PENGENALAN ISO 27001 : 2022 DI INDUSTRI P2P LENDING

IVOJI

ivoji.id

MENGAPA ISO 27001 : 2022 SANGAT PENTING BAGI KITA?

Mengimplementasikan Sistem Manajemen Keamanan Informasi (SMKI) berbasis standar internasional ISO 27001:2022

Sebagai perusahaan P2P Lending, kita mengelola data sensitif

Regulasi OJK: Kepatuhan terhadap standar keamanan informasi adalah kewajiban regulasi demi menjaga izin operasional kita.

Kepercayaan Pasar: Lender dan borrower hanya akan menempatkan dana dan datanya jika mereka percaya sistem kita aman.

Perubahan di Versi 2022: ISO 27001:2022 memperkenalkan kontrol keamanan yang lebih relevan dengan era digital saat ini, seperti keamanan cloud computing dan kesiapan menghadapi ancaman siber (cyber threat intelligence).

PRINSIP UTAMA KEAMANAN INFORMASI (CIA TRIAD)

- Confidentiality (Kerahasiaan): Memastikan data borrower/lender tidak bocor ke pihak yang tidak berwenang (misal: tidak membagikan data kontak nasabah di grup chat pribadi).

- Integrity (Integritas): Memastikan data akurat dan tidak diubah secara ilegal (misal: nilai pendanaan atau data credit score tidak dimanipulasi).

- Availability (Ketersediaan): Memastikan sistem aplikasi P2P Lending kita siap diakses kapan pun oleh pengguna saat dibutuhkan.

TANGGUNG JAWAB KITA BERSAMA (KEAMANAN SDM)

- Seluruh karyawan wajib menjaga keamanan informasi sebelum, selama, dan setelah masa bertugas
- Menandatangani dan mematuhi Perjanjian Kerahasiaan (Non-Disclosure Agreement / NDA).
- Mengikuti edukasi dan sosialisasi keamanan informasi secara rutin.
- Kebijakan Meja Bersih (Clean Desk Policy): Jangan meninggalkan dokumen berisi data keuangan nasabah atau dokumen perusahaan di atas meja tanpa pengawasan.
- Setiap tindakan yang melanggar kebijakan akan dikenai sanksi disiplin sesuai ketentuan yang berlaku.

MENGENAL KLASIFIKASI DATA PERUSAHAAN

- Confidential (Rahasia): Data yang hanya boleh diakses oleh personil tertentu dalam jumlah yang sangat terbatas (contoh: data nasabah, PII).
- Restricted (Terbatas): Data internal yang hanya boleh diakses oleh karyawan untuk kepentingan pekerjaan perusahaan.
- Public (Umum): Informasi yang bebas diakses oleh masyarakat umum di luar organisasi.

ATURAN HAK AKSES & PASSWORD

Mengimplementasikan Sistem Manajemen Keamanan Informasi (SMKI) berbasis standar internasional ISO 27001:2022

- Prinsip Akses: "Segala sesuatu umumnya dilarang, kecuali secara tegas diizinkan."
- Need to Know & Need to Use: Anda hanya diberikan akses pada informasi dan fasilitas TI yang benar-benar dibutuhkan untuk menjalankan tugas Anda.
- Ketentuan Password Aman:
  a. Wajib mengombinasikan huruf besar, huruf kecil, angka, dan karakter khusus.
  b. Password memiliki masa berlaku dan harus diganti secara berkala.
  c. Dilarang keras membagikan kredensial akun atau password kepada siapa pun

APA PERAN KITA SEBAGAI KARYAWAN INTERNAL?

- Keamanan Password & Akun: Gunakan Multi-Factor Authentication (MFA), jangan pernah membagikan akun internal ke rekan kerja lain.
- Penanganan Data Sensitif: Jangan mengunduh data nasabah ke perangkat pribadi. Gunakan jalur resmi perusahaan yang terenkripsi.
- Waspada Phishing: Berhati-hatilah terhadap email atau pesan mencurigakan yang meminta data login sistem P2P kita.
- Kebijakan Meja Bersih (Clean Desk Policy): Jangan meninggalkan dokumen berisi data keuangan nasabah atau dokumen perusahaan di atas meja tanpa pengawasan.