FORTAI WHITE PAPER | POLICY & POLICING SERIES

Audit-Ready Policing in the IPCC Era

How Agentic infrastructure intelligence converts every shift, every visitor, and every incident into tamper-evident, queryable evidence — before the complaint arrives.

PREPARED FOR

PDRM Special Dialogue V 2026 · Kuala Lumpur · 12–13 May 2026

AUTHORED BY

D1 FORTIFICATION PVT LTD

Bangalore, India.

fortai.digital ·

Version 1.0 · May 2026

Executive Summary

On 1 November 2023, the Independent Police Conduct Commission (IPCC) of Malaysia officially commenced operations under Act 839, ushering in a new era of statutory civilian oversight over the Polis Diraja Malaysia (PDRM). For the first time, a dedicated body holds a parliamentary mandate to receive, monitor, and investigate complaints of police misconduct, with particular focus on deaths in custody, sexual offences against detainees, and serious injuries occurring in police facilities.

The IPCC's arrival fundamentally changes the operational risk profile of every police station, lock-up, and detention facility in the country. What was previously a matter of internal discipline is now a matter of public record, parliamentary reporting, and external scrutiny. The question facing every Officer-in-Charge of a Police District (OCPD) is no longer whether a complaint will arrive — it is whether the station's records can withstand the moment when one does.

This is the central problem this paper addresses. Across the policing world, oversight bodies do not fail because investigators are insufficiently skilled or because officers are uniformly dishonest. They fail because the underlying evidentiary record is incomplete, inconsistent, or non-existent. Visitor logs at police station gates are written in pen on paper. Lock-up registers depend on the diligence of the duty officer at 03:00. Incident notes live in a personal diary. When a complaint surfaces six weeks later, reconstruction is forensic archaeology, not record retrieval.

> **The Core Argument**
>
> Audit-readiness cannot be retrofitted after a complaint. It must be the default operational state of every facility — generated automatically, captured continuously, and stored in a form that no individual officer can alter, lose, or misplace. This is not a surveillance problem. It is a governance problem.

FortAI's Agentic Infrastructure Intelligence (AII) platform delivers this default state. By converting the manual logs that police personnel already maintain — visitor entries, vehicle movements, shift handovers, incident notes, custody check-ins — into structured, timestamped, tamper-evident records queryable over WhatsApp, the platform produces what we call audit-ready policing: an operational posture in which the station is always prepared for inquiry, not because it anticipates wrongdoing, but because it has nothing to hide and everything to show.

Critically, FortAI requires no new hardware, no biometric kiosks, no body cameras, no facial recognition. The platform layers onto the existing manual practices of the policing institution and elevates them into a queryable digital intelligence system. It is built for the constraints of real police facilities — bandwidth-poor environments, multilingual personnel, budget-conscious procurement cycles, and political sensitivities around mass surveillance.

What This Paper Sets Out

- The structural evidentiary gaps that make any oversight regime — including the IPCC — vulnerable to failure, and why these gaps are an operational problem before they are a legal one.
- A framework for audit-ready policing built on six AI-driven officer roles deployed across a station's daily workflow, each producing a category of structured evidence.

- How WhatsApp-native querying makes the system usable by every rank, in every district, without retraining or hardware deployment.
- A governance model that aligns with the IPCC's statutory remit while protecting officer welfare and operational confidentiality — security through governance, not surveillance.
- A phased deployment pathway suitable for pilot at the District (IPD) level and scalable to State Contingents and Federal commands.

This paper is intended for senior PDRM leadership, Ministry of Home Affairs officials, IPCC commissioners and staff, and policy researchers concerned with the modernisation of Malaysian policing. The argument is straightforward: in the IPCC era, the stations that adopt audit-readiness as a default posture will be the stations that earn — and retain — public trust.

Contents

1. The IPCC Era: A Structural Shift in Police Accountability

Malaysia's journey towards independent police oversight has been long, contested, and incomplete. The Royal Commission to Enhance the Operation and Management of the Royal Malaysia Police (2005) recommended an Independent Police Complaints and Misconduct Commission (IPCMC) with full disciplinary authority. Successive governments tabled and withdrew variants of that proposal, until the Independent Police Conduct Commission Act 2022 (Act 839) was passed by Parliament, gazetted on 18 October 2022, and brought into force on 1 July 2023. The IPCC commenced operations on 1 November 2023.

The Commission's mandate, while narrower than the IPCMC originally envisioned, is nonetheless a defining moment for Malaysian policing. Under Section 4 of Act 839, the IPCC is empowered to receive complaints of misconduct against members of the police force, monitor and investigate such complaints, advise the government on integrity within the force, and submit an annual report to Parliament under Section 39. Section 37 mandates dedicated parliamentary funding to ensure the Commission can discharge its functions.

Beyond its formal powers, the IPCC's existence reshapes the operating environment of every police station. Three structural shifts are particularly consequential.

1.1 The Shift from Internal to External Scrutiny

Prior to the IPCC, police misconduct was overwhelmingly handled within the disciplinary architecture of the force itself, with the Enforcement Agency Integrity Commission (EAIC) providing limited external oversight across multiple agencies. The IPCC narrows the lens specifically onto PDRM and obliges the force to engage with a body whose findings, although advisory, are tabled in Parliament and published in annual reports. A complaint that previously moved through internal channels now creates an external paper trail that can be cited by Members of Parliament, civil society organisations, and the media.

