Kebijakan Kecerdasan Artifisial Yang Bertanggung Jawab
(*Responsible Artificial Intelligence Policy*)
PT Pupuk Iskandar Muda

PT Pupuk Iskandar Muda ("Perusahaan") berkomitmen memanfaatkan kecerdasan artifisial (*Artificial Intelligence*/AI) secara aman, etis, transparan, dan dapat dipertanggungjawabkan, dengan manusia tetap memegang kendali atas setiap keputusan penting. Pemanfaatan AI diarahkan untuk meningkatkan nilai tambah bisnis, efisiensi operasional, dan daya saing Perusahaan, dengan tetap mengutamakan keselamatan proses, keamanan informasi, perlindungan data, kepatuhan hukum, serta komitmen *Environmental, Social, and Governance* (ESG) Perusahaan.

PT Pupuk Iskandar Muda ("the Company") is committed to using artificial intelligence (AI) in a safe, ethical, transparent, and accountable manner, with humans remaining in control of every important decision. The use of AI is directed at enhancing business value, operational efficiency, and the Company's competitiveness, while prioritizing process safety, information security, data protection, legal compliance, and the Company's Environmental, Social, and Governance (ESG) commitments.

Kebijakan ini bertujuan memastikan pemanfaatan AI memberi nilai tambah bagi bisnis tanpa mengorbankan keselamatan, keamanan informasi, perlindungan data, dan kepatuhan hukum. Kebijakan berlaku untuk seluruh sistem dan layanan AI yang digunakan atau dikembangkan dalam kegiatan Perusahaan, baik melalui langganan, kontrak, maupun pengembangan internal, di seluruh lokasi operasional, serta mengikat seluruh insan Perusahaan, peserta magang, dan pihak ketiga yang diberi akses.

This Policy aims to ensure that the use of AI adds value to the business without compromising safety, information security, data protection, and legal compliance. It applies to all AI systems and services used or developed in the Company's activities, whether through subscription, contract, or internal development, across all operational locations, and binds all Company personnel, interns, and third parties granted access.

Sejalan dengan sentralisasi teknologi informasi di lingkungan Pupuk Indonesia Group, Kebijakan ini diterapkan selaras dengan komitmen *Responsible Artificial Intelligence* PT Pupuk Indonesia (Persero), Pedoman Sistem Manajemen Keamanan Informasi No. PI-TIN-PD-005, dan Prosedur Keamanan Teknologi Informasi No. PI-TIN-PR-010. Kebijakan ini menjadi payung bagi prosedur turunan terkait pengelolaan AI; apabila terdapat perbedaan, ketentuan Kebijakan ini yang berlaku sepanjang tidak bertentangan dengan ketentuan Pupuk Indonesia (Persero) selaku Pemegang Saham.

In line with the centralization of information technology across Pupuk Indonesia Group, this Policy is applied in alignment with the Responsible Artificial Intelligence commitment of PT Pupuk Indonesia (Persero), the Information Security Management System Guidelines No. PI-TIN-PD-005, and the Information Technology Security Procedure No. PI-TIN-PR-010. This Policy serves as the umbrella for derivative procedures on AI management; in the event of any discrepancy, the provisions of this Policy prevail insofar as they do not conflict with the provisions of Pupuk Indonesia (Persero) as Shareholder.

Kebijakan ini disusun dengan mengacu pada peraturan perundang-undangan, standar, dan komitmen berikut:

This Policy is developed with reference to the following laws and regulations, standards, and commitments:

1. Undang-Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, sebagaimana telah diubah terakhir dengan Undang-Undang No. 1 Tahun 2024 / *Law No. 11 of 2008 on Electronic Information and Transactions, as last amended by Law No. 1 of 2024*
2. Undang-Undang No. 27 Tahun 2022 tentang Pelindungan Data Pribadi / *Law No. 27 of 2022 on Personal Data Protection*
3. Peraturan Pemerintah No. 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik / *Government Regulation No. 71 of 2019 on the Operation of Electronic Systems and Transactions*
4. Surat Edaran Menteri Komunikasi dan Informatika No. 9 Tahun 2023 tentang Etika Kecerdasan Artifisial / *Circular Letter of the Minister of Communication and Informatics No. 9 of 2023 on Artificial Intelligence Ethics*
5. Peraturan Menteri BUMN No. PER-2/MBU/03/2023 tentang Pedoman Tata Kelola dan Kegiatan Korporasi Signifikan BUMN / *Regulation of the Minister of SOEs No. PER-2/MBU/03/2023 on Governance Guidelines and Significant Corporate Activities of SOEs*
6. ISO/IEC 42001:2023 *Artificial Intelligence Management System* dan ISO/IEC 27001:2022 *Information Security Management System* sebagai acuan praktik terbaik / *as best-practice references*
7. EU *Artificial Intelligence Act* (Regulation (EU) 2024/1689) sebagai acuan praktik terbaik internasional untuk kategori AI terlarang / *as an international best-practice reference for prohibited AI categories*
8. Komitmen *Responsible Artificial Intelligence* PT Pupuk Indonesia (Persero) / *Responsible Artificial Intelligence commitment of PT Pupuk Indonesia (Persero)*

