Kebijakan dan Prosedur Implementasi *Artificial Intelligence (AI)*

DINAS KOMUNIKASI DAN INFORMATIKA

PROVINSI JAWA TENGAH

2025

Versi	1.0
Status	Aktif
Nomor Dokumen	500.12/409/DISKOMINFO/2025
Klasifikasi	Terbatas
Pemilik Dokumen	Dinas Komunikasi dan Informatika Provinsi Jawa Tengah

Lembar Kendali Versi Dokumen

Versi	Tanggal penerbitan	Penulis	Deskripsi perubahan
1.0	31 Oktober 2025	Jakt Albary, S.Kom	Pembuatan awal dokumen

Daftar Isi

Daftar Lampiran

1. Tujuan dan Sasaran

Kebijakan dan Prosedur Implementasi Artificial Intelligence (AI) di Dinas Komunikasi dan Informatika Provinsi Jawa Tengah disusun untuk menetapkan standar proses implementasi teknologi AI yang aman, patuh terhadap regulasi, etis, dan terukur.

Kebijakan ini bertujuan untuk memastikan bahwa setiap solusi berbasis AI, termasuk di dalamnya Natural Language Processing (NLP), Retrieval-Augmented Generation (RAG), visi komputer, dan sistem rekomendasi, memiliki dasar hukum yang jelas, tata kelola data yang baik, kontrol keamanan yang memadai, serta mekanisme evaluasi mutu dan monitoring pasca-produksi yang terstruktur.

Selain itu, kebijakan ini juga dimaksudkan untuk menyediakan kerangka kerja integrasi antara solusi AI dengan aplikasi dan layanan pemerintah daerah agar selaras dengan arsitektur Sistem Pemerintahan Berbasis Elektronik (SPBE) dan prinsip-prinsip Satu Data Indonesia.

2. Ruang Lingkup

Kebijakan dan Prosedur Implementasi Artificial Intelligence (AI) ini berlaku untuk Organisasi Pemerintahan Daerah Provinsi Jawa Tengah yang melakukan kegiatan perencanaan, pengembangan, pengujian, pengoperasian, atau pengawasan terhadap sistem berbasis AI, baik yang diimplementasikan secara lokal (on-premise) maupun melalui layanan komputasi awan (cloud).

Ruang lingkup kebijakan ini mencakup seluruh siklus hidup implementasi AI, mulai dari tahap perencanaan, perancangan, pengembangan, pengujian, penerapan (go-live), operasional, pemantauan, pemeliharaan, hingga penonaktifan sistem.

Kebijakan ini juga mencakup penerapan teknologi AI generatif dan non-generatif, termasuk namun tidak terbatas pada penggunaan model berbasis Retrieval-Augmented Generation (RAG), Natural Language Processing (NLP), visi komputer, serta sistem berbasis pembelajaran mesin lainnya.

3. Tanggung Jawab

- Pemilik Kebijakan (Diskominfo): menetapkan kebijakan, melakukan pengawasan dan audit (A/R).
- Data Owner (OPD sumber data): persetujuan akses data, klasifikasi & kualitas data (A/R).
- Data Steward: kurasi, metadata, kualitas, retensi & arsip (R).
- AI Product Owner: prioritas fitur, persetujuan go-live, indikator kinerja (A/R).
- AI/ML Engineer: arsitektur model, pipeline, evaluasi, MLOps (R).
- Security & Privacy Officer: DPIA, kontrol keamanan, PDP, incident handling (A/R).
- Legal & Compliance: kesesuaian regulasi, kontrak vendor, lisensi (C/A).
- QA/Testing: rencana uji, UAT/BAST, model validation (R).
- Ops/SRE: deployment, monitoring, SLO, incident response (R).

Note: (C: Consulted, R: Responsible, A: Accountable)

4. Referensi

- ISO/IEC 42001:2023 tentang Artificial Intelligence Management System (AIMS),
- Peraturan Menteri Kominfo Nomor 4 Tahun 2016 tentang Organisasi dan Tata Kerja Dinas Kominfo Provinsi/Kabupaten/Kota,
- Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik (SPBE),
- Peraturan Gubernur (Pergub) Provinsi Jawa Tengah Nomor 40 Tahun 2022 tentang Penyelenggaraan Sistem Pemerintahan Berbasis Elektronik (SPBE),
- Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi,
- Strategi Nasional Kecerdasan Artifisial Indonesia 2020–2045,

5. Definisi

5.1. Organisasi & Tata Kelola

- Pemilik Kebijakan (Policy Owner): Unit pada Diskominfo yang berwenang menetapkan, menyetujui, dan mengubah kebijakan ini.
- Pemilik Data (Data Owner): OPD sumber data yang berwenang atas akses, klasifikasi, dan penggunaan data.
- Pengelola Data (Data Steward): Peran kurasi data (metadata, kualitas, retensi/arsip) sesuai arahan Pemilik Data.
- AI Product Owner: Penanggung jawab tujuan produk AI, prioritas fitur, dan keputusan go-live.
- Tim Tata Kelola AI: Tim lintas fungsi yang memverifikasi kepatuhan, keamanan, dan etika penerapan AI.

5.2. Data & Privasi

- Data Pribadi: Setiap data tentang orang perseorangan yang teridentifikasi/teridentifikasi secara langsung atau tidak langsung.
- Data Pribadi Sensitif: Subset data pribadi yang memiliki dampak tinggi (mis. data kesehatan, biometrik).
- PII (Personally Identifiable Information): Informasi yang dapat mengidentifikasi individu (mis. NIK, alamat, nomor telepon).
- Minimisasi Data (Data Minimization): Mengumpulkan/memproses data sebatas yang diperlukan untuk tujuan yang sah.
- Pembatasan Tujuan (Purpose Limitation): Pemrosesan data hanya untuk tujuan yang telah ditetapkan.
- Penyamaran Data (Masking/Pseudonymization): Teknik mengaburkan data agar tidak langsung mengidentifikasi subjek.
- Anonimisasi (Anonymization): Proses menghapus keterkaitan data dengan individu sehingga tidak dapat dikenali kembali.
- Retensi Data (Data Retention): Masa simpan data sesuai ketentuan dan kebutuhan layanan.
- Residensi Data (Data Residency): Lokasi fisik/negara tempat data disimpan/diolah.

