

Product brochure

Electronic monitoring for the prison department, the courts and the police department, owned outright.

A 24-hour control room, curfew and zone rules checked every minute, tamper alarms, two-way call through the tag, case management and evidence a court can verify. The data stays in Malaysia, and the maps run inside the platform.

Watched around the clock	One alarm queue and one live map in a 24-hour control room.
Alarms the moment it happens	A cut strap, a breach of curfew or a zone entered.
Evidence a court can check	Signed, with a verification code on every document.
Kept in Malaysia	In the agency's own data centre or a Malaysian government cloud.

What it does

The control room

Operators watch one alarm queue and one live map, around the clock. Every alarm arrives with the person, the order and the last known position, and every step taken on it is timestamped.

The alarm queue	Every open alarm in one grid, Critical first, with the person, the agency, the alarm, its age against the response target and the operator handling it. An alarm past its target moves up and is shown to the shift supervisor. Critical, High, Medium and Low, each with its own response target. Assigned and reassigned by the shift supervisor. Filters by agency, control room, alarm type and status.
The live map wall	Every person on monitoring on a live map, with their zones drawn round them and alarms marked where they happened. A dark large-screen theme is built for the wall of a control room that never switches off. The map is served from inside the platform, so no position goes to an outside map service. History played back on the same map. Several people followed side by side on one screen.
The person record, one click away	From any alarm, the operator opens the person: photo, order, curfew hours, zones, devices and their battery, the case officer, and every alarm and contact on the case. Each view of a person's location is written to the audit trail.
Shift handover	At the end of a shift the supervisor hands over the open alarms, the escalations waiting on a case officer and the police responses still out, and the next supervisor accepts them. Nothing is left in a notebook or a chat.

Alarms and response

An alarm comes from the device or is worked out by the platform from the rules in the order. Either way the operator follows the agency's playbook for it, and every step is timestamped.

Alarms from the device	The strap cut or opened, the lock released, the power bank removed, the battery low or critical, the device offline, GPS lost, the SOS button pressed, and the device turned back on after charging. A strap with steel and optical fibre raises the alarm the moment it is cut. A tag that cannot be switched off by the wearer. Positions and alarms stored on the tag without signal and sent when it returns.
Alarms the platform works out	A curfew breach, an exclusion zone entered, an inclusion zone left, a zone schedule broken, a device not charged by the reminder time, no movement for too long, and a position that jumps further than a person could travel.
A playbook per alarm, per agency	Each alarm has a severity, a response target and a playbook of steps set by the agency. The operator acknowledges, checks the map and the history, and works the steps in order, so a night shift handles a strap alarm the same way the day shift does. Resolve with a reason. Escalate to the case officer. Request a police response.
Two-way call and SOS	The operator calls the wearer through the tag itself, so the first question is asked in seconds, not after a home visit. A wearer who presses SOS is put through to the numbers the agency sets, up to three per device.
Police response and the field app	A response request goes to a field responder's app with only what the responder needs: who, where, the alarm and a photo. The responder navigates there, records the outcome with photos on scene, and the operator sees it on the alarm. The only thing that crosses from one agency to another. Accepted, on the way, on scene and closed, each timestamped.

Curfew and zone rules

The order sets the home address, the curfew hours, the places a person must keep away from and the area they must stay in. Those conditions become rules the platform checks every minute.

Curfew at home, from three signals	During curfew hours the platform checks that the person is at home from the home beacon, the home Wi-Fi and the position together. A single weak GPS fix indoors does not raise a breach, and leaving home does. A home beacon with a range of up to 60 m, on the wall or the floor. The home Wi-Fi registered on the device. Curfew hours by day of the week.
Exclusion zones	Places a person must keep away from, such as a victim's home, a workplace or a school, drawn on the map with a buffer. Entering one raises an alarm at once, with the position and the time.
Inclusion zones and schedules	The area a person must stay in, such as a district, a workplace during working hours or a route to a reporting office. A zone can have its own schedule, so a workplace counts only on working days.