1.2 The Mandatory Referral of Custody Incidents

Section 4 of Act 839 establishes a particularly important obligation: any incident involving sexual crimes against, or any incident resulting in serious injury or death of, any person in the lock-up or custody of police force members must be referred to the IPCC. This is not a discretionary referral. It is a mandatory disclosure obligation that places custody management at the centre of the IPCC's attention. Every lock-up roster, every detainee welfare check, and every incident note now exists in a regulatory environment where its accuracy may be tested by an external body within weeks of the event.

By December 2024, the IPCC had received 529 complaints, with cases involving abuse of power referred to the MACC and criminal matters returned to PDRM for action. The complaint volume confirms what was already evident: the public, civil society, and the legal profession are actively engaging with the new mechanism.

1.3 The Public Trust Imperative

Critics of the Act, including the Malaysian Bar and several civil society organisations, have argued that the IPCC's lack of disciplinary authority and search-and-seizure powers limits its effectiveness. They have also flagged structural concerns about commissioner appointments and the requirement to provide advance notice for visits to police premises. While these debates remain active and may result in further legislative reform, they have a single unifying implication for PDRM

operations: the spotlight is not going away. If anything, the perceived weaknesses of the current Act will intensify pressure on the police to demonstrate, through their own records and conduct, that civilian oversight is not a threat but a shared standard of integrity.

> **The Operational Reality**
>
> Whether the IPCC remains in its current form, is amended toward the IPCMC model, or is supplemented by additional accountability mechanisms, the trajectory is one-directional. Malaysian policing has entered a period of permanent, structured, external scrutiny. The stations that thrive in this environment will be those that treat audit-readiness as a daily operational discipline rather than a reactive scramble.

1.4 A Regional Pattern, Not an Isolated Reform

Malaysia is not alone. Across the Asia-Pacific region, parliamentary oversight bodies, anti-corruption commissions, and human rights institutions are tightening their focus on policing practice. India's National Human Rights Commission has expanded reporting requirements on custody deaths. The Philippines' Internal Affairs Service has institutionalised post-incident review. Indonesia's Kompolnas issues annual public assessments. Australia, the United Kingdom, and New Zealand operate fully empowered oversight commissions that have become the international reference points for the IPCC's eventual evolution.

What unites these reforms is a single underlying assumption that police agencies cannot afford to ignore: oversight, once established, expands. It rarely contracts. The technological and operational posture a force adopts in response to today's mandate will determine its readiness for tomorrow's expansion of that mandate.

2. The Evidentiary Gap: Why Oversight Regimes Fail

If oversight bodies were uniformly successful, the historical record would not contain repeated cycles of inquiry, recommendation, reform, and renewed inquiry. They are not uniformly successful. The reasons are many — political, institutional, cultural — but a single factor recurs across jurisdictions and regimes with striking consistency: the underlying evidence is missing.

We define the evidentiary gap as the structural shortfall between the records an oversight body needs to make a finding and the records that police facilities actually generate, retain, and produce on demand. This gap is rarely the result of deliberate destruction. More often, it is the cumulative product of three operational realities common to every police station, including those operated to the highest professional standards.

2.1 The Manual Logbook Problem

The vast majority of activity at a police station is recorded by hand. Visitor logs at the front desk, vehicle movements at the gate, lock-up entries and exits, meal distributions to detainees, welfare check timings, vendor visits, complainant arrivals, and shift handovers are typically captured in bound paper registers or loose forms. Each entry depends on the diligence, legibility, and presence of the duty officer at the moment the event occurs.

When operational tempo rises — during festive surges, public order events, or major investigations — entries become abbreviated, deferred, or skipped entirely. When tempo is low, fatigue and routine produce the same effect for different reasons. By the end of a single shift, a typical urban station has generated dozens of partial records distributed across multiple registers, none of which are searchable, cross-referenced, or backed up.

2.2 The Reconstruction Problem

When a complaint arrives — whether from a member of the public, a defence counsel, an MP's office, or the IPCC itself — the station is required to reconstruct events that occurred days, weeks, or months earlier. Reconstruction relies on retrieving the relevant register, locating the relevant page, deciphering the relevant handwriting, and corroborating the entry against other records that may or may not exist.

Where the original record is incomplete, the reconstruction relies on memory. Memory is unreliable, contestable, and easily challenged. Where memory is supplemented by good faith — and we do not assume otherwise — the result still falls short of what an external investigator can defend in a parliamentary report. The evidentiary gap is a problem of provenance: nobody can prove, beyond the duty officer's word, what was logged, when, and by whom.

2.3 The Discoverability Problem

Even where complete records exist, they are not discoverable in any operationally meaningful sense. A station commander asked to confirm whether a particular vehicle entered the compound between 22:00 and 23:00 on a given date faces a manual search across one or more registers. A district commander asked to identify all stations with detainee welfare check intervals exceeding two hours over the past quarter cannot answer the question at all without a multi-week audit. The IPCC, asked to assess patterns of conduct across multiple districts, faces an undertaking that few oversight bodies anywhere in the world have the resources to complete.

Discoverability is the silent killer of accountability. A record that cannot be retrieved is, for every practical purpose, a record that does not exist.

2.4 What This Means in Practice

Consider three scenarios drawn directly from the categories of incident that Section 4 of Act 839 obliges PDRM to refer to the IPCC.