5.3. Kerangka Etik & Dampak

- Pernyataan AI yang Bertanggung Jawab (Responsible AI Statement): Dokumen tujuan, manfaat, risiko, dan batasan sistem AI.
- DPIA (Data Protection Impact Assessment): Kajian dampak perlindungan data pribadi atas sistem AI.
- EIA (Ethical Impact Assessment): Kajian dampak etis dan sosial atas sistem AI.
- Human-in-the-Loop (HITL): Keterlibatan manusia dalam keputusan berdampak tinggi.

5.4. Teknologi & Arsitektur

- Kecerdasan Buatan (Artificial Intelligence/AI): Sistem yang melakukan tugas kognitif (memahami bahasa, prediksi, dsb.).
- Model AI/ML (Model): Komponen terlatih dari data untuk menjalankan tugas tertentu.
- Model Bahasa Besar (Large Language Model/LLM): Model yang memproses dan menghasilkan teks alami.
- NLP (Natural Language Processing): Cabang AI untuk pemahaman/pengolahan bahasa alami.
- RAG (Retrieval-Augmented Generation): Teknik generatif yang mengambil sumber referensi lalu menghasilkan jawaban berdasar sumber tersebut.
- Grounding: Praktik memastikan keluaran AI dilengkapi dasar/sumber yang terverifikasi.
- Hallucination: Keluaran AI yang salah/tidak berbasis fakta/sumber.
- API (Application Programming Interface): Mekanisme integrasi antar sistem.
- Integrasi Berbasis Peran/Atribut (RBAC/ABAC): Pengendalian akses berdasarkan peran atau atribut pengguna.
- Embedding: Representasi numerik dari teks untuk pencarian semantik.
- Penyimpanan Vektor (Vector Store): Basis data untuk menyimpan embedding dan metadata.
- BM25: Metode temu-balik kata kunci (lexical retrieval) yang melengkapi pencarian semantik.
- Indeks & Penyegaran Indeks (Index Refresh): Struktur data untuk temu-balik dan proses pembaharuannya (mis. standar T+1 hari kerja).
- Fallback/Safeguard: Mekanisme aman saat sumber tak ditemukan/risiko tinggi (mis. alihkan ke kanal resmi).

5.5. Kualitas, Kinerja, & Operasi

- UAT (User Acceptance Test): Uji penerimaan oleh pengguna/OPD.
- BAST (Berita Acara Serah Terima): Dokumen serah terima setelah uji penerimaan terpenuhi.
- Observability: Kemampuan sistem dipantau melalui log, metrik, dan jejak (tracing).
- SLO/SLA/SLI: Target layanan/komitmen/indikator terukur (mis. ketersediaan 99,5%).
- Latensi p95: 95% permintaan diselesaikan di bawah ambang waktu yang ditentukan.

- Throughput (QPS/RPS): Jumlah permintaan yang diproses per detik.
- Rollback Plan: Rencana kembali ke versi sebelumnya bila rilis baru bermasalah.
- Runbook/Playbook: Panduan langkah teknis penanganan operasional/insiden.
- Go-live/Produksi: Tahap saat sistem mulai dipakai pengguna nyata.
- Canary/Blue-Green Release: Strategi peluncuran bertahap/berpasangan untuk menurunkan risiko.

5.6. Keamanan Informasi

- Security by Design / Privacy by Design: Prinsip merancang keamanan/privasi sejak awal.
- Manajemen Rahasia & Kunci (Secret/KMS): Pengelolaan kredensial dan kunci kriptografi.
- Enkripsi In-Transit/At-Rest: Perlindungan data saat transmisi/penyimpanan.
- Audit Trail: Jejak aktivitas untuk akuntabilitas dan forensik.
- Uji Keamanan (Vulnerability/Penetration Test): Pengujian kelemahan dan eksploitasi terkendali.
- Red Teaming: Pengujian ofensif terkontrol untuk menilai ketahanan sistem.
- Serangan Prompt (Prompt Injection/Jailbreak): Upaya memanipulasi model agar melanggar kebijakan.
- Kebocoran Data (Data Leakage): Terbukanya data kepada pihak yang tidak berwenang.
- Insiden & Tingkat Keparahan (Severity): Kejadian yang mengganggu layanan beserta klasifikasi dampaknya.
- CAPA (Corrective & Preventive Actions): Tindakan korektif dan pencegahan pasca insiden/audit.

5.7. Evaluasi Model & Metrik Mutu (RAG/Generatif)

- Grounded Answer Rate: Persentase jawaban yang menyertakan sumber yang benar.
- Hallucination Rate: Persentase jawaban yang tidak berdasar/faktual.
- Retrieval Hit Rate: Persentase kueri yang berhasil menemukan konteks/sumber yang relevan.
- Faithfulness: Kesesuaian jawaban terhadap sumber yang dirujuk.
- Model/Data/Concept Drift: Perubahan performa karena data/konsep dunia nyata bergeser.
- Model Card / Datacard: Ringkasan terstandar tentang model/dataset (tujuan, data, batasan, risiko, evaluasi).

5.8. Praktik Rekayasa & Siklus Hidup

- MLOps: Praktik end-to-end pengembangan, deployment, dan pemantauan model AI/ML.
- Manajemen Perubahan (Change Management): Proses perencanaan, persetujuan, dan dokumentasi perubahan.
- Versi (Versioning/SemVer): Penomoran terstruktur untuk melacak perubahan perangkat lunak/model/dataset.

- Kepatuhan (Compliance): Kesesuaian terhadap regulasi, standar, dan kebijakan yang berlaku.

6. Peninjauan Dokumentasi

Dokumen ini harus ditinjau paling sedikit 1 (satu) kali dalam 1 (satu) tahun atau apabila terdapat perubahan signifikan dalam proses bisnis organisasi untuk menjamin kesesuaian dan kecukupan dengan kondisi terkini. Setiap perubahan terhadap dokumen ini harus didokumentasikan dan disetujui melalui proses manajemen transformasi layanan.