A zones library per agency	Courts, offices, schools and other places an agency uses often are kept in its own library, ready to add to an order without drawing them again.
Rule changes within the order	A case officer requests a change within what the order allows, such as a later curfew for a night shift at work, and a supervisor approves it. The change, who asked and who approved are on the case.

Case management

Each case officer owns a caseload. The case holds the person, the order, the devices, every alarm and every contact, so the officer reads compliance from the record rather than from a phone call to the control room.

The caseload	Every person on the officer's caseload in one grid: the order, its end date, compliance this week, open alarms, the last contact and the next report date. Cases needing attention sort to the top.
The person and the order	The person's photo, MyKad or passport number, address and next of kin, and the order that placed them on monitoring, with its conditions, its end date and the agency that issued it. Sample wording on screens until each agency confirms its own.
Compliance at a glance	Curfew kept, zones respected, the device charged and worn, by day and by week. A breach links to the alarm and to how the control room handled it.
The contact log	Every visit, call and report made by the person, recorded by the case officer on the case, beside the letters and SMS sent to the person.
Access by post, not by person	Permissions belong to the post a person holds, such as a case officer at a district office. When staff move, the replacement takes over the post and its caseload with a handover, and nothing has to be granted again.
The end of the order	At the end date the device is removed, the case is closed and archived, and its records are kept for the agency's retention period and then purged. Removing a device before the end date needs a second person to approve.

Enrolment and devices

An enrolment officer registers the person, pairs and fits the tag, installs the home beacon and confirms the first good fix before the person leaves. The device's whole life, from stock to repair, is on the record.

Enrolment	The person's photo, identity, address and next of kin are registered, the rules from the order are loaded and reviewed, and the tag is paired by its IMEI and SIM. The case is not live until the first good fix is confirmed.
Fitting and the home beacon	The strap is sized, fitted and locked, the home beacon is installed and paired, and the home Wi-Fi is registered. The field app walks the officer through each step as a checklist. Straps in sizes from 140 to 315 mm. A beacon on the wall or the floor, indoors or out.

The devices it works with	Ankle tags, wrist or ankle bracelets, home beacons and power banks. Each model reports to the platform's own gateway, which turns its messages into one event model, so a new model can be added without changing the rest of the platform. Satellite positioning outdoors, Wi-Fi, Bluetooth and the mobile network indoors. 4G with 2G fallback. Sealed to IP68. Charged from a power bank while it is worn.
Swap and removal	A faulty device is swapped without closing the case, and the new one is paired before the old one is unpaired. A device is removed at the end of the order, or early with a second person's approval.
Stock, inspection and repairs	Each agency keeps its own stock of tags, beacons, power banks and straps. A returned device is inspected, cleaned and put back in stock, or sent for repair, and its history follows it. SIM cards managed with the device they sit in. Firmware rolled out over the air, in stages.

Court evidence

A breach becomes a signed evidence document, with the location history behind it. Each document carries a hash and a verification code, so a court can check a printout has not been altered.

Signed evidence documents	A breach report sets out the order, the condition broken, the alarm, the positions before and after, and how the control room responded, with a map. It is signed by the issuing officer. Official letters and SMS to the person produced from the same case. Location history for any period, on the same footing.
A code a court can verify	Every document carries a hash of its contents and a verification code. Anyone holding the printout can check the code against the platform and see whether it matches what was issued.
The court portal	A court registrar sees the court's own cases and nothing else: the people the court has placed on monitoring, a compliance summary for each, and the evidence reports requested and received.
Evidence requests	The court requests a report for a case and a period, the agency produces it, and the registrar downloads it from the portal. Each request, each document and each download is written to the audit trail.

Who it's for

Prison Department	For people on parole and licensed release: enrolment at the office, curfew at home and zones from the licence conditions, a caseload per officer, the control room on alarms, and evidence when a condition is broken.
Courts	For bail and court orders with electronic monitoring as a condition: the court's own cases in a portal, compliance summaries, evidence reports requested and downloaded, and documents a court can verify.

