PCI Compliance Policy - FlowAlp SAGL

Effective Date: 09 June 2026

Review Date: 09 June 2027

Approved By: Aramis Grata, CEO

Purpose and Scope

This policy defines how FlowAlp SAGL ("FlowAlp") manages its responsibilities under the Payment Card Industry Data Security Standard (PCI DSS) for payment-related services, including FlowAlp Pay and related event ticketing or checkout flows. FlowAlp relies on external PCI DSS compliant payment service providers and acquiring/payment infrastructure to process card transactions. FlowAlp does not store, process, or transmit cardholder data (CHD) on its own systems. Cardholder data is entered directly into and handled by PCI-certified payment systems, and FlowAlp systems must not capture, log, or retain CHD.

Principles

• All card transactions are processed exclusively through PCI DSS compliant payment providers and hosted or secure payment components used by FlowAlp Pay.

• FlowAlp does not store, process, or transmit cardholder data (CHD) or sensitive authentication data (SAD) on its own systems.

• FlowAlp systems, applications, logs, databases, backups, analytics tools, and support channels must not contain full card numbers, CVV/CVC, magnetic stripe data, PIN blocks, or other sensitive authentication data.

• Relevant employees and contractors with access to payment-related systems receive annual PCI security awareness training.

• Any suspected exposure of CHD must be escalated immediately to the PCI Compliance Owner and Management.

• PCI DSS responsibilities, provider attestations, and the applicable self-assessment process are reviewed and documented at least annually.

Responsibilities

Role	Responsibility
PCI Compliance Owner	Coordinates PCI activities, maintains this policy, verifies annual self-assessments or questionnaires, collects provider PCI evidence, and documents compliance.

IT / Technical Team	Ensures FlowAlp systems do not store, process, transmit, log, or cache CHD/SAD; integrates only approved PCI-compliant payment components; and reviews payment-related technical changes.
Product / Operations Team	Ensures operational processes for FlowAlp Pay, FlowAlp Ticket, and related checkout flows follow this policy; escalates anomalies or suspected card data exposure.
Management	Approves this policy, assigns responsibilities, and provides the necessary resources.
All personnel	Understand and follow this policy; never request, store, or share cardholder data through email, chat, support tickets, documents, or other FlowAlp systems.

Review and Communication

This policy is reviewed at least annually and whenever significant technological or business changes occur, including changes to payment providers, checkout architecture, sales channels, or incident response requirements. It is made available to FlowAlp employees and contractors and may be shared with payment partners, acquirers, auditors, or customers where appropriate.

Training and Review

All relevant employees and contractors receive annual PCI security awareness training or confirm their awareness of this policy. Training covers the prohibition on handling CHD, secure use of payment systems, incident escalation, phishing and social engineering risks, and correct handling of payment-related support requests.