

Security and data overview

How asasii emd keeps data in Malaysia, keeps agencies apart, ties access to posts, audits every view of a location, protects evidence, and handles training data and retention.

Where the data lives

Location	In Malaysia: the agency's own data centre or a Malaysian government cloud
Device data	Sent by the devices to the platform's own gateway; no device maker's cloud or portal holds it
Maps	Self-hosted map tiles; no position is sent to an outside map service
Ownership	The data is the agency's; its team holds the keys, the backups and the data

Agencies kept apart

Scope	Each agency sees only its own people, cases, devices and staff
Across agencies	Only a police response request crosses, carrying only what the responder needs: who, where, the alarm and a photo
Platform admin	idataraya's platform admin is the only role across agencies, and every action it takes is audited

Posts and roles

Posts	Permissions belong to posts, not people; a replacement takes over a post with a handover
Roles	Operator, shift supervisor, case officer, enrolment officer, field responder, court registrar, agency admin, director and platform admin
Approvals	Rule changes and escalations approved by a supervisor
Two-person rule	Removing a device before the order ends needs a second person

Audit

Location views	Every view of a person's location written to the audit trail
Exports	Every export and every evidence download written to the audit trail
Alarm handling	Every step on an alarm timestamped with who took it

Changes	Every change to a case, an order's rules or a device, with who, when and what
----------------	---

Evidence integrity

Documents	Signed by the issuing officer
Hash	A hash of the document's contents stored with it
Verification code	Printed on the document, so a court can check a printout has not been altered

Personal data

What is held	Photo, MyKad or passport number, address, next of kin, the order, positions and alarms
PDPA	Handled under the agency's own obligations and the Personal Data Protection Act 2010 where it applies
Retention	Kept for the retention period each agency sets, then purged
Training	Training mode keeps its own data apart from live cases and deletes it after seven days
Samples	Names, IC numbers and phone numbers in demonstrations are fictional

Devices

Tamper	Strap cut, strap opened, lock released and power bank removed each raise an alarm
Power	The wearer cannot turn a bracelet off; it turns on by itself after charging
Without signal	Positions and alarms stored on the device and sent when the network returns
Firmware	Rolled out over the air in stages by the platform admin

Continuity

Control room	Built for a control room that runs around the clock, with shift handover on the record
Backups	A drilled backup and restore
Updates	Applied by idataraya under the yearly agreement

asasii emd 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 · emd.asasii.com