7. Kebijakan Umum

Dalam rangka memastikan implementasi teknologi Artificial Intelligence (AI) di lingkungan Pemerintah Provinsi Jawa Tengah berjalan secara aman, layak, transparan, dan sesuai ketentuan hukum yang berlaku, maka Dinas Komunikasi dan Informatika Provinsi Jawa Tengah menetapkan kebijakan umum sebagai berikut:

- **Aspek Legal dan Etika**
  Setiap proyek AI wajib memiliki dasar hukum yang jelas serta disertai dengan *Data Protection Impact Assessment (DPIA)* dan *Responsible AI Statement* yang menjelaskan tujuan, manfaat, risiko, serta batasan penggunaan sistem AI.

- **Privacy by Design**
  Penerapan prinsip *Privacy by Design* dilakukan dengan memastikan bahwa setiap sistem AI mengutamakan perlindungan data pribadi melalui minimisasi data, pembatasan tujuan pemrosesan (*purpose limitation*), pengendalian akses, enkripsi, dan pencatatan aktivitas (*audit trail*).

- **Security by Design**
  Keamanan sistem menjadi prioritas utama melalui pelaksanaan *threat modeling*, pengujian keamanan, *system hardening*, manajemen kunci kriptografi, serta rotasi rahasia (*secret rotation*) secara berkala.

- **Transparansi dan Kemampuan Penjelasan (Explain Ability & Grounding)**
  Untuk sistem AI generatif atau berbasis *Retrieval-Augmented Generation (RAG)*, setiap keluaran sistem yang bersifat substantif harus memiliki keterlacakan sumber (*traceable source*), termasuk penyediaan fitur *view source* atau sitasi referensi.

- **Peran Manusia dalam Pengambilan Keputusan (Human-in-the-Loop)**
  Dalam hal sistem AI digunakan untuk pengambilan keputusan yang berdampak tinggi terhadap layanan publik seperti sosial, kesehatan, dan kependudukan, hasil keluaran AI wajib diverifikasi oleh petugas manusia yang berwenang.

- **Tata Kelola Data (Data Governance)**
  Setiap dataset yang digunakan dalam pengembangan dan pengoperasian AI harus memiliki penanggung jawab data (*data owner*) dan pengelola data (*data steward*), serta

diklasifikasikan berdasarkan sensitivitas, masa retensi, dan hak akses yang diatur dengan mekanisme berbasis peran (*RBAC/ABAC*).

- **Penggunaan Model dan Layanan Eksternal (Vendor/Model Eksternal)**
  Penggunaan model, API, atau layanan AI dari pihak ketiga harus melalui proses evaluasi terhadap lisensi, lokasi penyimpanan data (*data residency*), batas penggunaan (*rate limit*), biaya, *Service Level Agreement (SLA)*, serta rencana penghentian layanan (*termination plan*).

Kebijakan umum ini menjadi acuan bagi seluruh unit kerja dan mitra yang terlibat dalam perencanaan, pengembangan, dan pengoperasian solusi AI agar penerapannya sejalan dengan prinsip SPBE, arsitektur data pemerintah, serta kebijakan nasional terkait perlindungan data pribadi dan etika kecerdasan buatan.

8. Metodologi Proses

Metodologi implementasi Artificial Intelligence (AI) di lingkungan Pemerintah Provinsi Jawa Tengah menggunakan pendekatan **Model Hirarki atau *Framework Layered***, yang menggambarkan keterkaitan antara tata kelola, keamanan, proses implementasi, serta pemantauan dan evaluasi secara berjenjang dan berkesinambungan.

Gambar 1. Metode Framework Layered

Setiap lapisan dalam model ini memiliki fungsi dan tanggung jawab yang saling melengkapi, sehingga membentuk suatu siklus pengelolaan AI yang utuh, akuntabel, dan terukur. Lapisan-lapisan tersebut meliputi:

8.1. Lapisan Tata Kelola & Kepatuhan

Lapisan tertinggi yang berperan dalam menetapkan arah kebijakan, standar, regulasi, dan prinsip etika penggunaan AI. Tata kelola ini memastikan seluruh kegiatan

implementasi AI berjalan sesuai dengan ketentuan peraturan perundang-undangan, prinsip SPBE, perlindungan data pribadi, dan standar internasional seperti ISO/IEC 42001.

8.2. Lapisan Keamanan & Privasi

Lapisan ini memastikan bahwa setiap proses dan sistem AI memenuhi prinsip *Security by Design* dan *Privacy by Design*. Meliputi pengelolaan risiko keamanan siber, kontrol akses, audit trail, enkripsi data, serta mekanisme deteksi dan mitigasi pelanggaran privasi.

8.3. Lapisan Metodologi Implementasi

Lapisan inti yang mencakup enam tahapan utama dalam siklus hidup AI, yaitu:

a. Perencanaan

Pada tahap perencanaan, dilakukan identifikasi *use-case* yang sesuai dengan kebutuhan pelayanan publik dan strategi transformasi digital Pemerintah Provinsi Jawa Tengah. Kegiatan utama meliputi:

- Penyusunan use-case dan benefit case yang menjelask) yangan nilai tambah penerapan AI terhadap efektivitas pelayanan publik
- Analisis risiko mencakup aspek operasional, keamanan, hukum, dan reputasi.
- Penyusunan Data Protection Impact Assessment (DPIA) awal untuk memastikan kesesuaian dengan kebijakan perlindungan data pribadi.
- Kajian kelayakan teknis dan sumber daya (feasibility check mencakup latensi, biaya, ketersediaan data, dan kesiapan infrastruktur.

Keputusan untuk melanjutkan atau menunda implementasi dituangkan dalam dokumen *Go/No-Go Decision* yang disetujui oleh Pemilik Kebijakan dan *Data Owner*.

b. Desain dan Arsitektur

Tahap ini mencakup perancangan arsitektur sistem AI yang meliputi arsitektur logis dan fisik, alur data (*data flow*), integrasi antar sistem melalui API, kontrol akses, serta mekanisme pemantauan (*observability*).