Scenario 1 — A Death in Custody

A detainee in a district lock-up is found unresponsive at 04:20. The duty officer initiates emergency response and records the event. Six weeks later, the IPCC requests the welfare check log for the preceding 24 hours, the visitor log, the meal register, the shift handover note, and the vehicle movement register. The station produces partial records. Three checks are missing because the duty officer at the time was attending another incident. The visitor log is legible but incomplete because two entries were entered after the fact. The vehicle register has been overwritten on a separate page. Each gap is innocent. The combined effect is a record that cannot defend the station even though no misconduct occurred.

Scenario 2 — A Complaint of Improper Search

A member of the public files a complaint that an unauthorised vehicle search was conducted at a checkpoint at 19:40 on a particular date. The complaint reaches the IPCC, which requests the deployment register, the patrol log, and the body-worn or dashboard video where available. The patrol log records the deployment but does not capture the precise minute the patrol arrived at or departed the checkpoint. The deployment register confirms the personnel on duty but not their movements. There is no verified independent timestamp of the events at the checkpoint itself. The officers concerned may have acted entirely properly. They cannot prove it.

Scenario 3 — A Vendor Access Allegation

An allegation surfaces that a contracted vendor entered restricted premises outside authorised hours over a sustained period. The IPCC requests a 90-day vendor access history. The station's vendor log is maintained at the gate and recorded by hand. Reconstructing 90 days of entries requires retrieving multiple registers, transcribing approximately 600 entries, and cross-referencing against shift schedules. The exercise consumes 80 staff-hours and produces a record with acknowledged gaps. The gaps may not exonerate the vendor. They certainly do not exonerate the station's controls.

In each scenario, the evidentiary gap is the determining factor. The conduct of the officers may have been entirely proper, partially proper, or improper. The station's records cannot tell us with certainty which it was. This is the operational reality the IPCC inherits, and it is the reality that any serious modernisation of Malaysian policing must address before any other technological investment is considered.

3. Defining Audit-Ready Policing

We propose the term audit-ready policing to describe an operational posture in which a police facility is, by default and at all times, capable of producing on demand a complete, tamper-evident, and queryable record of its activities to any authorised inquirer — internal supervisor, external auditor, IPCC investigator, or counsel. Audit-readiness is not a project that is completed and filed. It is a continuous condition of the facility, sustained by the systems and disciplines that govern its daily operation.

The concept rests on five operational properties. Each property is a necessary condition. None is sufficient on its own.

3.1 The Five Properties of Audit-Readiness

PROPERTY	OPERATIONAL DEFINITION
Completeness	Every event of regulatory interest — every visitor, every vehicle, every detainee interaction, every welfare check, every shift change — is captured at the moment it occurs, with no reliance on subsequent transcription or memory.
Tamper-Evidence	Records carry a verifiable provenance such that any retrospective alteration is detectable. The objective is not to make alteration impossible — paper alteration is impossible to prevent — but to make it visible.
Discoverability	Records can be retrieved by query in seconds, across any time window, by any authorised user, without requiring a custodian to be present at the facility holding the original document.
Cross-Referencing	Records from different categories — visitor, vehicle, custody, incident, deployment — can be aligned along a common timeline so that a single event can be reconstructed from multiple corroborating sources.
Proportionality	The records captured are limited to those operationally and legally necessary. The system does not generate surveillance data on members of the public who are not the subject of police interest, and it does not subject officers to monitoring beyond the legitimate scope of their duties.

3.2 What Audit-Readiness Is Not

It is important to distinguish audit-ready policing from several adjacent concepts that are sometimes confused with it.

- **Audit-readiness is not surveillance.** Surveillance entails the ongoing observation of subjects without specific operational justification. Audit-readiness entails the structured recording of events that police personnel are already obliged to record, in a form that supports retrieval and verification.
- **Audit-readiness is not predictive policing.** Predictive systems use historical data to forecast where or by whom future offences may be committed, raising serious civil liberties concerns. Audit-readiness looks backward, not forward, and addresses the integrity of records about events that have already occurred.
- **Audit-readiness is not body-worn cameras.** Body-worn camera programmes are an important parallel reform with their own merits and operational considerations. Audit-readiness is concerned with the structural records of facilities, not the capture of individual encounters in the field, although the two approaches complement one another.
- **Audit-readiness is not facial recognition.** FortAI's platform does not perform identification of unidentified subjects. It records events as they are reported by the personnel responsible for them, in the same way these events have always been reported, with the addition of structured digital provenance.

In short, audit-ready policing is the modernisation of paperwork. Its ambition is at once narrower and more consequential than the technological projects with which it is sometimes conflated.

4. FortAI's Agentic Infrastructure Intelligence Architecture

FortAI delivers audit-ready policing through a platform we call Agentic Infrastructure Intelligence (AII). The category name is deliberate. It signals that the system operates at the level of physical infrastructure — stations, lock-ups, gates, perimeters, deployment locations — and that the intelligence it produces is generated by autonomous AI agents rather than retrieved from static databases. AII converts the manual operational language of policing into structured, queryable knowledge.

4.1 Architectural Principles

Five design principles govern every aspect of the FortAI platform. Each principle reflects a constraint we have observed in real police and large-scale security environments across South and Southeast Asia.

1. No new hardware. The platform requires no biometric kiosks, no RFID readers, no body-worn cameras, no CCTV upgrades, no fixed terminals. It works with the smartphones that personnel already carry and the registers they already maintain.
2. WhatsApp, Botim, WeChat native interaction. All queries, alerts, and reports are delivered through WhatsApp, an interface every officer in Malaysia and the region uses every day. There is no new application to install, no login to remember, and no training programme to run.
3. Multilingual by design. The platform handles Bahasa Malaysia, English, Tamil, Mandarin, and other regional languages natively. Officers query in the language they prefer; the system responds in that language.
4. Bandwidth-resilient. The platform is engineered for environments with intermittent connectivity. Records captured offline synchronise when connectivity is restored, with no loss of timestamp integrity.
5. Governance over surveillance. The platform is configured to record what governance and oversight require, and nothing more. This boundary is not optional; it is enforced architecturally.

