Pegadaian

PEDOMAN SISTEM MANAJEMEN KEAMANAN INFORMASI (SMKI)
PERATURAN DIREKSI NO 111 TAHUN 2024

Pernyataan

Dokumen ini merupakan rangkuman “Pedoman Sistem Manajemen Keamanan Informasi (SMKI)” PT Pegadaian yang ditetapkan melalui Peraturan Direksi Nomor 111 Tahun 2024. Kebijakan ini disusun untuk memastikan pengelolaan dan perlindungan informasi perusahaan berjalan sesuai prinsip kerahasiaan (confidentiality), keutuhan (integrity), dan ketersediaan (availability). SMKI mengacu pada standar ISO/IEC 27001:2013 serta regulasi nasional, khususnya Peraturan Menteri Komunikasi dan Informatika Nomor 4 Tahun 2016 tentang Sistem Manajemen Pengamanan Informasi.

Latar Belakang & Komitmen

Pegadaian menyadari bahwa informasi merupakan aset strategis yang berpengaruh terhadap pengambilan keputusan manajemen. Oleh karena itu, dibutuhkan tata kelola keamanan informasi yang komprehensif untuk melindungi perusahaan dari ancaman internal maupun eksternal. Melalui penerapan SMKI, Pegadaian berkomitmen menjaga keberlangsungan bisnis, meningkatkan ketahanan siber, serta mematuhi regulasi dan standar terbaik dalam pengelolaan informasi.

Referensi

Pedoman ini disusun berdasarkan:

- Anggaran Dasar PT Pegadaian beserta seluruh perubahannya.
- Peraturan Menteri Komunikasi dan Informatika No. 4 Tahun 2016 tentang Sistem Manajemen Pengamanan Informasi.
- Standar ISO/IEC 27001:2013 tentang Information Security Management System.

Lingkup Penerapan

Kebijakan SMKI berlaku pada seluruh aset informasi yang dimiliki dan dikelola oleh Pegadaian, termasuk data, perangkat keras, perangkat lunak, jaringan komunikasi, fasilitas pendukung, serta sumber daya manusia. Cakupan penerapan meliputi kantor pusat, kantor wilayah, kantor area, cabang, hingga unit pelayanan di seluruh Indonesia.

Peran & Tanggung Jawab

Tanggung jawab penerapan SMKI berada pada seluruh elemen organisasi. Direksi memastikan koordinasi strategis, sementara Direktorat TI mengelola fasilitas keamanan

Pegadaian

informasi sesuai kebijakan. Chief Information Security Officer (CISO) bertugas mengoordinasikan operasional keamanan informasi, didukung oleh Information Security Officer (ISO) di tiap unit. Seluruh karyawan dan pihak eksternal yang mengakses aset informasi wajib mematuhi ketentuan SMKI.

Implementasi & Strategi

SMKI dijalankan melalui sejumlah kebijakan dan kontrol utama, antara lain:

- Manajemen Risiko Keamanan Informasi: identifikasi, asesmen, dan mitigasi risiko keamanan informasi termasuk residual risk.
- Pengendalian Akses dan Aset Informasi: klasifikasi informasi, pengaturan hak akses, serta pengelolaan aset informasi sesuai standar keamanan.
- Pengendalian SDM: peningkatan kesadaran keamanan (security awareness), perjanjian kerahasiaan, serta prosedur pengelolaan SDM sebelum, selama, dan setelah bekerja.
- Pengendalian Operasional TI: standar software desktop, penggunaan email dan internet, pengamanan pengembangan sistem, serta monitoring aktivitas TI.
- Business Continuity Management (BCM): memastikan keberlangsungan operasional saat terjadi insiden atau bencana.
- Hubungan dengan Pihak Ketiga: pengaturan kerja sama dengan vendor dan mitra agar sesuai standar keamanan.
- Kebijakan Tambahan: mencakup threat intelligence, cloud security, konfigurasi, data masking, data leakage prevention, information deletion, dan web filtering.

Penutup

Dengan diberlakukannya SMKI, Pegadaian menegaskan komitmennya untuk melindungi seluruh aset informasi perusahaan dari ancaman yang dapat merugikan bisnis, reputasi, dan kepercayaan pemangku kepentingan. SMKI menjadi pedoman strategis untuk meningkatkan tata kelola keamanan informasi secara berkelanjutan, mendukung transformasi digital perusahaan, serta memastikan kepatuhan pada regulasi nasional maupun standar internasional.