Untuk sistem berbasis *Retrieval-Augmented Generation (RAG)*, rancangan harus memenuhi ketentuan sebagai berikut:

- Menggunakan sumber data resmi pemerintah seperti dokumen kebijakan, SOP, regulasi, atau FAQ.
- Melakukan proses *data cleaning*, *chunking*, dan *normalisasi* untuk menjaga kualitas data.
- Melindungi data pribadi dengan mekanisme penghapusan atau penyamaran (*masking/omission*) sesuai ketentuan privasi.

- Menggunakan metode pengindeksan hibrida (*vector store* dan *BM25*) dengan metadata yang memuat asal dokumen, versi, dan tanggal.
- Menjamin transparansi hasil keluaran dengan mencantumkan sitasi atau sumber data (*grounded answer*).
- Menyediakan mekanisme *fail-safe* atau *fallback* agar sistem tidak memberikan informasi yang menyesatkan.

c. Pengembangan

Tahap ini dilakukan dengan menerapkan prinsip *secure coding* dan tata kelola pengembangan perangkat lunak yang baik. Aspek utama yang diatur antara lain:

- Penerapan standar penulisan kode dan panduan prompt engineering.
- Pengelolaan rahasia sistem (secret management) dan penerapan configuration as code.
- Pencatatan versi dataset, data card, dan model card yang menjelaskan sumber, tanggal, serta potensi bias.
- Pelaksanaan pengujian unit dan integrasi, termasuk kerangka evaluasi otomatis (evaluation harness).

d. Pengujian dan Validasi

Sebelum implementasi dioperasikan, dilakukan pengujian dan validasi menyeluruh untuk menjamin mutu dan keamanan sistem AI. Cakupan pengujian meliputi:

- Kualitas model dan jawaban, meliputi tingkat ketepatan (*grounded answer rate*), kesalahan faktual (hallucination rate), dan tingkat keberhasilan pengambilan data (*retrieval hit rate*).
- Performa teknis, meliputi waktu tanggap (latency), kapasitas proses, dan uji beban.
- Keamanan dan privasi, termasuk pengujian terhadap prompt injection, data leakage, dan pemindaian data pribadi.
- Kepatuhan regulasi, mencakup ketentuan Undang-Undang Perlindungan Data Pribadi, SPBE, serta kebijakan kearsipan.

Dokumentasi hasil uji dituangkan dalam *User Acceptance Test (UAT)* dan *Berita Acara Serah Terima (BAST)* dengan standar kelulusan minimal 95%.

e. Operasionalisasi (Go-live dan Produksi)

Tahap operasionalisasi dilakukan setelah sistem dinyatakan layak jalan. Pengelolaan sistem mencakup:

- Persetujuan change control, rencana peluncuran (rollout plan), serta rencana pemulihan (rollback plan).

- Penerapan observability dashboard untuk memantau latensi, kesalahan, tingkat penggunaan, dan biaya.
- Penetapan Service Level Objective (SLO) dan Service Level Agreement (SLA) yang mencakup ketersediaan sistem minimal 99,5% dan pembaruan indeks data maksimal T+1 hari kerja.
- Penyusunan runbook insiden yang memuat prosedur penanganan gangguan, eskalasi, serta komunikasi kepada pemangku kepentingan.

f. Pemeliharaan dan Penghentian Layanan

Sistem AI yang telah beroperasi wajib dikelola secara berkelanjutan dengan memperhatikan aspek pemeliharaan, peningkatan mutu, dan keamanan. Kegiatan mencakup pembaruan data, deteksi *model drift*, penyesuaian kebijakan keamanan, serta evaluasi performa berkala.

Apabila sistem dihentikan, dilakukan prosedur *decommissioning* dan pengarsipan data sesuai dengan ketentuan kearsipan pemerintah.

8.4. Lapisan Pemantauan & Evaluasi

Lapisan terakhir yang memastikan efektivitas dan kepatuhan sistem AI setelah dioperasikan. Meliputi kegiatan monitoring performa, audit berkala, evaluasi dampak sosial dan etis, serta pelaporan hasil kepada pemangku kepentingan untuk mendukung perbaikan berkelanjutan (continuous improvement).

9. Mekanisme Pengendalian dan Evaluasi Implementasi AI

Mekanisme pengendalian dan evaluasi implementasi Artificial Intelligence (AI) di lingkungan Pemerintah Provinsi Jawa Tengah bertujuan untuk memastikan bahwa seluruh kegiatan pengembangan dan penerapan AI berjalan sesuai dengan ketentuan kebijakan, regulasi, serta prinsip-prinsip tata kelola pemerintahan yang baik (*good governance*).

Kegiatan pengendalian dan evaluasi dilakukan secara terstruktur, terukur, dan berkelanjutan melalui beberapa tahapan berikut:

9.1. Pengendalian Implementasi (Control Mechanism)

Pengendalian dilakukan untuk menjamin bahwa sistem AI dikembangkan dan dioperasikan sesuai dengan prinsip keamanan, etika, serta kepatuhan hukum yang berlaku. Pengendalian ini mencakup:

a. Pengendalian Kebijakan dan Tata Kelola

Setiap proyek AI wajib memiliki *Dokumen Kebijakan Internal*, *Responsible AI Statement*, serta persetujuan tertulis dari Pemilik Kebijakan (Policy Owner) dan Penanggung Jawab Data (Data Owner).

b. Pengendalian Teknis dan Keamanan

   Meliputi penerapan *access control*, enkripsi data, manajemen rahasia (*secret management*), *vulnerability scanning*, serta pengujian keamanan (*penetration testing*) secara berkala.

c. Pengendalian Etika dan Privasi

   Setiap model AI wajib melalui *Data Protection Impact Assessment (DPIA)* dan *Ethical Impact Assessment (EIA)* sebelum diterapkan, untuk memastikan tidak terjadi pelanggaran privasi, bias, atau dampak sosial yang merugikan.

d. Pengendalian Akses dan Akuntabilitas

   Pemberian akses dilakukan berbasis peran (*role-based access control / RBAC*) atau atribut (*attribute-based access control / ABAC*), serta dilengkapi dengan audit trail yang terdokumentasi.

