

Security and data overview

How asasii acceptance handles identity, access, audit, card data, personal data, retention, merchant due diligence and continuity.

Identity and access

Single sign-on	With the institution's own identity provider
Multi-factor authentication	Enforced by the identity provider for the institution's users, and on for merchant users
Roles	Segregation of duties: approving merchants, fees and settlement sit in separate roles
Settlement approval	Two people; no one can prepare a run and give its second approval
Merchant users	Roles per person, so a counter can send a link without seeing settlement
Break-glass accounts	Local accounts, held sealed

idataraya access

Support sessions	Opened from a support case, time-boxed and approved by the institution's named owner
Record	Every action in a session is in the institution's audit log
Revocation	The institution can revoke access at any time

Audit

What is recorded	Every action, with the value before and after, the user and the origin
Integrity	The log cannot be edited or deleted
Retention	Seven years
Export	Exportable from the console

Where the data lives

Environment	The institution's own environment, its data centre or its cloud account
Ownership	The institution owns the software, the customisations, the data and the audit log

Domains	The institution's own checkout and portal domains, certificate and email sender
----------------	---

Card data

Handling	Card data goes to the acquirer's processor, never to the store or the platform
On the platform	The processor's tokens and references only
Embedded checkout	Card fields are the processor's, rendered inside the SDK, so the merchant's app never handles a card number and the merchant stays at PCI SAQ-A
Customer authentication	3-D Secure, shown as a confirmation in the customer's own bank app

Personal data and retention

Law	Personal Data Protection Act 2010
Retention	Per data class, confirmed by the institution's IT against its PDPA register and backup policy
Default classes	Transactions and the audit log seven years, request logs ninety days, webhook payloads thirty days, card data never
Customer contact	Two years after the last payment
Card tokens	Until the merchant closes

API and webhooks

Keys	Scoped to what they need, rotated on a schedule with an overlap, restricted by origin and IP, and rate limited
Late rotation	The institution is told when a key has not rotated by its date
Webhooks	Signed with HMAC SHA-256, with a versioned schema
Idempotency	A key on every POST, checked before go-live and shown in the request log

Merchant due diligence

Documents	SSM registration, TIN, the directors' identity and settlement account proof, each held with an expiry date
Settlement account	A penny test recorded before activation
Screening	Sanctions and PEP, SSM status and adverse media, at onboarding and monthly

Continuity

Routing fallbacks	A fallback processor after timeouts, and a notice with DuitNow QR offered when an FPX bank is slow
Webhooks	Retried with backoff for 72 hours, and replayable
Monitoring	From inside the institution's environment
Response	Times by severity, measured against the agreement

asasii acceptance is a product of idataraya Sdn Bhd (1263428-K), Kuala Lumpur. Deployed in the client's own environment, customised and maintained by idataraya. info@idataraya.com · acceptance.asasii.com