STIPEND PLATFORM

Compliance Pack

How learner stipend disbursements, card data, and personal information are protected on the Stipend platform — with references to the standards and South African legislation we align to.

Version 1.0 · 2026-05-03

PCI-DSS	POPIA	FICA	ISO 27001
Level 1 issuer	Act 4 of 2013	FIC Act 38 of 2001	Issuer & cloud platform

At a glance

Stipend never stores raw card numbers or CVVs. Card details are tokenised by our PCI-DSS Level 1 issuer and revealed inside an isolated iframe our application cannot read. Identity data collected for FICA is encrypted at rest, accessed via row-level security policies, and minimised on every screen. Maker–checker is enforced in code on every disbursement run and every administrative action is written to an append-only audit log.

Controls mapped to standards

Control area	Implementation	Standard / source
Card data isolation	PAN/CVV never touch our servers. Reveal renders inside the issuer's PCI-scoped iframe; signed reveal tickets expire in 60 seconds.	PCI-DSS v4.0.1
Tokenisation & key management	Issuer-managed BIN; tokens stored, never raw PAN. Application secrets segregated per environment.	PCI-DSS Req. 3 & 8
Identity & PII protection	ID numbers encrypted at rest, RLS policies, data-minimised admin views, deletion on request.	POPIA (Act 4 of 2013)
KYC / AML	Per-learner KYC before card issue. Sanctions/PEP screening before disbursement; failures freeze the run.	FIC Act 38 of 2001
Maker–checker authorisation	Dual approval enforced in code on every stipend run; cryptographic signatures preserved.	ISO/IEC 27001 A.5.15 / A.8.2
Audit logging	Append-only audit log of approvals, freezes, top-ups and reveals; exportable on demand.	NIST SP 800-92

Control area	Implementation	Standard / source
Access control	Role-based access (admin, facilitator, learner). Server-side validated via Postgres roles + RLS.	ISO/IEC 27001 A.5.18
Attendance integrity	Time-rotating QR with site check-in for in-person sessions; tamper-evident attendance records.	Internal control · supports POPIA accuracy principle

Source documentation

Each section below links to the authoritative source for the standard or legislation referenced.

PCI-DSS — Payment Card Industry Data Security Standard

Stipend's card surface is built so that primary account numbers, CVV2 and expiry data never enter our servers, browsers or logs. Reveal happens inside the issuer's PCI-scoped iframe, gated by short-lived signed tickets. This dramatically reduces our PCI scope (SAQ-A class) while still letting learners view and use their cards.

- PCI Security Standards Council — document library
- PCI SSC — e-commerce guidance (iframes / hosted fields)

POPIA — Protection of Personal Information Act, 4 of 2013

Personal information collected for KYC and stipend administration is processed lawfully under conditions 1–8 of POPIA. ID numbers and contact details are encrypted at rest, surfaced only to roles with a defined operational need, and never displayed where they are not required. Learners can request access, correction or deletion via the platform.

- POPIA — full text (Act 4 of 2013)
- Information Regulator (South Africa)

FICA — Financial Intelligence Centre Act, 38 of 2001

Each learner is KYC-verified before a card is issued. Sanctions and politically-exposed-person screening run before each disbursement; failed screening freezes the run, not just the affected row, until reviewed. Suspicious transaction monitoring is supported by the audit log.

- FIC Act — AML/CFT obligations
- Financial Intelligence Centre

ISO/IEC 27001 — Information security management

Our infrastructure providers (cloud platform and card issuer) operate under ISO/IEC 27001:2022 certified information security management systems. Stipend's own controls — access management, change control, secure SDLC, audit logging — are designed against the same control catalogue.

- ISO/IEC 27001:2022
- NIST SP 800-92 — log management guide

Audit, integrity & money movement

Stipend runs follow a maker–checker pattern enforced in code: the user who prepares a run cannot approve it. Approvals, freezes, top-ups, card reveals and configuration changes are written to an append-only audit log with actor, timestamp and entity reference. Auditor-ready exports can be produced for any cohort or period.

- South African Reserve Bank — National Payment System
- BCBS 239 — risk data aggregation principles

Disclaimer: this document summarises the platform's control posture and references applicable standards. It is not legal advice and does not constitute formal certification. Certifications held by upstream providers (issuer, cloud platform) are maintained by those providers.