9.2. Evaluasi Implementasi (Evaluation Mechanism)

Evaluasi bertujuan untuk menilai efektivitas, efisiensi, dan kepatuhan dari sistem AI yang telah diimplementasikan. Evaluasi dilaksanakan secara berkala oleh tim lintas fungsi yang ditetapkan melalui keputusan Kepala Dinas Komunikasi dan Informatika Provinsi Jawa Tengah. Evaluasi dilakukan dengan memperhatikan aspek-aspek berikut:

a. Evaluasi Kinerja Teknis

   Pengukuran performa model berdasarkan metrik seperti *accuracy*, *precision*, *recall*, *latency*, dan *robustness* terhadap data baru atau masukan ekstrem.

b. Evaluasi Kualitas Jawaban dan Keandalan Model

   Untuk sistem AI generatif (termasuk RAG), dilakukan penilaian *grounded answer rate*, *hallucination rate*, serta *faithfulness score* secara periodik.

c. Evaluasi Kepatuhan Regulasi dan Keamanan Data

   Pemeriksaan terhadap penerapan regulasi Perlindungan Data Pribadi (UU No. 27 Tahun 2022), SPBE, serta pedoman internal keamanan informasi (ISO/IEC 27001 dan 42001).

d. Evaluasi Dampak Etis dan Sosial

   Analisis potensi dampak sosial, diskriminasi, atau penyalahgunaan model AI terhadap pelayanan publik dan persepsi masyarakat.

e. Evaluasi Ekonomi dan Efisiensi Operasional

f. Penilaian manfaat biaya (*cost-benefit analysis*) terhadap sumber daya komputasi, lisensi, serta dampak penghematan waktu layanan publik.

9.3. Pelaporan dan Tindak Lanjut

Hasil pengendalian dan evaluasi wajib dituangkan dalam Laporan Evaluasi Implementasi AI, yang memuat:

a. Temuan dan rekomendasi perbaikan,
b. Status kepatuhan terhadap kebijakan dan regulasi,

c. Rencana tindakan korektif dan pencegahan (*Corrective and Preventive Actions – CAPA*),
d. Jadwal pelaksanaan tindak lanjut.

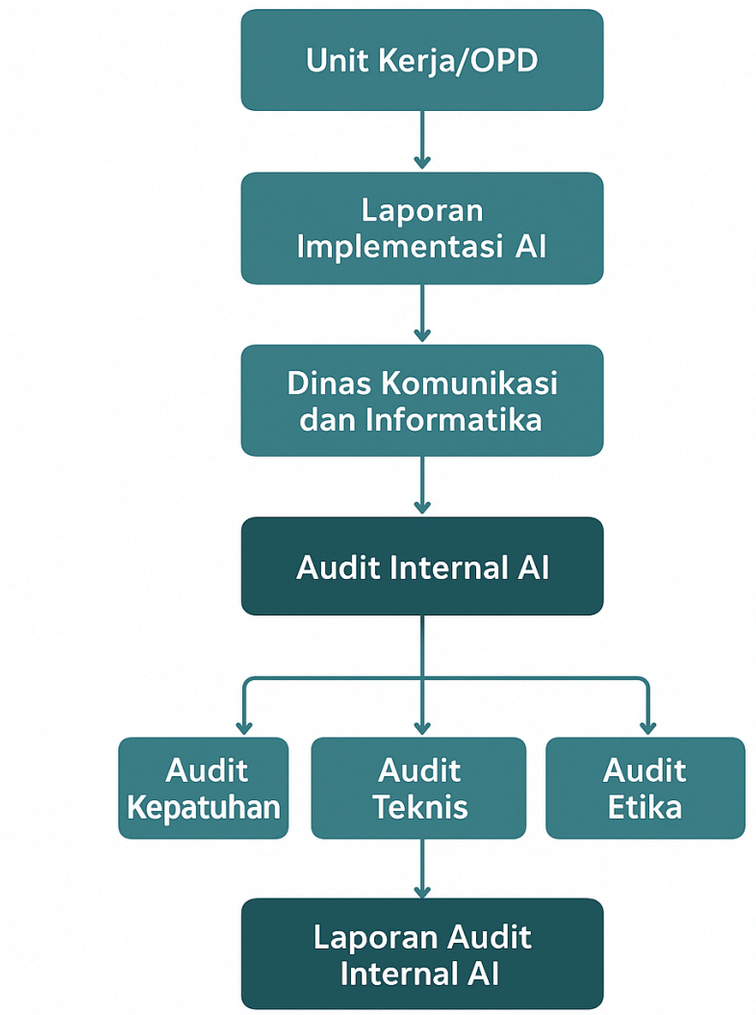
Laporan disampaikan kepada Kepala Dinas Komunikasi dan Informatika Provinsi Jawa Tengah dan dilaporkan secara agregat kepada Sekretaris Daerah sebagai bagian dari Laporan Evaluasi SPBE Tahunan.

9.4. Continuous Improvement

Sebagai bagian dari siklus hidup AI, hasil evaluasi dijadikan dasar dalam peningkatan berkelanjutan (*continuous improvement*) terhadap kebijakan, prosedur teknis, maupun model AI yang digunakan. Setiap perbaikan terdokumentasi dalam *register perubahan* yang disetujui oleh Pemilik Kebijakan.

10. Pelaporan dan Audit Implementasi AI

Mekanisme pelaporan dan audit implementasi kecerdasan buatan (AI) bertujuan untuk memastikan bahwa seluruh kegiatan perencanaan, pengembangan, dan pengoperasian sistem AI berjalan sesuai dengan kebijakan, prinsip tata kelola, dan ketentuan peraturan perundang-undangan.



Gambar 2. diagram alur audit dan pelaporan AI

Alur pelaporan dan audit dapat digambarkan dalam empat tahap utama sebagai berikut:

10.1. Mekanisme Pelaporan

a. Pelaporan Unit Pengelola Sistem AI

Setiap perangkat daerah atau unit kerja yang mengembangkan dan/atau mengoperasikan sistem berbasis AI wajib menyampaikan laporan pelaksanaan kegiatan secara berkala kepada Dinas Komunikasi dan Informatika Provinsi Jawa Tengah selaku koordinator tata kelola AI.

