AiiPD

Ai Interdisciplinary Professional Development

Security and Compliance Baseline

Internal Security Audit, Privacy Impact Assessment and Standards Alignment

GDPR Article 32 · ISO/IEC 27001 · IRAP · Australian Privacy Principles

Document version: 1.0 (Baseline)
Date: June 2026
Prepared by: Liam Michael Clancy, Founder and Principal
Classification: Confidential — for prospective partners and clients under NDA
www.aiipd.com.au · liamclancy@aiipd.com

Important: status of this document

This is a self-assessed baseline, not a certification.

This document records AiiPD's current and planned technical and organisational security measures, and its self-assessed alignment with recognised standards. It is prepared in good faith to support due diligence and enterprise procurement conversations.

It does not represent formal certification against ISO/IEC 27001, an completed IRAP assessment, or a regulator's determination of GDPR or Australian Privacy Act compliance. Formal certification requires assessment by an accredited external body. Where a control is marked Planned or Partial, it is not yet fully operational. AiiPD does not claim certifications it does not hold.

AiiPD operates at an early commercial stage. This baseline reflects a security-by-design posture appropriate to that stage, and a roadmap to formal assurance as the platform scales.

Contents

1. Executive summary

AiiPD is a civic intelligence and professional development platform that processes public-source institutional data, limited personal data (contact and account information for subscribers and clients), and client-supplied documents for analysis. Because our buyers include local government, regulated human-services providers and, potentially, government agencies, security and privacy are commercial prerequisites, not afterthoughts.

This baseline documents the technical and organisational measures AiiPD applies across four reference frameworks: the EU General Data Protection Regulation Article 32 (security of processing), ISO/IEC 27001 (information security management), the Australian Information Security Registered Assessors Program (IRAP) for government-facing work, and the Australian Privacy Principles (APPs) under the Privacy Act 1988.

Our posture is security-by-design and data-minimisation-by-default. We collect the least personal data necessary, we do not sell personal data, we do not use client data to train third-party AI models, and we keep a human in the loop for every consequential output. The sections below set out specific measures, a control-by-control GDPR Article 32 checklist, an ISO 27001 Annex A coverage map, an IRAP readiness view, and a Privacy Impact Assessment for the platform's core processing activities.

2. Scope and data inventory

2.1 What AiiPD processes

AiiPD processes four broad data categories:

- Public-source institutional data: council annual reports, budgets, strategic plans, ABS datasets, open-data portals and similar. This is published information, not personal data, though it is handled with provenance and verification controls.
- Account and contact data: names, organisational affiliation, email addresses and role information for subscribers, clients and enquirers. This is the primary personal-data holding.
- Client-supplied content: documents, engagement records and datasets a client provides for analysis. This may contain personal data, and is processed under the client's instructions as data processor.
- Derived analytical outputs: DRMC layer scores, RSC interpretive codings, benchmark indicators and reports. These are interpretive assessments, not validated measurements, and carry the standard DRMC caveat.

2.2 What AiiPD deliberately does not do

- No sale of personal data, and no advertising-based monetisation of personal data.
- No use of client or subscriber data to train third-party AI models.
- No individual-level behavioural prediction products, no covert profiling, no voter profiling and no surveillance modules. These are prohibited uses under the DRMC Ethics Guide.
- No storage of special-category data (health, biometric, political opinion as individual records) except where a client expressly contracts for analysis of material they are lawfully entitled to share, under additional safeguards.

3. GDPR Article 32 checklist: security of processing

Article 32 requires technical and organisational measures appropriate to the risk, including (a) pseudonymisation and encryption, (b) ongoing confidentiality, integrity, availability and resilience, (c) the ability to restore availability after an incident, and (d) a process for regularly testing and evaluating effectiveness. The table below maps AiiPD's measures and their current status.

