Kebijakan dan Komitmen
Tata Kelola & Keamanan Teknologi Informasi
PT Pupuk Iskandar Muda

Guna mendukung pencapaian visi dan misi Perusahaan, mengoptimalkan penciptaan nilai bagi pemegang saham, serta memenuhi tanggung jawab terhadap seluruh pemangku kepentingan dalam dinamika iklim usaha yang kian kompetitif, PT Pupuk Iskandar Muda menetapkan dan menjalankan Tata Kelola dan Keamanan Teknologi Informasi.

Penerapan sistem ini ditujukan untuk menjaga keandalan infrastruktur dan keberlangsungan operasional layanan, serta memastikan perlindungan terhadap seluruh aset teknologi informasi berdasarkan prinsip utama kerahasiaan *(confidentiality)*, integritas *(integrity)*, dan ketersediaan *(availability)*. Hal ini diwujudkan melalui serangkaian mitigasi ancaman siber yang komprehensif serta komitmen penuh dalam penyelenggaraan tata kelola teknologi informasi.

Komitmen Manajemen dan Tata Kelola TI

Dalam rangka mewujudkan sasaran tersebut, PT Pupuk Iskandar Muda berkomitmen penuh untuk:

1. Membangun dan menyelenggarakan arsitektur tata kelola keamanan informasi yang kokoh, adaptif, serta terproteksi guna mendukung pencapaian sasaran strategis Perusahaan.
2. Menyediakan dan menjamin kecukupan alokasi sumber daya dalam tahapan perencanaan, penerapan, operasional, pemeliharaan, hingga evaluasi dan pengembangan berkelanjutan Tata Kelola Keamanan Informasi.
3. Menyosialisasikan pentingnya pengelolaan teknologi informasi yang efektif, terukur, dan patuh terhadap standar acuan Tata Kelola Keamanan Informasi di seluruh unit kerja.
4. Menjamin kepatuhan menyeluruh terhadap perundang-undangan, ketentuan regulator, serta seluruh kewajiban kontraktual yang berlaku terkait keamanan informasi dan operasional TI.
5. Memberikan supervisi, arahan strategis, dan panduan kepada seluruh jajaran insan perusahaan agar berperan aktif dalam memperkuat efektivitas Tata Kelola Keamanan Informasi.
6. Menyelenggarakan program edukasi, pelatihan, dan peningkatan kesadaran keamanan siber (*cyber security awareness*) secara berkesinambungan bagi seluruh jenjang pegawai serta mitra kerja terkait.
7. Mengadopsi inovasi dan perkembangan teknologi mutakhir yang relevan untuk meningkatkan mutu dan performa Tata Kelola Keamanan Informasi secara berkelanjutan.
8. Mendampingi manajemen lini operasional dalam menerapkan ketentuan teknis TI sesuai batasan wewenang dan cakupan tanggung jawab masing-masing.

9. Memastikan seluruh instrumen regulasi, pedoman pengelolaan keamanan informasi, prosedur manajemen perubahan, serta manual Tata Kelola Keamanan Informasi telah disahkan secara resmi, dipublikasikan, dan diimplementasikan.
10. Menyusun serta memperbarui rencana pengelolaan layanan TI secara berkala guna memastikan keselarasan terhadap target manajemen dan kebutuhan pemangku kepentingan.
11. Mengintegrasikan kerangka kerja dan metodologi mitigasi risiko teknologi informasi secara harmonis ke dalam kerangka Manajemen Risiko Korporasi (*Enterprise Risk Management*).
12. Memastikan setiap direktorat, divisi, dan departemen menjalankan peran serta tanggung jawabnya secara sinergis untuk menjaga kesinambungan ekosistem Tata Kelola Keamanan Informasi.
13. Menyelenggarakan audit internal berkala yang independen dan terstruktur untuk mengevaluasi derajat kepatuhan serta keandalan penerapan Tata Kelola Keamanan Informasi.
14. Melaksanakan tinjauan berkala terhadap efektivitas dan kinerja operasional Tata Kelola Keamanan Informasi sebagai landasan perbaikan dan penyempurnaan berkesinambungan.
15. Menetapkan sasaran mutu, memelihara indikator kinerja, dan meningkatkan standar implementasi Tata Kelola Keamanan Informasi secara konsisten.
16. Memastikan kepatuhan dan konsistensi seluruh elemen insan perusahaan dalam mematuhi seluruh ketentuan dalam kebijakan ini.
17. Memberikan perlindungan menyeluruh terhadap kerahasiaan, keutuhan, dan ketersediaan data maupun aset informasi dari ancaman internal serta eksternal.
18. Menerapkan sistem pemantauan terpadu, mekanisme deteksi dini, serta penanganan insiden keamanan siber yang responsif guna menekan dampak operasional seminimal mungkin.
19. Merumuskan, membukukan, serta menegakkan standar kendali keamanan informasi yang wajib dipatuhi oleh vendor, mitra bisnis, konsultan, maupun penyedia barang dan jasa pihak ketiga.