Laporan dimaksud paling sedikit memuat:

- Status pelaksanaan (tahap pengembangan, uji coba, atau operasional);
- Capaian kinerja sistem (akurasi, keandalan, performa, serta hasil evaluasi teknis);
- Catatan kejadian insiden (misalnya kesalahan sistem, gangguan layanan, kebocoran data, atau bias keluaran);
- Langkah mitigasi dan rencana perbaikan yang telah atau akan dilaksanakan.

b. Kompilasi dan Review oleh Tim Tata Kelola AI

Tim Tata Kelola AI pada Dinas Komunikasi dan Informatika melakukan verifikasi terhadap kelengkapan, konsistensi, dan validitas laporan. Hasil verifikasi digunakan untuk menilai tingkat kepatuhan terhadap prinsip tata kelola, keamanan informasi, perlindungan data pribadi, dan etika penggunaan AI.

Berdasarkan hasil review, tim dapat memberikan rekomendasi teknis maupun administratif untuk peningkatan kualitas penerapan AI.

10.2. Mekanisme Audit

a. Audit Internal

Audit internal dilaksanakan oleh unit pengawasan fungsional (Inspektorat Provinsi atau unit pengawasan internal lainnya) secara periodik dan/atau insidentil terhadap penerapan sistem AI. Audit ini mencakup aspek:

- Kepatuhan terhadap kebijakan, standar, dan pedoman implementasi AI;
- Keamanan data dan informasi sesuai ketentuan Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi;
- Penerapan standar internasional seperti ISO/IEC 42001:2023 tentang Sistem Manajemen Kecerdasan Buatan (Artificial Intelligence Management System);
- Efektivitas pengendalian internal dan mitigasi risiko operasional.

b. Pelaporan Hasil Audit

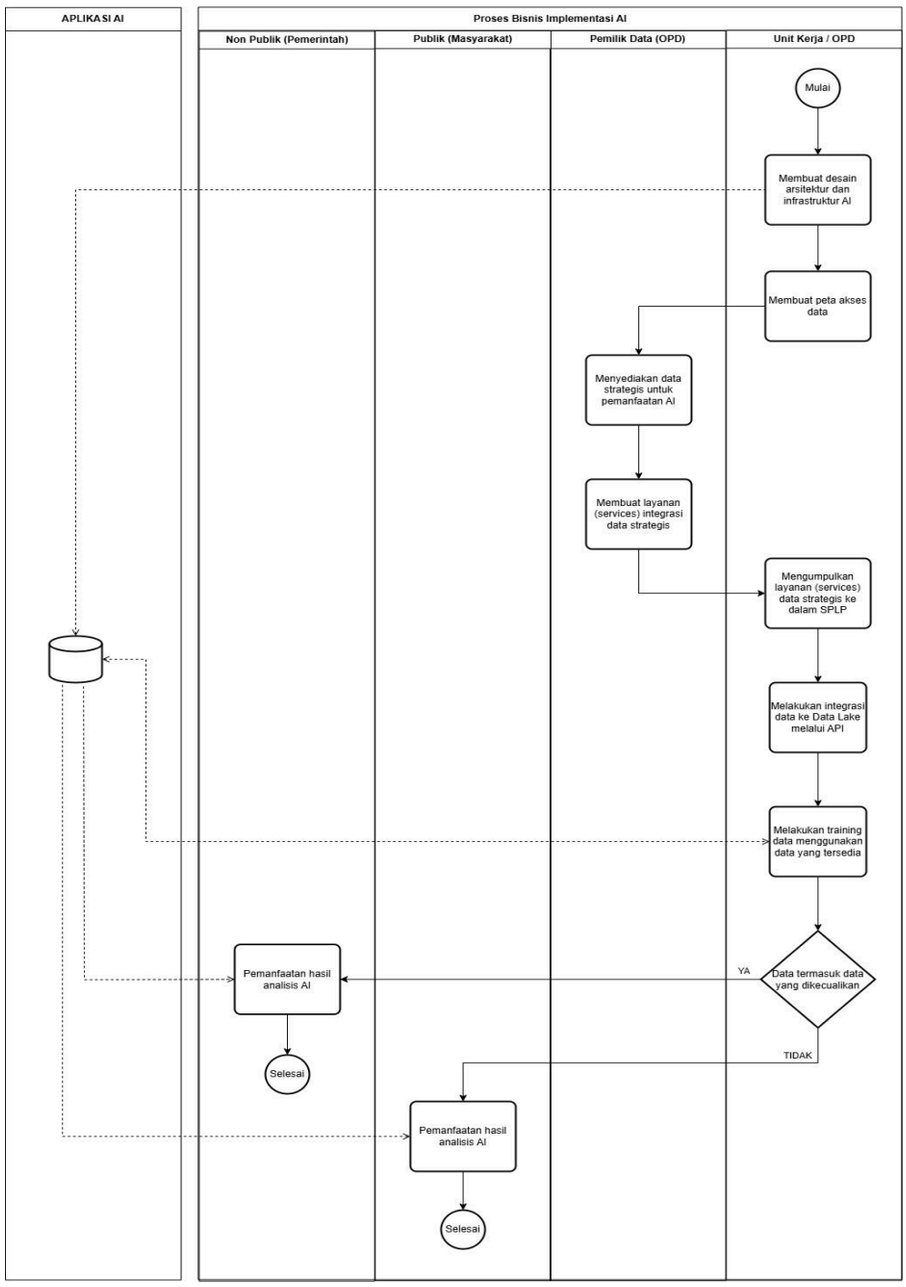
Hasil audit dituangkan dalam laporan resmi yang memuat temuan, analisis risiko, serta rekomendasi perbaikan dan peningkatan. Laporan hasil audit disampaikan kepada Kepala Dinas Komunikasi dan Informatika Provinsi Jawa Tengah untuk diteruskan kepada perangkat daerah terkait guna pelaksanaan tindak lanjut.

c. Tindak Lanjut dan Evaluasi Berkala

Perangkat daerah wajib menyusun dan melaporkan rencana aksi (*action plan*) atas rekomendasi hasil audit.

