Jl. Tipar Cakung Nomor 8, Desa/Kelurahan Sukapura, Kec. Cilincing
Kota Adm. Jakarta Utara, Provinsi DKI Jakarta, Kode Pos: 14140
+62 811 870 321 (Phone & Whatsapp)

KEBIJAKAN DASAR KEAMANAN INFORMASI

Nomor: 01/LST/ISO/KDKI/IX/2025
Versi : 1.0

1. Pernyataan Kebijakan

PT Logika Sarana Teknologi (selanjutnya disebut "Perusahaan") berkomitmen untuk melindungi kerahasiaan, integritas, dan ketersediaan semua aset informasi yang dikelola, termasuk data karyawan, data pelanggan, kekayaan intelektual, dan sistem informasi. Kebijakan ini merupakan fondasi dari Sistem Manajemen Keamanan Informasi (Information Security Management System/ISMS) yang dirancang sesuai dengan standar internasional ISO/IEC 27001:2022.

Manajemen senior berkomitmen untuk mendukung implementasi, pemeliharaan, dan perbaikan berkelanjutan dari ISMS ini. Semua karyawan, kontraktor, dan pihak ketiga yang bekerja sama dengan Perusahaan wajib mematuhi kebijakan dan prosedur keamanan informasi yang telah ditetapkan.

2. Tujuan

Tujuan dari kebijakan ini adalah untuk:

- Memastikan perlindungan aset informasi Perusahaan dari segala bentuk ancaman, baik yang disengaja maupun tidak disengaja.
- Memenuhi persyaratan hukum, peraturan, dan kontrak yang relevan terkait keamanan informasi.
- Menciptakan budaya kesadaran keamanan informasi di seluruh organisasi.
- Memastikan kelangsungan bisnis (business continuity) dengan meminimalkan dampak dari insiden keamanan.
- Menjaga kepercayaan dari pelanggan dan pemangku kepentingan lainnya.

3. Ruang Lingkup

Kebijakan ini berlaku untuk seluruh entitas, proses bisnis, sistem, aplikasi, jaringan, dan aset informasi yang dimiliki atau dikelola oleh PT Logika Sarana Teknologi. Ruang lingkup ini mencakup, namun tidak terbatas pada:

- Seluruh karyawan, termasuk staf tetap, kontrak, dan magang.
- Kontraktor, vendor, dan pihak ketiga yang memiliki akses ke aset informasi Perusahaan.
- Semua perangkat keras (server, komputer, perangkat mobile) dan perangkat lunak (aplikasi, sistem operasi) yang digunakan dalam kegiatan operasional.
- Semua data, baik dalam bentuk digital maupun fisik, yang disimpan, diproses, atau ditransmisikan oleh Perusahaan.

Jl. Tipar Cakung Nomor 8, Desa/Kelurahan Sukapura, Kec. Cilincing
Kota Adm. Jakarta Utara, Provinsi DKI Jakarta, Kode Pos: 14140
+62 811 870 321 (Phone & Whatsapp)

4. **Prinsip-Prinsip Keamanan Informasi**
   Perusahaan mengadopsi prinsip dasar ISO 27001 sebagai pilar utama, yaitu:
   - **Kerahasiaan (Confidentiality):** Memastikan bahwa informasi hanya dapat diakses oleh pihak yang berwenang.
   - **Integritas (Integrity):** Memastikan bahwa informasi tetap akurat dan lengkap, serta terlindung dari modifikasi yang tidak sah.
   - **Ketersediaan (Availability):** Memastikan bahwa informasi dan sistem terkait dapat diakses oleh pengguna yang berwenang saat dibutuhkan.

5. **Tanggung Jawab**
   Direktur Utama: Bertanggung jawab penuh atas implementasi ISMS dan peninjauan kebijakan ini secara berkala.
   Manajemen Senior: Bertanggung jawab untuk memastikan sumber daya yang memadai tersedia untuk mendukung ISMS.
   Tim Keamanan Informasi: Bertanggung jawab untuk mengembangkan, memelihara, dan mengawasi implementasi ISMS.
   Semua Karyawan dan Pihak Ketiga: Bertanggung jawab untuk memahami dan mematuhi kebijakan, prosedur, dan pedoman keamanan informasi. Pelanggaran terhadap kebijakan ini dapat mengakibatkan tindakan disipliner.

6. **Peninjauan dan Pembaharuan Kebijakan**
   Kebijakan ini akan ditinjau setidaknya setiap satu tahun sekali atau lebih sering jika terjadi perubahan signifikan dalam bisnis, teknologi, atau lingkungan ancaman. Peninjauan akan dilakukan oleh Tim Keamanan Informasi dan disetujui oleh Direktur Utama.

Ditetapkan oleh:

Takashi Yoshitsugu
Direktur Utama
Tanggal: 17 September 2025