Kebijakan dan komitmen ini berlaku mutlak serta mengikat bagi seluruh jajaran organ pengurus, manajemen, dan karyawan di lingkungan PT Pupuk Iskandar Muda.

Ditetapkan di Krueng Geukueh, Aceh Utara
Pada tanggal : 02 November 2026

Filius Yuliandi

Direktur Utama
PT Pupuk Iskandar Muda

POLICY AND COMMITMENT ON INFORMATION TECHNOLOGY GOVERNANCE AND SECURITY

To support the achievement of the Company's vision and mission, optimize value creation for shareholders, and fulfill responsibilities to all stakeholders within an increasingly competitive business environment, PT Pupuk Iskandar Muda establishes and implements an Governance and Information Technology Security.

The implementation of this system aims to maintain infrastructure reliability and service operational continuity, as well as ensure the protection of all information technology assets based on the primary principles of confidentiality, integrity, and availability. This is realized through a comprehensive series of cyber threat mitigations and full commitment to the execution of information technology governance.

Management Commitment and IT Governance

To achieve these goals, PT Pupuk Iskandar Muda is fully committed to:

1. Establishing and maintaining a robust, adaptive, and protected information security governance architecture to support the Company's strategic objectives.
2. Providing and ensuring adequate resource allocation throughout the planning, implementation, operation, maintenance, evaluation, and continuous development phases of Information Security Governance.
3. Communicating the importance of effective, measurable, and compliant information technology management aligned with Information Security Governance reference standards across all organizational units.
4. Ensuring full compliance with all relevant laws, regulatory mandates, and contractual obligations pertaining to information security and IT service delivery.
5. Providing supervision, strategic direction, and guidance to all personnel to actively contribute to the effectiveness of Information Security Governance.
6. Conducting continuous cyber security awareness programs, education, and training for all employee levels and relevant business partners.
7. Adopting relevant cutting-edge technological innovations to continuously enhance the quality and performance of Information Security Governance.
8. Supporting operational line management in implementing IT technical provisions within their respective domains of authority and responsibility.

9. Ensuring all regulatory instruments, information security management guidelines, IT service change management procedures, and Information Security Governance manuals are officially approved, published, and implemented.
10. Formulating and updating IT service management plans periodically to ensure alignment with management goals and stakeholder requirements.
11. Harmoniously integrating IT risk mitigation frameworks and methodologies into the Enterprise Risk Management (ERM) framework.
12. Ensuring each directorate, division, and department executes its respective roles and responsibilities synergistically to maintain the continuity of the Information Security Governance ecosystem.
13. Conducting independent and structured periodic internal audits to evaluate compliance levels and operational reliability of Information Security Governance implementation.
14. Performing periodic reviews of ITMS operational effectiveness and performance as a foundation for continuous improvement and refinement.
15. Establishing quality objectives, maintaining performance indicators, and consistently elevating Information Security Governance implementation standards.
16. Ensuring compliance and consistency across all corporate personnel in adhering to all provisions of this policy.
17. Providing comprehensive protection for the confidentiality, integrity, and availability of all data and information assets against both internal and external threats.
18. Implementing an integrated monitoring system, early detection mechanisms, and responsive cybersecurity incident handling to minimize operational impacts.
19. Formulating, documenting, and enforcing information security control standards that must be complied with by third parties, including vendors, business partners, consultants, and suppliers.

This policy and commitment is absolute and legally binding for all governing bodies, management, and employees within PT Pupuk Iskandar Muda.

Issued in Krueng Geukueh, North Aceh

On the date of: November 02, 2026

Filius Yuliandi

President Director
PT Pupuk Iskandar Muda