4.2 The Three Layers

The FortAI platform comprises three logical layers. We describe each in turn in the next page.

LAYER	FUNCTION
Capture Layer	The point at which a duty officer records an event. This may be a photograph of a paper register, a voice note, a structured WhatsApp message, or a typed entry. Whatever the input format, it is timestamped, geo-stamped, and attributed to the personnel on duty.
Extraction Layer	Multiple AI models — for vision, language, and structured-data parsing — convert raw inputs into a normalised record schema. Names, vehicle plates, times, durations, anomalies, and entity relationships are extracted, validated, and indexed.
Intelligence Layer	Six purpose-built AI Officers — VIGIL, SUPPLY, PATROL, SENTINEL, ANALYST, and WATCH — each apply domain-specific logic to the structured records, surfacing anomalies, generating alerts, answering queries, and producing the daily, weekly, and monthly reports that station and district commanders require.

4.3 Tamper-Evidence and Provenance

Every record entering the FortAI platform is cryptographically sealed at the moment of capture. The seal binds the record content to the timestamp, the device of capture, and the identity of the personnel responsible. Subsequent retrieval, modification, or deletion produces a corresponding entry in an immutable audit log. The objective is forensic provenance: when a record is presented to an internal supervisor, a court, or the IPCC, its integrity can be independently verified without reliance on the testimony of the duty officer.

This is not blockchain marketing. It is a straightforward application of cryptographic hashing and time-stamping techniques that have been standard practice in regulated industries for over two decades. We have engineered them into a workflow that police personnel can use without specialised technical knowledge.

4.4 The Query Interface

The capture and extraction layers would be of little practical value if their output remained inaccessible to the personnel who need it. The FortAI query interface is designed to serve exactly the people who own operational risk — Officers-in-Charge of Police Stations (OCS), Officers-in-Charge of Police Districts (OCPD), State Contingent commanders, and inspectorate teams — through the channel they already use.

A station commander asks, in WhatsApp, in the language of their choice: "List all visitors to the station on 14 April between 18:00 and 22:00." The platform returns a structured list within seconds, complete with the personnel who logged each entry and any anomalies flagged at the time of capture. There is no portal, no dashboard, no client application. There is the question and the answer.

Why WhatsApp (Messaging Platforms Can Differ According To What's Required)

We selected WhatsApp as the primary interface for a single, decisive reason: it is already the operational nervous system of policing across the region. Senior officers conduct operational coordination on it. Field personnel report on it. Districts brief contingents on it. Building on this foundation rather than competing with it eliminates the adoption friction that defeats most public-sector technology programmes.

5. The Six AI Officers (next page continued)

FortAI's intelligence layer is organised around six named AI Officers, each responsible for a category of operational record. The officer metaphor is more than a marketing convenience. It reflects the way personnel actually conceptualise their duties: visitor control is a discrete responsibility, vendor management is another, patrol oversight is a third. By aligning the system's logical architecture with the operational architecture of the station, we ensure that every record has a clear owner and every query has a clear answer.

AI OFFICER	DOMAIN	FUNCTION IN AN AUDIT-READY STATION
VIGIL	**Visitor Intelligence**	Captures and structures every entry to the station: complainants, family members of detainees, contractors, official visitors. Cross-references against expected appointments, flags repeat or anomalous visitors, produces day, week, and month reports on demand.
SUPPLY	**Vendor & Supply Chain**	Records every vendor, contractor, and supplier interaction with the facility — fuel deliveries, food services, maintenance, IT support. Maintains a verified vendor profile with access histories, eliminating the single largest source of unrecorded movement on most premises.
PATROL	**Deployment & Movement**	Tracks the deployment, movement, and timing of patrol units, beat constables, and mobile teams. Geo-stamped check-ins replace paper deployment registers. Produces verifiable patrol histories that defend stations against allegations of absence or improper conduct in the field.
SENTINEL	**Custody & Lock-up**	The most operationally sensitive officer, given the IPCC's mandatory referral obligations. Captures and timestamps every detainee event: entry, welfare check, meal, family visit, medical attention, transfer, release. Welfare check intervals are monitored automatically; missed checks generate alerts to the OCS and OCPD.
ANALYST	**Reporting & Insights**	The cross-cutting officer that turns the records produced by VIGIL, SUPPLY, PATROL, SENTINEL and WATCH into the daily, weekly, monthly, and on-demand reports that station and district commanders need. Powers the WhatsApp query interface and produces the exception reports that go to inspectorate teams.
WAT C H	**Incident & Exception**	Captures incidents, exceptions, and unusual events — disturbances at the gate, public complaints at the desk, equipment failures, unscheduled visits by senior officers. Structures unstructured events into a categorised, searchable incident corpus that supports both internal review and external inquiry.

5.1 How the Officers Work Together

The power of the architecture lies in the cross-referencing between officers. A single moment in the operational life of a station typically generates records across multiple domains. A vehicle arriving at the gate at 02:14 is logged by SUPPLY (if a vendor) or VIGIL (if an official visitor). The personnel on duty at the gate are logged by PATROL. If the visitor proceeds to the lock-up, SENTINEL records the interaction with any detainee. If anything unusual occurs, WATCH captures it. ANALYST aligns all five records along the same timeline and presents them as a single, coherent narrative on request.