Untuk memudahkan pemahaman, istilah-istilah dalam Kebijakan ini memiliki pengertian sebagai berikut:

For ease of understanding, the terms used in this Policy have the following meanings:

Istilah / *Term*	**Pengertian**	***Definition***
Kecerdasan Artifisial (AI)	Sistem berbasis mesin yang menghasilkan keluaran berupa prediksi, konten, rekomendasi, atau keputusan dari data masukan, termasuk AI generatif, pembelajaran mesin, dan AI Agent.	*A machine-based system that generates outputs such as predictions, content, recommendations, or decisions from input data, including generative AI, machine learning, and AI Agents.*
AI Agent	Sistem AI yang dapat menjalankan tindakan secara mandiri, seperti mengubah data, menjalankan transaksi, atau mengoperasikan aplikasi lain.	*An AI system capable of taking actions autonomously, such as modifying data, executing transactions, or operating other applications.*

Istilah / *Term*	Pengertian	*Definition*
Layanan AI Terdaftar	Layanan AI yang telah lolos asesmen keamanan dan privasi serta disetujui untuk digunakan oleh fungsi Teknologi Informasi.	*An AI service that has passed a security and privacy assessment and has been approved for use by the Information Technology function.*
Shadow AI	Penggunaan layanan AI yang tidak terdaftar atau akun pribadi untuk mengolah data Perusahaan.	*The use of unregistered AI services or personal accounts to process Company data.*
Human-in-the-loop	Mekanisme yang memastikan manusia meninjau, menyetujui, dan dapat menghentikan keluaran atau tindakan AI sebelum berdampak.	*A mechanism ensuring that humans review, approve, and can stop AI outputs or actions before they take effect.*
AI Berisiko Tinggi	Pemanfaatan AI yang keluarannya dapat berdampak signifikan terhadap keselamatan proses pabrik, K3, lingkungan, hak individu, keputusan kepegawaian, kelayakan mitra, atau kepatuhan hukum.	*AI use whose outputs may significantly affect plant process safety, occupational health and safety, the environment, individual rights, personnel decisions, partner eligibility, or legal compliance.*
Pemilik Layanan AI	Unit kerja atau pejabat yang ditetapkan sebagai penanggung jawab atas suatu layanan AI, akun, dan penggunaannya.	*The work unit or officer designated as accountable for an AI service, its accounts, and its use.*

Adapun seluruh pemanfaatan AI di Perusahaan berpegang pada sembilan prinsip berikut.

Therefore, all use of AI in the Company adheres to the following nine principles.

Prinsip / *Principle*	Komitmen Perusahaan	*Company Commitment*
1. Privasi dan perlindungan data / *Privacy and data protection*	Data pribadi diproses sesuai UU No. 27 Tahun 2022 dan hanya bila ada dasar pemrosesan yang sah. Data pribadi disamarkan sebelum masuk ke alur data AI, analisis mengutamakan data agregat, dan Perusahaan memastikan datanya tidak dipakai penyedia untuk melatih model.	*Personal data is processed in accordance with Law No. 27 of 2022 and only where there is a lawful basis. Personal data is masked before entering AI data pipelines, analysis prioritizes aggregated data, and the Company ensures its data is not used by providers to train models.*
2. Keamanan siber / *Cybersecurity*	Sistem AI dilindungi dari ancaman siber di sepanjang siklus hidupnya sesuai Sistem Manajemen Keamanan Informasi berbasis ISO/IEC 27001, untuk menjaga kerahasiaan, integritas, dan ketersediaan data.	*AI systems are protected from cyber threats throughout their lifecycle in accordance with the ISO/IEC 27001-based Information Security Management System, to safeguard the confidentiality, integrity, and availability of data.*