Control area	AiiPD technical and organisational measure	Status
Encryption in transit	TLS 1.2+ enforced on all web, API and database connections. HSTS enabled. No plaintext transport of credentials or personal data.	**Implemented**
Encryption at rest	Database and object storage encrypted at rest using provider-managed AES-256 (PostgreSQL managed encryption; encrypted blob storage for documents).	**Implemented**
Pseudonymisation	Account identifiers separated from analytical content where feasible; client documents referenced by opaque IDs rather than embedded personal identifiers.	**Partial**
Access control	Role-based access control (RBAC) via the application auth layer (NextAuth). Least-privilege roles. Admin actions logged. No shared accounts.	**Implemented**
Multi-factor authentication	MFA enforced for administrative and developer access to hosting, database and code repositories.	**Partial**
Secrets management	API keys and credentials stored as environment secrets, never in source control. Rotation procedure documented. Separate keys per environment.	**Implemented**
Network security	Managed hosting with provider firewalling; database not exposed to the public internet; API rate limiting.	**Partial**
Confidentiality	Staff and contractor confidentiality obligations; NDA-gated access to client data; data-minimisation by default.	**Implemented**
Integrity	Source provenance and verification status recorded for every evidence record; version control on all reports; named human reviewer before release.	**Implemented**
Availability & resilience	Managed hosting with provider redundancy; automated database backups; documented restore procedure.	**Partial**
Backup & restore	Automated daily backups with point-in-time recovery; periodic restore testing.	**Planned**
Logging & monitoring	Application and access logging; admin action audit trail; alerting on anomalous access.	**Partial**
Vulnerability management	Dependency scanning on the codebase; patch cadence for the application stack; review of third-party libraries.	**Partial**
Testing & evaluation	Periodic internal security review; this baseline reviewed and updated at least annually; penetration test planned before government-facing deployment.	**Planned**
Incident response	Documented breach response and notification procedure aligned to GDPR 72-hour and OAIC Notifiable Data Breaches timelines.	**Partial**
Data processor controls	Written processing terms for client engagements; sub-processor list maintained; client instructions govern client data.	**Partial**

4. ISO/IEC 27001 Annex A coverage

ISO/IEC 27001:2022 defines an Information Security Management System (ISMS) and 93 Annex A controls across four themes: Organisational, People, Physical and Technological. AiiPD has not undertaken certification. The table records self-assessed coverage of the control themes to demonstrate a structured approach and to scope a future certification project.

Annex A theme	AiiPD position	Status
Organisational controls	Information security roles defined (Founder as accountable owner); acceptable use, access control and supplier policies documented; threat intelligence and incident management procedures established.	**Partial**
People controls	Confidentiality obligations for all personnel and contractors; security awareness expectations; screening for roles with data access; defined responsibilities on engagement and exit.	**Partial**
Physical controls	Cloud-hosted infrastructure inherits provider physical security (certified data centres); no on-premise production servers; endpoint security on devices accessing data.	**Implemented**
Technological controls	Encryption, secure authentication, logging, malware protection, secure development practices, backup, network security and data leakage prevention as detailed in section 3.	**Partial**

Path to certification

A realistic ISO 27001 certification path for AiiPD: (1) formalise the ISMS scope and Statement of Applicability; (2) complete the documented policy set; (3) operate the ISMS for a defined period with evidence; (4) Stage 1 and Stage 2 audit by an accredited certification body. This is a 9 to 15 month project and is sequenced to follow first revenue, consistent with the staged roadmap in the investor prospectus.

5. IRAP readiness (Australian government)

The Information Security Registered Assessors Program (IRAP) provides assessment of systems against the Australian Government Information Security Manual (ISM). It is relevant only if AiiPD pursues Australian Government data at higher sensitivity. For local government and standard commercial work it is not required.

AiiPD's IRAP position is readiness, not assessment. The platform's security-by-design measures map to many ISM controls (access control, encryption, logging, personnel security), and hosting on an Australian region of a major cloud provider supports data-sovereignty requirements. A formal IRAP assessment would be commissioned only if and when a specific government engagement at OFFICIAL: Sensitive or above requires it, using a registered IRAP assessor.

- Data sovereignty: production data hosted in Australian cloud regions where government engagement requires it.
- ISM alignment: access control, encryption, audit logging and personnel measures mapped to ISM control families.
- Assessment trigger: commissioned per-engagement when a government client's classification requires it, not maintained speculatively.