This is the practical answer to the reconstruction problem identified in Section 2. When the IPCC requests a reconstruction of events occurring six weeks earlier, the platform produces it in seconds, with full provenance, in a form that is independently verifiable.

5.2 The Officers as a Force Multiplier

We are conscious of the limits of any technology framing. The AI Officers do not replace personnel. They eliminate the administrative overhead that prevents personnel from doing the work they joined the force to do. A station commander who currently spends two hours a day on register reviews and end-of-shift summaries reclaims those two hours for supervision, mentorship, and community engagement. The officers handle the paperwork. The officer in uniform handles the policing.

> **An Honest Boundary**
>
> The AI Officers are an operational and administrative layer. They are not investigative agents, they do not make disciplinary judgements, and they do not replace human review. Every alert, every anomaly, every flag is presented to a human officer who retains complete decision authority. The platform's role is to ensure that the human officer has the complete record on which to base that decision.

6. Mapping FortAI to the IPCC Statutory Framework

We now turn to the specific ways in which the FortAI platform supports PDRM's obligations under the IPCC Act 2022. Our intent in this section is operational, not legal: we are not interpreting the Act, but illustrating how a station equipped with FortAI is positioned to respond to inquiries falling within the IPCC's mandate.

The mapping below addresses the four categories of IPCC engagement that most directly affect station operations.

6.1 Mandatory Referral of Custody Incidents (Section 4)

Section 4 obliges PDRM to refer to the IPCC any incident involving sexual crimes against, or any serious injury or death of, any person in police custody. The post-referral inquiry will require a complete record of the affected person's experience in custody from the moment of arrest to the moment of the incident. SENTINEL captures every welfare check, meal, medical event, family visit, and movement. VIGIL captures every visitor to the station during the period. PATROL captures the deployment of personnel. WATCH captures any anomaly noted at the time. ANALYST aligns all four into a single retrievable timeline.

The benefit is not merely administrative. The OCPD called to brief the IPCC arrives with a complete, timestamped, tamper-evident record. The narrative is supported, not improvised. Where the conduct of officers was proper, the record shows it. Where there are questions to answer, those questions are addressed against verified evidence.

6.2 Public Complaints to the Commission (Section 4)

The IPCC reported 529 complaints by December 2024, spanning abuse of power, alleged misconduct in the field, custodial concerns, and procedural disputes. For each complaint, the affected station will eventually be asked to produce its records of the event. With FortAI, the production is a query. Without it, the production is an investigation in itself.

This matters at scale. A district contingent receiving multiple parallel inquiries cannot resource the manual reconstruction effort required for each. With FortAI, the OCPD's office responds to ten inquiries with the same effort previously required for one — and produces a more complete record for each.

6.3 Annual Reports to Parliament (Section 39)

The IPCC's annual reports will draw on aggregate data across districts and contingents. Where PDRM is invited to provide systemic information — average welfare check intervals, visitor logging compliance rates, exception incidents per 1,000 detainee-days — the absence of structured data forces the force to either decline the invitation or to mount a costly survey. With FortAI, the data is already structured. State Contingent commanders can produce comparable, defensible figures within the response windows the Commission expects.

6.4 Visits to Police Premises (Section 16)

The IPCC has the power to visit police premises, with advance notice, to inspect facilities and conditions. Critics of the Act have argued that the advance-notice requirement undermines the value of these visits. We do not enter that debate. Our observation is operational: a station that maintains audit-readiness as a daily discipline is no more or less prepared for a visit twenty-four hours from now than it is for a visit two months from now. Audit-readiness eliminates the very category of preparation that the advance-notice critique presupposes.

6.5 What the Mapping Means

Considered together, these four categories of IPCC engagement converge on a single requirement: the station must be able to demonstrate, on demand, the integrity of its records over any time window the Commission specifies. FortAI is engineered specifically to produce this demonstration.

IPCC ENGAGEMENT	EVIDENCE REQUIRED	FORTAI CAPABILITY
Custody incident referral	Complete custody timeline; visitor list; deployment log	SENTINEL + VIGIL + PATROL aligned via ANALYST
Public complaint inquiry	Event reconstruction within minutes-precision time window	WhatsApp query against full provenance corpus
Pattern/aggregate inquiry	Systemic data across districts and time windows	ANALYST cross-station and cross-period reports
Premises visit	Live operational records for any period	Always-on audit-ready posture; no preparation lag
Annual parliamentary report	Aggregate compliance and incident statistics	Pre-structured data exports for State Contingent submission

None of these capabilities depends on the technical sophistication of the station's personnel, the connectivity of the district, or the budgetary cycle of the contingent. The capabilities are the platform's default state.

7. Governance, Not Surveillance: The Civil Liberties Boundary

Any platform that captures structured records of police activity raises legitimate civil liberties questions. We take these questions seriously, both because they are intrinsically important and because the long-term acceptance of audit-ready policing depends on getting the boundary right.

Our position is straightforward: FortAI is a governance system, not a surveillance system. The distinction is not rhetorical. It is reflected in the architecture, the data scope, and the access controls of the platform.

7.1 What FortAI Records

FortAI records the events that police personnel are already obliged to record under existing standing orders, in a form that supports retrieval and verification. It records:

- Visitors to police facilities, their stated purpose, and their interaction with personnel.
- Vehicle and vendor movements at police premises.
- Custody events affecting persons lawfully detained.
- Deployment, movement, and on-duty timing of police personnel.
- Incidents and exceptions occurring within or adjacent to the facility.