Dinas Komunikasi dan Informatika melakukan evaluasi pelaksanaan tindak lanjut secara berkala sekurang-kurangnya satu kali dalam satu tahun sebagai bagian dari proses *continuous improvement* penerapan sistem AI di lingkungan Pemerintah Provinsi.

11. PROSEDURE



Semarang, 31 Oktober 2025

KEPALA DINAS KOMUNIKASI DAN INFORMATIKA
PROVINSI JAWA TENGAH

AGUNG HARIYADI, SE, MM
Pembina Utama Muda
NIP. 19701202 199003 1 002

LAMPIRAN 1 - Template DPIA (ringkas)

Data Protection Impact Assessment (DPIA)

Aspek	**Deskripsi**
Nama Proyek AI	Pengembangan Antarmuka AI (NLP + RAG) di Superapps JNN
Data yang Diproses	Teks pengaduan, dokumen publik, metadata pengguna (tanpa PII sensitif)
Risiko Privasi	Kebocoran PII, akses tidak sah, bias pada jawaban
Dampak	Kerugian reputasi, pelanggaran hukum (UU PDP), kepercayaan publik menurun
Mitigasi	Masking PII, enkripsi data in-transit & at-rest, RBAC/ABAC, audit log
Residual Risk	Rendah–Sedang
Persetujuan	Ditandatangani oleh Data Owner & Privacy Officer

LAMPIRAN 2 - Register Sistem AI

Template / Contoh Register Sistem AI

ID	Nama Sistem	Department	Tipe AI	Use Case	Risk Level	Data Sources	Status	Owner	Last Assessment
AI-001	Chatbot Pelayanan	Humas	NLP	Customer Service	Medium	FAQ Database, Chat Logs	Production	Kepala Humas	2024-10-01
AI-002	Fraud Detection	Pajak	Classification	Fraud Detection	High	Tax Returns, Transaction Data	Production	Kepala IT	2024-09-15
AI-003	Document OCR	Administrasi	Computer Vision	Document Digitization	Low	Scanned Documents	Pilot	Kepala Arsip	2024-10-15

LAMPIRAN 3 - Template Model Card & Data Card

a) Model Card (contoh)

Aspek	**Deskripsi**
Nama Model	IndoNLP-RAG-v1
Tujuan	Menjawab pertanyaan layanan publik berbasis teks Bahasa Indonesia
Data Latih	Dokumen publik JNN, FAQ OPD, dataset open Bahasa Indonesia
Batasan	Tidak boleh dipakai untuk keputusan hukum/kesehatan
Risiko Bias	Bahasa gaul tidak selalu dikenali
Evaluasi	Grounded answer rate 95%, hallucination rate ≤ 3%
Versi	1.0 (Maret 2025)

b) Data Card (contoh)

Aspek	**Deskripsi**
Nama Dataset	FAQ SP4N-LaporGub & Regulasi Pemprov
Sumber	Dokumen resmi, API OPD, website pemprov
Periode Data	2019–2025
Cakupan	35 Kabupaten/Kota Jawa Tengah
Akses	Hanya admin terverifikasi
Lisensi	Internal Pemprov
Quality Checks	Deduplication, cleaning, PII masking

LAMPIRAN 4 - Checklist UAT/BAST AI

User Acceptance Test (UAT) & Berita Acara Serah Terima (BAST)

No	Skenario Uji	Lulus (✓ / ✗)	Catatan
1	AI bisa menjawab “cek pajak motor B 1234 XYZ” dengan sitasi resmi		
2	AI menolak kueri dengan PII tanpa izin (contoh: NIK)		
3	AI menjawab “cara daftar lowongan kerja” dengan akurat		
4	Latensi p95 ≤ 2,5 detik saat uji beban 100 QPS		
5	Fallback “tidak ditemukan” diarahkan ke kanal resmi		
6	Grounded answer rate ≥ 95%		
7	Hallucination rate ≤ 3%		

LAMPIRAN 5 - Matriks Risiko & Risk Register

PANDUAN PENGGUNAAN FORM

Form ini digunakan untuk:

1. Identifikasi risiko baru dalam sistem AI Chatbot Mas & Mbak
2. Update risiko existing dengan informasi terkini
3. Track mitigasi actions dan monitoring progress
4. Dokumentasi audit trail untuk compliance

Instruksi Pengisian:

1. Isi semua field yang bertanda **[REQUIRED]**
2. Field optional boleh kosong jika tidak relevan
3. Gunakan rating scale yang sudah disediakan
4. Tanggal format: **DD-MM-YYYY**
5. Kirimkan ke Risk Manager setelah selesai

FORM: RISK IDENTIFICATION & REGISTRATION

a. Identifikasi Risiko

Field	Input	Format
Risk ID [REQUIRED]	R-JNN-[Category]-[Number]	Text (Auto-generated)
Risk Title [REQUIRED]	_____	Max 80 characters
Risk Category [REQUIRED]	[ ] Technical [ ] Operational [ ] Security/Privacy [ ] Governance [ ] Other: _____	Dropdown
Severity/Priority [REQUIRED]	[ ] Critical [ ] High [ ] Medium [ ] Low	Selection
Date Identified [REQUIRED]	_____	DD-MM-YYYY
Identified By [REQUIRED]	_____	Name & Title
Risk Owner [REQUIRED]	_____	Name & Department
Risk Owner Contact	Email: _____ Ph: _____	Email/Phone

b. Deskripsi Risiko

RISK DESCRIPTION & CONTEXT

```
Jelaskan risiko secara detail dalam 3–5 kalimat:

Risiko:
_____________________________________________________________________
_____________________________________________________________________
_____________________________________________________________________
_____________________________________________________________________

Konteks/Latar Belakang:
_____________________________________________________________________
_____________________________________________________________________
_____________________________________________________________________

Penyebab Potensial:
_____________________________________________________________________
_____________________________________________________________________

Dampak Potensial:
_____________________________________________________________________
_____________________________________________________________________
_____________________________________________________________________
```

