveness.
- Establish a continual improvement policy with respect to information security for the organization.
- Ensure that arrangements that involve external organisations having access to information systems and services are based on a formal agreement that defines all necessary security requirements.
- Issue and approve final policy documents.
- Ensure that all staff are aware of policies and IT Security requirements.

Information Security Officer – Mark Kerr

The Information Security Officer is responsible for ensuring the ISMS conforms to the requirements of ISO 27001 and for reporting on the performance of the ISMS to the Concept Apps Limited management team.

Reporting to the Management Team on all security related matters on a regular basis.

Communicate the information security policy to all relevant personnel and customers where appropriate.

Implement the requirements of the information security policy.

Manage risks associated with access to the service or systems.

Ensure that security controls are documented.

Quantify and monitor the types, volumes and impacts of security incidents and malfunctions.

Establish and maintain a continual improvement action list and report on improvement activities.

Ensure that procedures are in place to define the recording, prioritisation, business impact, classification, updating, escalation, resolution and formal closure of all security incidents.

Ensure that all staff involved in incident management shall have access to relevant information such as known errors, problem resolutions and the configuration management database.

Manage and classify major incidents according to a process.

Arrange and attend service review meetings on a regular basis.

PII in the cloud

To ensure effective communication and accountability in the processing of Personally Identifiable Information (PII) within public cloud environments, the Concept Apps Limited have designated a specific point of contact.

The ISO is the primary liaison for the cloud service customer, responsible for:

- Addressing inquiries.
- Facilitating requests, and
- managing communications related to the processing of PII under the contractual agreement.

The contact details of the designated representative shall be documented and made readily available to the customer throughout the duration of the contract.

Information Asset Owners

Responsible for specific, named information assets.

Maintain and review security controls for allocated asset(s).

Participate in risk assessments concerning their asset(s).

Ensure the relevant entry in the asset inventory is kept up to date.

Employees and Contractors

All employees, including contractors of Concept Apps Limited are trained in their information security responsibilities and are held accountable.

Auditor(s)

Responsible for assessing and evaluating the ISMS.

Contact with Special Interest Groups & Authorities

Contact shall be maintained inline with interested parties listed above, for instance, subscription to ICO mailouts to list changes in data protection legislation and also working with organisations such as the Gambling Commission for regulated activities Invest NI, Small Business Federation.

Assessing Competency

At least one member of the Information Security Management Committee should be certified in ISO27001 Lead Implementer or Auditor.

Our staff should be listed on the Competency Matrix, which will be completed as part of their probation by the Head of People. There will be an annual update to this document.

Resources

Senior leadership are committed to providing all necessary resources that are essential to the implementation and control of the Management System and Concept Apps Limited's aim of controlling risk and meeting customer requirements. Resources shall include human resources and specialised skills, technology and financial resources. In particular, consideration will be given to resource requirements in relation to:

- People
- Infrastructure (Technology)
- Environment
- Monitoring and measurement – Information security objectives
- Organisational knowledge

Internal & External Issues

Factor	External Context	Internal Context
Political	Ongoing geopolitical instability (e.g. Middle East conflict impacting global energy supply chains) is contributing to inflation, economic uncertainty, and potential disruption to global service providers relied upon by TFP.	TFP must maintain agility in responding to changing government policies, funding environments, and regulatory expectations impacting sports organisations and payment processing services.
Economic	Sustained cost of living pressures and inflation are reducing disposable income, potentially lowering club membership uptake and transaction volumes processed through the TFP platform.	Increasing operational costs (e.g. payment provider fees, cloud infrastructure, and skilled workforce costs in Northern Ireland) require ongoing pricing, supplier management, and efficiency optimisation.
Sociocultural	Customers (clubs and members) have increasing expectations around secure, seamless digital payments and transparency in how personal data is handled.	Hybrid working practices and competition for skilled technical and support staff impact workforce stability, knowledge retention, and the ability to scale securely.
Technological	The cyber threat landscape continues to evolve, with increased risk of phishing, ransomware, and credential-based attacks targeting SaaS platforms and payment systems.	TFP's reliance on its core technology stack (e.g. Ruby on Rails, AWS infrastructure) requires continuous patching, monitoring, and resilience planning to ensure availability, security, and scalability.
Legal	Compliance with UK GDPR and evolving data protection laws requires TFP, as a Data Processor, to maintain appropriate safeguards and support Data Controllers (clubs) in meeting their obligations.	TFP must ensure adherence to contractual, regulatory, and internal governance requirements (e.g. Data Processing Agreements, ISMS policies), including effective incident management and audit readiness.
Environmental	Increasing societal and regulatory focus on sustainability is encouraging reduced reliance on paper-based processes and supporting the adoption of digital payment platforms such as TFP.	TFP minimises environmental impact through cloud-based infrastructure, remote working practices, and responsible handling and disposal of IT equipment (e-waste).

Improvement

The organisation is committed to the concept of continual improvement through use of the stated policies, objectives and targets, audit results, analysis of data, corrective and preventive actions and management reviews.

The organisation has established and maintains documented procedures to ensure that nonconformity is identified, and corrective actions are introduced to eliminate and reduce nonconformities and improve the effectiveness and suitability of the ISMS.