7.2 What FortAI Does Not Record

Equally important is the inventory of data the platform does not capture. FortAI does not:

- Identify individual members of the public through facial recognition or similar biometric techniques (integration to CCTV possible).
- Track the movements of members of the public who are not the subject of legitimate police interest.
- Aggregate or share data with private commercial parties.
- Generate predictive models about individuals, communities, or populations.
- Monitor the personal communications, off-duty activities, or social associations of police personnel.

> **Architectural Boundary, Not Policy Promise**
>
> These exclusions are enforced at the level of the platform's architecture. They are not a policy that can be quietly relaxed by a system administrator with elevated privileges. Where the boundary needs to evolve in response to new statutory authority or operational requirements, the change must be made through the formal governance process, with corresponding audit and oversight implications.

7.3 Access Controls

Access to FortAI records is governed by a tiered permission model that mirrors the operational hierarchy of PDRM. An OCS sees records pertaining to their station. An OCPD sees records pertaining to their district. A State Contingent commander sees aggregate data across the contingent. Specific, individually attributed inquiries — for example, the

welfare history of a named detainee — generate audit log entries that are themselves visible to internal audit and, where appropriate, to the IPCC.

The platform's audit log is itself audit-ready. An inquiry into who accessed what, when, and for what stated purpose can be produced on demand, in the same WhatsApp interface as any operational query.

7.4 Alignment with the DPDP Act 2023 and PDPA 2010

FortAI is engineered to comply with Malaysia's Personal Data Protection Act 2010 (PDPA) and incorporates lessons from emerging regional data protection regimes including India's Digital Personal Data Protection Act 2023. Personal data is collected only for specified, lawful purposes; retention periods are configurable and time-bound; data subject rights are supported through structured workflows; and cross-border data transfers are subject to the relevant safeguards. Where the IPCC, MACC, or other authorised body requests data, the request is itself a logged event.

7.5 The Long View

Civil society scepticism of police technology programmes is not unreasonable. Police forces around the world have, in places and at times, deployed technology in ways that subsequently proved unjustifiable. The strongest defence against such drift is not a public assurance but an architectural constraint backed by an external audit trail. FortAI's design reflects this conviction. The platform is built not only to serve PDRM in the IPCC era, but to serve PDRM in any future era of expanded oversight that the IPCC era may evolve into.

8. Officer Welfare and the Dignity of the Force

The IPCC framework, like any oversight regime, can be experienced by individual officers as adversarial. The history of policing in many jurisdictions includes painful examples of frontline personnel left exposed by the absence of records that, had they existed, would have demonstrated their proper conduct. The Royal Commission of 2005 itself acknowledged this dynamic in its observations on the relationship between accountability and morale.

We believe that audit-ready policing serves officer welfare more strongly than any other technological reform currently being discussed. Three considerations make the case.

8.1 Records Defend the Innocent More Than They Condemn the Guilty

In the overwhelming majority of cases where a complaint is filed, the officers concerned have acted within the bounds of their duty. The challenge is proving it. The duty officer who recorded the welfare check at 02:14 is sometimes the same officer accused weeks later of having neglected the detainee. The patrol team that conducted a vehicle stop at 19:40 in accordance with checkpoint procedures may face an allegation of impropriety three months later. In each case, the verifiable record is the officer's strongest defence. A station with audit-ready records is a station that protects its personnel.

8.2 Reduced Administrative Burden

FortAI replaces the most time-consuming administrative tasks — register reconciliation, end-of-shift summaries, monthly compliance returns — with automated outputs. We have observed that station commanders typically reclaim between 90 and 150 minutes per shift previously spent on documentation. This time returns to supervision, mentorship, community engagement, and the rest of the work that brought officers into the force.

8.3 The Welfare of the Detainee Is the Welfare of the Custodian

The most distressing cases the IPCC will encounter — and that PDRM most strongly wishes to prevent — involve serious harm to persons in custody. SENTINEL's automated welfare-check monitoring is, before it is anything else, a safety system for detainees. A missed welfare check generates an alert before a deterioration becomes a crisis. The custodian on duty receives the support of the system in carrying out a duty that is, at the busiest hours of the night shift, the responsibility of fewer personnel than the situation warrants.

> **A Note on the Profession**
>
> We approach Malaysian policing with deep respect for an institution whose 217-year history reflects extraordinary service to the nation. The arrival of the IPCC is not a verdict on the profession. It is a structural evolution that the profession itself, in its most reflective leadership statements, has acknowledged as appropriate to the modern era. Our role is not to interpret that evolution, but to provide the operational infrastructure that lets every station meet it from a position of strength.

9. Phased Deployment Pathway for PDRM

We propose a four-phase deployment pathway designed to demonstrate operational value at each stage and to respect the budgetary, procedural, and political realities of a national police service. The pathway is illustrative; specific timing and scope would be agreed with the relevant authorities.

Phase 1 — Pilot at Three Police Districts (IPDs)

We recommend selecting three Police Districts of differing operational character: an urban high-volume district (for example, in Kuala Lumpur or Selangor), a coastal or border district with significant vehicle movement, and a smaller-population district where deployment of personnel is the principal operational concern. A 90-day pilot allows the platform to be configured to local procedures, the personnel to acclimatise to WhatsApp-based reporting, and the District commanders to validate the operational and audit benefits.