RISK TRIGGER / KONDISI

```
Kondisi apa yang akan menyebabkan risiko ini terjadi?

[ ] System failure              [ ] Data quality issue
[ ] Security breach             [ ] Human error
[ ] Regulatory change          [ ] External event
[ ] Natural disaster           [ ] User behavior
[ ] Vendor/supplier issue      [ ] Lainnya: _________

Penjelasan:
_____________________________________________________________________
_____________________________________________________________________
```

c. Penilaian Probabilitas

Risk Score	Risk Level	Action Required
1-5	**LOW**	Monitor regularly
6-11	**MEDIUM**	Action within 6 months
12-18	**HIGH**	Priority action within 3 months
19-25	**CRITICAL**	Immediate action required

d. Penilaian Dampak

```
Seberapa besar dampak jika risiko terjadi?

Dampak pada berbagai dimensi:

1. OPERATIONAL IMPACT
   [ ] Negligible – Tidak ada gangguan
   [ ] Minor     – Gangguan kecil <1 jam
   [ ] Moderate  – Gangguan 1–8 jam
   [ ] Major     – Gangguan 1–3 hari
   [ ] Critical  – Gangguan >3 hari

2. FINANCIAL IMPACT
   [ ] Negligible – Rp 0–10 juta
   [ ] Minor     – Rp 10–50 juta
   [ ] Moderate  – Rp 50–200 juta
   [ ] Major     – Rp 200–500 juta
   [ ] Critical  – Rp >500 juta

3. REPUTATIONAL IMPACT
   [ ] Negligible – Tidak ada dampak reputasi
   [ ] Minor     – Dampak terbatas ke internal
   [ ] Moderate  – Dampak ke media lokal
   [ ] Major     – Dampak ke media nasional
   [ ] Critical  – Dampak internasional, kehilangan kepercayaan

4. LEGAL/COMPLIANCE IMPACT
   [ ] None      – Tidak ada implikasi legal
   [ ] Minor     – Warning dari regulator
   [ ] Moderate  – Administrative penalty
   [ ] Major     – Financial penalty + legal action
   [ ] Critical  – Criminal liability

5. PUBLIC SAFETY IMPACT
   [ ] None      – Tidak ada dampak keselamatan
   [ ] Minor     – Minimal risk to few people
   [ ] Moderate  – Risk ke puluhan orang
   [ ] Major     – Risk ke ratusan orang
   [ ] Critical  – Risk ke jutaan orang

Pilih Impact Level Overall:
[ ] NEGLIGIBLE (Level 1)
[ ] MINOR (Level 2)
[ ] MODERATE (Level 3)
[ ] MAJOR (Level 4)
[ ] CRITICAL (Level 5)

Impact Score: _____ (1–5)

Deskripsi Dampak Terperinci:
_____
_____
_____
```

e. Penilaian Risiko

```
Risk Score = Probability Score × Impact Score

Probability Score:    _____ (1–5)
Impact Score:         _____ (1–5)
_____________________________________
RISK SCORE:           _____ (1–25)

Risk Level:
[ ] CRITICAL   (Score 20–25)  – Immediate action required
[ ] HIGH       (Score 12–19)  – Priority action needed
[ ] MEDIUM     (Score 6–11)   – Action required within 6 months
[ ] LOW        (Score 1–5)    – Monitor, action if circumstances change

Risk Appetite: [ ] ACCEPTABLE   [ ] TOLERABLE   [ ] UNACCEPTABLE
```

f. Eksisting Kontrol dan Mitigasi

```
Kontrol/mitigasi apa yang sudah ada untuk mengurangi risiko?

CONTROL 1: _____________________________
Effectiveness: [ ] Highly Effective (80–100%)
               [ ] Effective (60–80%)
               [ ] Partially Effective (40–60%)
               [ ] Minimally Effective (20–40%)
               [ ] Ineffective (0–20%)

CONTROL 2: _____________________________
Effectiveness: [ ] Highly Effective (80–100%)
               [ ] Effective (60–80%)
               [ ] Partially Effective (40–60%)
               [ ] Minimally Effective (20–40%)
               [ ] Ineffective (0–20%)

CONTROL 3: _____________________________
Effectiveness: [ ] Highly Effective (80–100%)
               [ ] Effective (60–80%)
               [ ] Partially Effective (40–60%)
               [ ] Minimally Effective (20–40%)
               [ ] Ineffective (0–20%)

CONTROL 4: _____________________________
Effectiveness: [ ] Highly Effective (80–100%)
               [ ] Effective (60–80%)
               [ ] Partially Effective (40–60%)
               [ ] Minimally Effective (20–40%)
               [ ] Ineffective (0–20%)

Overall Control Effectiveness: _____ % (Average)

Gap Analysis – Kontrol apa yang masih diperlukan?
_____________________________________________________________________
_____________________________________________________________________
```

Skala Penilaian dan Definisi

a. Skala Probabilitas

Rating	Range	Definition
VERY LOW	1-10%	Extremely unlikely to occur
LOW	11-30%	Unlikely to occur
MEDIUM	31-60%	May occur
HIGH	61-80%	Likely to occur
VERY HIGH	81-100%	Very likely to occur

b. Skala Dampak

Rating	Definition
1 - NEGLIGIBLE	Minimal business impact, easily recoverable
2 - MINOR	Limited impact, recoverable within days
3 - MODERATE	Moderate impact, affects operations for weeks
4 - MAJOR	Severe impact, affects organization significantly
5 - CRITICAL	Catastrophic impact, threatens viability

c. Matriks Skor Risiko

Rating	Definition
1 - NEGLIGIBLE	Minimal business impact, easily recoverable
2 - MINOR	Limited impact, recoverable within days
3 - MODERATE	Moderate impact, affects operations for weeks
4 - MAJOR	Severe impact, affects organization significantly
5 - CRITICAL	Catastrophic impact, threatens viability

d. Klasifikasi Tingkat Risiko

Risk Score	Risk Level	Action Required
1-5	**LOW**	Monitor regularly
6-11	**MEDIUM**	Action within 6 months
12-18	**HIGH**	Priority action within 3 months
19-25	**CRITICAL**	Immediate action required