Information Security Policy

Change Control

Version	Created by	Owned by	Change date	Changes/Comments	Approved by
1.0	Stephen Houston	CTO	08/04/2022	Initial	CEO
1.1	Stephen Houston	CTO	04/12/2023	Reviewed by management	CEO
1.2	Stephen Houston	CTO	27/02/2024	Reviewed by management	CEO
1.3	Tom Shields	CTO	19/03/2024	Added SMART for objectives	CEO
1.4	Mark Kerr	CIO	06/04/2025	Annual Review	CEO
1.5	Mark Kerr	CIO	05/03/2026	Annual Review	CEO

Table of Contents

Purpose

This document outlines our approach to information security, including how we manage customer data.

Audience

Everyone within Concept Apps Ltd (trading as TeamFeePay) must be aware of and comply with this policy.

Objectives

- Ensure that each element of data is only accessible by those individuals who need it for their job function
- Ensure that the data is secured, and that any risk to that security is identified and agreed within our risk appetite
- Define how we back up the data and ensure operational stability

Objective 1: Data Access Control

Specific	Ensure that each element of data is only accessible by relevant individuals based on their job function.
Measurable	Implement role-based access controls (RBAC) to restrict data access.
Achievable	Collaborate with IT and department heads to define access levels and permissions.
Relevant	Enhance data security and privacy by limiting access to authorized personnel.
Time-bound	Complete RBAC implementation by the end of Q2 2024.

Objective 2: Data Security and Risk Management

Specific	Ensure data security and identify risks within our risk appetite.
Measurable	Conduct regular security assessments and risk assessments.
Achievable	Collaborate with the cybersecurity team to assess vulnerabilities and establish risk thresholds.
Relevant	Mitigate security threats and align risk management with organizational goals.
Time-bound	Conduct the next security assessment by the end of Q3 2024.

Objective 3: Data Backup and Operational Stability

Specific	Define data backup procedures and ensure operational stability.
Measurable	Establish automated backup schedules and test data restoration processes.
Achievable	Work with IT and operations teams to implement backup solutions.
Relevant	Minimize data loss and maintain business continuity.
Time-bound	Complete data backup setup and testing by the end of Q1 2024.

Data classifications

We divide our data up into 4 main categories. Regardless of classification, all data is encrypted at rest and in transit.

- User/Member supplied data files, this has the highest level of classification as it is typically used to convey sensitive information (such as birth certificates) from the User to a Club or Governing Body. Access to these files is heavily restricted, logged, and only available through time limited (expiring) links.
- User/Member operational data, this defines a user (member) on the system, and contains personal information, and information about their payment history. Access is restricted to only those individual who need the information for their job roles.

Authorisation and access control policy

- Data is only accessible by those individuals who need it to perform their job function
- Data access controls are applied by the application, both when displaying the data, and when exporting it to other systems
- Export functionality is permissioned and any use of it is logged
- All activity inside the application is logged and recorded
- Each user has individual logins for each system that we use, those logins are not shared between individuals
- Multi-factor authentication is used wherever it is available through the services that we use

Data support and operations

- All data is encrypted at rest, and also in transit
- All backups are encrypted
- Data is held within the EU for EU members
- We follow the principles outlined in the UK Data Protection Act 2018 (GDPR)

Security awareness and behaviour

- Staff are made aware of our Information Security Policy when they join the company, and during our annual Security Training
- Further IT security training is provided by our Insurance Company as part of our Cyber Insurance Policy
- Each full-time member of staff has a company supplied computer which they use for company business, this enforces our IT security policies via Microsoft InTune ensuring the device remains in compliance with those policies
    - Should a user try to use a different device, then the policies will be applied there or failing that, the user will only have access to a limited set of functionality on that device

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.
This policy is reviewed annually by the CTO