Police Department	For people under police supervision orders: zones and reporting rules from the order, the control room on alarms, response requests sent to field responders on their app, and outcomes recorded on scene.
Control rooms	For the people on shift around the clock: the alarm queue in order of severity, the live map wall, the agency's playbook for each alarm, a call through the tag, and a shift handover that leaves nothing open.

A day in the control room on asasii emd

09:00 A new order	A court places a person on bail with monitoring. The order sets the home address, a curfew from 10 pm to 6 am and one exclusion zone.
10:30 Enrolment	The enrolment officer registers the person, fits and locks the tag, installs the home beacon and confirms the first good fix before the person leaves.
14:10 Low battery	A tag on another case reports a low battery. The person is reminded by SMS, and the alarm closes when charging starts.
19:00 Shift handover	The day supervisor hands over two open alarms and one escalation, and the night supervisor accepts them on the record.
22:14 Curfew breach	A person is not home at the start of curfew. The beacon, the home Wi-Fi and the position all agree, and a High alarm opens.
22:16 A call through the tag	The operator calls the wearer through the tag. He is ten minutes away, on his way home from work, and the call is logged.
22:31 Home	The beacon sees the tag again. The operator resolves the alarm with a reason and escalates it to the case officer for the morning.
Next day A breach report	The case officer requests a breach report. It comes back signed, with a verification code, ready for the court.

A platform the agency owns, not a vendor portal

Tags usually come with the maker's own tracking portal. asasii emd replaces it with a platform built for Malaysian agencies, run in the agency's own environment.

	A device maker's portal	asasii emd
Where the data lives	The maker's cloud, often abroad	The agency's own data centre or a Malaysian government cloud
The maps	An outside map service sees every position	Self-hosted maps, so no position leaves the platform
The devices	One maker's tags only	Several models through one gateway, and more added later

Agencies	One account, shared	Each agency sees only its own people, cases and staff
Evidence	Screenshots and exported spreadsheets	Signed documents with a verification code

Security and Malaysian compliance

Data kept in Malaysia	In the agency's own data centre or a Malaysian government cloud, never a device maker's cloud.
Self-hosted maps	Map tiles served from inside the platform, so no position goes to an outside map service.
Every view audited	Each view of a person's location and every export written to the audit trail.
Agencies kept apart	Each agency sees only its own people, cases, devices and staff.
Two-person removal	Removing a device before the order ends needs a second person to approve.
Training kept apart	A training mode with its own data, deleted after seven days.

Services

Scope, pilot and proposal	Send the orders your agency places on monitoring, how many people are on monitoring or expected to be, and how alarms are handled today. An engineer replies with a pilot plan, a deployment plan and a proposal. It goes live in one control room and one office first, with the agency's own playbooks and the wording of its own orders.
Installation in Malaysia	asasii emd runs in the agency's own data centre or a Malaysian government cloud, with the device gateway and the maps inside it. idataraya installs it, hardens it, loads the agency's posts, roles, playbooks and zones, and keeps it current. The agency's team holds the keys, the backups and the data.
Support and maintenance	One team looks after the platform, the gateway and the field app for the life of the agreement, with response times set by severity for a control room that never closes. Severity-based response times, measured monthly. Continuous monitoring of the platform and the device gateway. A drilled backup and restore. Security patches and device firmware rollouts. Support and incident response.
The yearly agreement	Releases, patches, device firmware rollouts, the customisations made for you, monitoring, severity-based response and restoration targets, and the changes needed as orders and policy move. Hosting stays with the agency, and the platform belongs to it.

Talk to our team

Send us the orders your agency places on monitoring, how many people are on monitoring or expected to be, and how alarms are handled today. An engineer replies with a pilot plan, a deployment plan and a proposal.

Send us	The orders your agency places on monitoring, How many people are on monitoring, or expected to be, How alarms are handled today
You get back	A pilot plan, A deployment plan, A proposal
Email	info@idataraya.com
Website	emd.asasii.com/contact/

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