6. Australian Privacy Principles alignment

As an Australian organisation handling personal information, AiiPD aligns its practices to the 13 Australian Privacy Principles under the Privacy Act 1988 (Cth). Key positions:

Principle	AiiPD position	Status
APP 1 Open & transparent	Privacy policy published on the website; this baseline available under NDA; clear purpose statements.	Partial
APP 3 Collection	Only personal information reasonably necessary for the function is collected; minimisation by default.	Implemented
APP 5 Notification	Individuals notified at point of collection of purpose and handling.	Partial
APP 6 Use & disclosure	Personal information used only for the purpose collected or directly related purposes; no secondary sale.	Implemented
APP 8 Cross-border	Sub-processors and hosting regions documented; safeguards applied for any offshore processing.	Partial
APP 11 Security	Technical and organisational measures per section 3; reasonable steps to protect and destroy or de-identify when no longer needed.	Partial
APP 12 & 13 Access & correction	Process for individuals to access and correct their personal information on request.	Partial

AiiPD is also alert to the Notifiable Data Breaches scheme: an eligible data breach triggers assessment and, where required, notification to affected individuals and the Office of the Australian Information Commissioner.

7. Privacy Impact Assessment (summary)

Processing activity 1: subscriber and client accounts

Personal data: name, email, organisation, role. Purpose: account management, communication, service delivery. Lawful basis: contract and legitimate interest (GDPR) / necessary for function (APP). Risk: low. Controls: encryption, RBAC, minimisation, access on request. Residual risk: low and acceptable.

Processing activity 2: client-supplied content for analysis

Personal data: variable, may appear in client documents. Purpose: deliver contracted analysis. Role: data processor under client instruction. Risk: medium, depending on content. Controls: NDA-gated access, processing terms, sub-processor control, deletion on completion, no model-training use. Residual risk: medium-low, managed by contract and access control.

Processing activity 3: candidate intelligence products

This activity carries elevated reputational and ethical risk and is therefore governed by explicit prohibitions, not just technical controls. Personal data about candidates is limited to public-source material. The DRMC Ethics Guide prohibits voter profiling, misinformation, smear content and covert persuasion. Outputs are evidence-based local intelligence only, with named human review. Residual risk is controlled by hard prohibited-use boundaries written into every engagement.

Processing activity 4: derived analytical outputs

DRMC and RSC outputs are interpretive, not validated measurement, and are never presented as individual diagnosis or determination. The standard caveat accompanies every output. Risk: low, provided the caveat and human-review controls hold.

8. Governance, dual-use and AI safeguards

AiiPD's security posture is reinforced by ethical governance that is constitutive, not advisory:

- A documented prohibited-use clause in every licence and engagement: no surveillance, no covert profiling, no individual behavioural prediction products, no political manipulation.
- Human-in-the-loop: no automated output becomes a final civic, ethical or regulatory judgement. A named reviewer signs off.
- Separation of current interpretive RSC outputs from any future validated Relational Resonance Metrics, so capability is never overstated.
- Multi-model AI use (Claude, and where contracted other providers) governed by data-handling rules: no client data used for model training; provider data-processing terms reviewed.
- Client education materials explaining methodological limits, community review rights and escalation pathways for sensitive contexts.

9. Assurance roadmap

AiiPD commits to maturing this baseline on the following sequence, aligned to commercial growth:

- Now to 6 months: complete documented policy set; enforce MFA across all admin access; implement automated backup with restore testing; publish privacy policy and data-handling statement.
- 6 to 12 months: formalise the ISMS scope and Statement of Applicability; commission an external penetration test before any government-facing deployment; complete sub-processor register and processing terms.
- 12 months and beyond: pursue ISO/IEC 27001 certification; commission IRAP assessment if a government engagement requires it; annual review and re-test of all controls.

This document is a good-faith self-assessment prepared for due diligence purposes. It is not a certification, audit opinion or regulatory determination. RSC and DRMC outputs are interpretive assessments, not validated measurements. Clancy, L. (2026i). AiiPD, Adelaide.