- **Duration:** 90 days.
- **Scope:** All five operational domains (visitor, vendor, deployment, custody, incident); ANALYST queries available to OCS and OCPD.
- **Success metrics:** 100% capture rate on visitor and custody events; less than 60-second response time on standard ANALYST queries; 90% reduction in time spent on end-of-shift documentation; positive personnel feedback exceeding 75%.
- **Governance:** Quarterly briefing to the Inspector-General of Police's office and IPCC liaison.

Phase 2 — State Contingent Roll-out

Following a successful pilot, the platform is rolled out across one or two State Contingents. This phase introduces cross-district aggregation and exception reporting at the contingent level, demonstrating value to State Contingent commanders for the first time at scale.

- **Duration:** 180 days.
- **Scope:** All districts in the selected contingents; quarterly reports to the Inspector-General; pilot integration with IPCC liaison protocols.

Phase 3 — National Roll-out

Subject to the outcomes of Phase 2, the platform is extended to all State Contingents over an 18-month period. Roll-out sequencing is determined by readiness, with dedicated change management, training (in Bahasa Malaysia, English, and additional languages as locally appropriate), and inspectorate engagement at each stage.

- **Duration:** 18 months.
- **Scope:** All districts and stations nationwide; full ANALYST query access for IGP, Deputy IGP, Directors, and State Contingent commanders.

Phase 4 — Federal and Specialised Deployments

The final phase extends the platform to federal commands, specialised divisions (Internal Security and Public Order, Criminal Investigation, Narcotics Crime Investigation, Special Branch as appropriate, Marine Operations Force, Federal Reserve Unit), and integrated deployments with the IPCC for parliamentary reporting purposes. This phase also includes

the productionisation of integrations with adjacent agencies — MACC, Immigration, Customs — where lawful, controlled inter-agency data exchange supports operational effectiveness.

An Honest Estimate

End-to-end transformation of a national police service is a multi-year programme. The phased pathway above is calibrated to demonstrate value at every stage, to allow course correction without sunk-cost lock-in, and to respect the budgetary cycles of the Ministry of Home Affairs. We do not propose a big-bang deployment, and we would advise against any vendor that does.

9.1 Cost Profile

FortAI is licensed on a per-station, per-month basis with volume tiers reflecting national, contingent, and district commitments. Because the platform requires no new hardware, the total cost of ownership is dominated by the licence fee and a one-time configuration and training engagement at each phase. We are prepared to discuss commercial terms with the Ministry of Home Affairs and PDRM on a basis that supports the Phase 1 pilot at no licence cost, with subsequent phases governed by mutually agreed performance milestones.

9.2 Risk Mitigation

Every technology deployment in a sensitive operational environment carries risk. We address the principal categories in the next page.

RISK	DESCRIPTION	MITIGATION
Adoption resistance	Personnel may perceive any new system as additional administrative burden	WhatsApp-native interface eliminates new app learning; phased rollout with frontline champions; training in operational languages
Data sensitivity	Custody and incident records are highly sensitive personal data	PDPA and DPDP-aligned architecture; tiered access controls; audit log of all access; in-country data residency options
Connectivity gaps	Some districts have intermittent mobile connectivity	Offline capture with timestamp-preserving sync; resilience to multi-day disconnection
Vendor dependency	Long-term reliance on a single technology provider	Open data export formats; contractual commitment to data portability; on-premise deployment option for federal commands
Civil liberties scrutiny	Public concern about expanded police data capture	Architectural enforcement of governance-not-surveillance boundary; transparent data scope; routine engagement with SUHAKAM and the Bar Council

10. Conclusion: The Audit-Ready Posture as National Asset

We began this paper with a straightforward observation: the arrival of the IPCC has changed, irreversibly and rightly, the operating environment of every Malaysian police station. The question is not whether to respond. The question is what kind of response best serves the institution, the public, and the officers in uniform who carry the responsibility of policing on behalf of the nation.

We have argued that the most important response is also the most operationally fundamental: the systematic elimination of the evidentiary gap that has, in every jurisdiction and every era, been the determining factor in the success or failure of oversight regimes. A station whose records are complete, tamper-evident, discoverable, cross-referenceable, and proportionate is a station that engages with the IPCC, the public, and its own internal supervisors from a position of strength, dignity, and integrity. A station without those records is exposed, regardless of the conduct of its personnel.

FortAI's Agentic Infrastructure Intelligence platform is the operational layer that delivers this default audit-ready state. It does so without new hardware, without surveillance overreach, and without imposing unfamiliar tools on the personnel who use it. Six AI Officers — VIGIL, SUPPLY, PATROL, SENTINEL, ANALYST, and WATCH — convert the manual logbooks of every station into a structured intelligence corpus queryable through the WhatsApp interface that PDRM personnel already trust and use every day.

The benefits compound. Officers reclaim time from documentation. Detainees benefit from automated welfare monitoring. Station commanders respond to inquiries in seconds rather than days. State Contingent commanders see aggregate compliance in real time. The Inspector-General's office can produce parliamentary-grade data without surveys and reconstruction efforts. The IPCC engages with a force whose records support, rather than complicate, its statutory work. The public sees a police service whose accountability is demonstrated by daily evidence rather than asserted by occasional press release.

> **The Strategic Argument, Restated**
>
> Audit-readiness is not a defensive posture. It is a national asset. A police service that has internalised the discipline of structured, verifiable record-keeping is a police service equipped to handle every future expansion of oversight, every future shift in public expectation, and every future crisis of confidence — from a position of evidence rather than improvisation. This posture, more than any single piece of legislation or any single technology, is what defines a modern, professional police force in the era of civilian oversight.