Prinsip / *Principle*	Komitmen Perusahaan	*Company Commitment*
3. Keadilan dan pencegahan bias / *Fairness and bias prevention*	Layanan AI dipantau dan diuji secara berkala agar akurat, konsisten, non diskriminatif, dan tidak menimbulkan perlakuan yang tidak adil terhadap individu atau kelompok.	*AI services are periodically monitored and tested to remain accurate, consistent, non-discriminatory, and free from unfair treatment of individuals or groups.*
4. Kendali manusia / *Human control*	AI membantu, manusia memutuskan. Setiap keluaran AI diverifikasi manusia sebelum digunakan, dan keputusan berdampak signifikan tidak diserahkan sepenuhnya kepada sistem otomatis. Manusia berwenang melakukan intervensi atau menghentikan sistem AI.	*AI assists, humans decide. Every AI output is verified by a human before use, and decisions with significant impact are not left entirely to automated systems. Humans have the authority to intervene in or stop AI systems.*
5. Transparansi dan keterjelasan / *Transparency and explainability*	Keterlibatan AI dalam suatu keluaran diberi label sehingga dapat diketahui penerimanya. Untuk penggunaan berisiko tinggi, dasar, data, dan logika umum yang menghasilkan keluaran AI harus dapat dijelaskan kepada pengambil keputusan dan pihak terdampak.	*The involvement of AI in an output is labeled so that recipients can recognize it. For high-risk uses, the basis, data, and general logic producing AI outputs must be explainable to decision-makers and affected parties.*
6. Akuntabilitas / *Accountability*	Setiap layanan, akun, dan penggunaan AI memiliki Pemilik Layanan AI yang jelas dan jejak audit, sehingga tanggung jawab atas keluaran AI selalu dapat ditelusuri.	*Every AI service, account, and use has a clearly designated AI Service Owner and an audit trail, so that accountability for AI outputs can always be traced.*
7. Batasan penggunaan / *Defined boundaries*	Hanya Layanan AI Terdaftar yang boleh digunakan, oleh personel berwenang, untuk tujuan yang telah disetujui. Perusahaan menetapkan secara tertulis penggunaan yang diizinkan, yang memerlukan persetujuan khusus, dan yang dilarang, sebagaimana diatur dalam pilar manajemen risiko dan klasifikasi AI.	*Only Registered AI Services may be used, by authorized personnel, for approved purposes. The Company defines in writing which uses are permitted, which require special approval, and which are prohibited, as set out in the risk management and AI classification pillar.*
8. Tanggung jawab lingkungan / *Environmental responsibility*	Efisiensi energi dan jejak ekologis menjadi kriteria dalam memilih layanan dan penyedia AI, termasuk pusat data dan model milik pihak ketiga. Pemanfaatan lisensi dioptimalkan, dan konsumsi energi AI pada infrastruktur milik Perusahaan dipantau serta dilaporkan dalam laporan keberlanjutan.	*Energy efficiency and ecological footprint are criteria in selecting AI services and providers, including third-party data centers and models. License utilization is optimized, and AI energy consumption on Company-owned infrastructure is monitored and disclosed in the sustainability report.*
9. Larangan praktik AI terlarang / *Prohibited AI practices*	Perusahaan tidak menggunakan atau mengembangkan AI untuk manipulasi perilaku, eksploitasi kerentanan individu atau kelompok, penilaian sosial (*social scoring*), atau pengawasan biometrik	*The Company does not use or develop AI for behavioral manipulation, exploitation of the vulnerabilities of individuals or groups, social scoring, or unauthorized biometric surveillance, in line with the*

Prinsip / *Principle*	Komitmen Perusahaan	*Company Commitment*
	tanpa izin, sejalan dengan kategori AI terlarang dalam EU AI Act.	*prohibited AI categories under the EU AI Act.*

Tata kelola AI mengikuti struktur tata kelola teknologi informasi dan keamanan informasi Perusahaan yang terintegrasi dengan Pupuk Indonesia Group.

AI governance follows the Company's information technology and information security governance structure, which is integrated with Pupuk Indonesia Group.

