

Security and data overview

How asasii pos handles identity, audit, personal data, card data, devices and continuity.

Identity and access

Single sign-on	With the retailer's own identity provider
Multi-factor authentication	Required on every console
At the till	An employee ID and PIN on the terminal registered to the outlet; no shared logins

Audit

What is recorded	Every action, with the previous value
Retention	Seven years
At the counter	Discounts, holds, returns and voids each carry a reason on record

Where the data lives

Environment	The retailer's own cloud account or data centre
Ownership	The retailer owns the data; the retailer's team holds the keys, the backups and the data
Operation	idataraya installs the platform, hardens it and keeps it current

Personal data

Customer and staff data	Stay in the retailer's own environment, under the Personal Data Protection Act 2010
Export	Every record exports on request

Card data

Handling	Taken by the acquirer's card reader and gateway; it never touches the terminal or the platform
On the terminal	Tokens and settlement references only

Devices

Dedicated devices	Terminals are provisioned so only the asatii pos app runs
Registration	Each terminal is registered to its outlet with a store, outlet and terminal code
Lost terminal	Revoked from the fleet console

Continuity

At the counter	Terminals keep selling through a network drop and sync when the line returns
Backup	A drilled backup and restore

Monitoring and response

Monitoring	Continuous, from within the retailer's environment
Response	Severity-based response times, measured monthly

Integration

API	Documented, for sales, receipts, stock and takings
------------	--

asatii pos 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 · pos.asatii.com