Malaysia stands at a defining moment for its policing institution. The IPCC era has arrived. The stations that adopt audit-readiness as a default operational posture today will be the stations that earn — and retain — the trust of the people they serve. We are honoured to support that journey.

We invite the leadership of the Polis Diraja Malaysia, the Ministry of Home Affairs, and the Independent Police Conduct Commission to engage with us on the path forward. We are prepared to begin pilot deployments at any time, on terms designed to demonstrate value before commitment. The pathway from the first pilot district to a fully audit-ready national service is multi-year, but the first thirty days of operational benefit at a single pilot station are sufficient to begin reshaping the conversation.

Appendix A: Glossary of Terms

TERM	DEFINITION
Act 839	The Independent Police Conduct Commission Act 2022, gazetted 18 October 2022, in force from 1 July 2023.
Agentic Infrastructure Intelligence (AII)	The category of AI platform that operates autonomous agents at the level of physical infrastructure to convert manual operational records into queryable structured intelligence. FortAI is the leading exponent of this category.
Audit-Ready Policing	An operational posture in which a police facility is, by default and at all times, capable of producing on demand a complete, tamper-evident, and queryable record of its activities.
DPDP Act 2023	India's Digital Personal Data Protection Act 2023; referenced as a regional benchmark for data protection principles.
EAIC	The Enforcement Agency Integrity Commission, the predecessor body to the IPCC for general police oversight in Malaysia.
IGP	Inspector-General of Police, the head of the Royal Malaysia Police.
IGSO	Inspector-General Standing Orders, governing operational matters under sections 96 and 97 of the Police Act 1967.
IPCC	The Independent Police Conduct Commission, established under Act 839, operational from 1 November 2023.
IPCMC	The Independent Police Complaints and Misconduct Commission, the more empowered oversight body proposed by the 2005 Royal Commission and not yet enacted.
OCPD	Officer-in-Charge of a Police District; the senior officer responsible for an Ibu Pejabat Daerah.
OCS	Officer-in-Charge of a Police Station.

PDPA 2010	Malaysia's Personal Data Protection Act 2010.
PDRM	Polis Diraja Malaysia, the Royal Malaysia Police.
Provenance	The verifiable origin and history of a record, including its time of creation, its creator, and any subsequent modifications.
Tamper-Evidence	The architectural property of a record system that any unauthorised alteration is detectable upon retrieval.

Appendix B: Sample WhatsApp Query Library for Station Commanders

The following queries are illustrative of the natural-language interactions available to authorised personnel through the FortAI WhatsApp interface. The platform handles such queries in Bahasa Malaysia, English, Tamil, and Mandarin as standard.

Visitor and Access Queries

- List all visitors to the station between 18:00 and 22:00 on 14 April 2026.
- Show every entry by Encik Ahmad bin Hassan over the past 30 days.
- Which vendors entered the compound after 20:00 in the past week?
- Were any visits to the lock-up by family members of detainees not pre-authorised?

Custody Queries

- Show the complete welfare check log for detainee record number D2026-0412.
- List any welfare check intervals exceeding 90 minutes in the past seven days.
- Produce the full custody timeline for the named detainee from arrival to release.
- Were any medical visits to detainees recorded in March 2026?

Deployment Queries

- Which patrol units were on duty in Sector 4 on 21 March between 19:00 and 21:00?
- Show the deployment record of Sergeant Tan for the past month.
- List any patrols where the geo-stamped check-in interval exceeded the standing order threshold.

Incident and Exception Queries

- Show all WATCH entries categorised as gate disturbances over the past 90 days.
- Were any IPCC-referrable incidents recorded at this station in Q1 2026?
- Produce the full incident log for the night shift on 9 February.

Aggregate and Compliance Queries (OCPD and above)

- Which stations in this district had welfare check compliance below 95% in the past month?
- Compare visitor logging completeness across the past four quarters.
- Generate the monthly IPCC compliance digest for District submission.

Appendix C: About FortAI and D1 Fortification

FortAI

FortAI is a one of a kind product, platform delivers Agentic Infrastructure Intelligence to enterprise, hospitality, healthcare, education, and government clients across India, with active deployments at landmark facilities including Pritech Park SEZ, Essensai67, Marks Square, the Bangalore Turf Club, and Restolex.

FortAI's mission is to make every facility audit-ready by default through the systematic conversion of manual operational records into structured, queryable, tamper-evident intelligence. The platform is engineered for environments where new hardware is not feasible, where personnel speak multiple languages, and where the operational pace does not allow for complex new tools.

D1 Fortification

D1 Fortification Pvt. Ltd. is the parent enterprise context in which FortAI's policing and security expertise has been developed. ISO 9001:2015 certified, D1 deploys more than 5,000 security personnel across the Indian states of Karnataka, Kerala, and Tamil Nadu, providing physical security services to corporate, residential, hospitality, and institutional clients. The combined enterprise brings together hands-on operational experience at the gate, in the lock-up, and at the perimeter, and the technological capability to translate that experience into a global standard for audit-ready operations.

For pilot deployment discussions, ministerial briefings, or further technical engagement:

D1 FORTIFICATION PVT LTD

Yohaan Kuruvilla,

Rajiv Kuruvilla

Founder & CEO, FortAI | Co-Chairman, D1 Fortification Pvt. Ltd.

Email: rajiv@d1secure.com

Web: fortai.digital

— End of White Paper —