Organ / Fungsi *Body / Function*	Peran dan Tanggung Jawab	*Roles and Responsibilities*
Dewan Komisaris melalui Komite Tata Kelola Terintegrasi, Pemantau Risiko dan Investasi / *Board of Commissioners through the Integrated Governance, Risk and Investment Monitoring Committee*	Mengawasi penerapan Kebijakan ini dan risiko AI sebagai bagian dari risiko Teknologi Informasi dan Keamanan Siber.	*Oversees the implementation of this Policy and AI risks as part of Information Technology and Cybersecurity risks.*
Direksi / *Board of Directors*	Menetapkan Kebijakan ini, menyediakan sumber daya, dan menyetujui pemanfaatan AI Berisiko Tinggi.	*Establishes this Policy, provides resources, and approves High-Risk AI use.*
Departemen Teknologi Informasi, berkoordinasi dengan Kompartemen Teknologi Informasi PT Pupuk Indonesia (Persero) / *Information Technology Department, in coordination with the Information Technology Compartment of PT Pupuk Indonesia (Persero)*	Mengelola daftar Layanan AI Terdaftar, melakukan asesmen keamanan dan privasi, mengendalikan akses, memantau kinerja layanan AI, dan menyusun prosedur turunan.	*Manages the Registered AI Services list, conducts security and privacy assessments, controls access, monitors AI service performance, and develops derivative procedures.*
Pejabat Pelindungan Data Pribadi (*Data Protection Officer*)	Memastikan pemrosesan data pribadi oleh AI sesuai UU Pelindungan Data Pribadi, termasuk *Data Protection Impact Assessment* (DPIA) untuk AI yang mengolah data pribadi.	*Ensures that personal data processing by AI complies with the Personal Data Protection Law, including a Data Protection Impact Assessment (DPIA) for AI that processes personal data.*
PI-CSIRT / *Pupuk Indonesia Computer Security Incident Response Team*	Menangani insiden keamanan siber yang melibatkan sistem AI, mulai dari deteksi, isolasi, penanganan, hingga pemulihan.	*Handles cybersecurity incidents involving AI systems, from detection and isolation to handling and recovery.*
Pemilik Layanan AI dan pimpinan unit kerja pengguna /	Bertanggung jawab atas penggunaan AI di unit kerjanya,	*Are accountable for AI use in their work units, ensure human*

Organ / Fungsi *Body / Function*	Peran dan Tanggung Jawab	***Roles and Responsibilities***
AI Service Owners and heads of user work units	memastikan verifikasi manusia atas keluaran AI, serta mengelola risiko AI sebagai *risk owner*.	*verification of AI outputs, and manage AI risks as risk owners.*
Satuan Pengawasan Intern / *Internal Audit Unit*	Mengaudit kepatuhan terhadap Kebijakan ini secara berkala berbasis risiko.	*Periodically audits compliance with this Policy on a risk basis.*

Dalam menerapkan AI yang bertanggung jawab, Perusahaan mengacu dan secara bertahap menyelaraskan diri dengan standar internasional berikut:

In applying responsible AI, the Company refers to and progressively aligns with the following international standards:

- ISO/IEC 42001:2023 Sistem Manajemen Kecerdasan Artifisial / *Artificial Intelligence Management System*;
- ISO/IEC 27001:2022 Sistem Manajemen Keamanan Informasi / *Information Security Management System*;
- NIST AI Risk Management Framework (NIST AI RMF 1.0).

Penerapan Kebijakan ini dipantau secara berkala sebagai bagian dari tata kelola teknologi informasi dan manajemen risiko Perusahaan, serta diaudit berbasis risiko oleh Satuan Pengawasan Intern. Kebijakan ditinjau sekurang-kurangnya satu kali dalam setahun untuk menyesuaikan dengan perkembangan teknologi, regulasi, dan ekspektasi pemangku kepentingan. Kebijakan ini dikomunikasikan kepada seluruh insan Perusahaan, dipublikasikan melalui situs web resmi Perusahaan, dan berlaku sejak tanggal ditetapkan.

The implementation of this Policy is periodically monitored as part of the Company's information technology governance and risk management, and is audited on a risk basis by the Internal Audit Unit. The Policy is reviewed at least once a year to keep pace with technological, regulatory, and stakeholder developments. This Policy is communicated to all Company personnel, published on the Company's official website, and is effective from the date of its issuance.

Ditetapkan di Krueng Geukueh, Aceh Utara
Issued in Krueng Geukueh, North Aceh

Pada tanggal : 02 November 2026
On the date of: November 02, 2026

Filius Yuliandi
Direktur Utama
PT Pupuk Iskandar Muda