■■ Data Security Protocol

PT. Contoh Perusahaan Teknologi Indonesia

Dokumen ini bersifat internal dan rahasia

1. Tujuan

Dokumen ini bertujuan untuk menetapkan protokol dan kebijakan keamanan data guna melindungi kerahasiaan, integritas, dan ketersediaan informasi perusahaan dari akses tidak sah, kebocoran data, serta serangan siber.

2. Ruang Lingkup

Protokol ini mencakup semua jenis data, baik yang disimpan secara fisik maupun digital, dan berlaku untuk seluruh sistem, jaringan, perangkat, serta personel yang mengakses data milik perusahaan.

3. Klasifikasi Data

Semua data harus diklasifikasikan berdasarkan sensitivitas:

Kategori	Deskripsi	Contoh
Data Publik	Informasi terbuka yang tidak membahayakan perusahaan	Konten web, siaran pers
Data Internal	Digunakan secara internal, tidak untuk publik	Dokumen kebijakan, laporan harian
Data Rahasia	Mengandung informasi bisnis penting	Data karyawan, kontrak kerja
Data Sensitif/Kritis	Data berdampak tinggi jika bocor	Data pribadi pelanggan, strategi bisnis, data fi

4. Perlindungan Data Saat Disimpan (Data at Rest)

Semua data rahasia/sensitif harus dienkripsi (AES-256). Akses dibatasi dengan prinsip least privilege. Backup otomatis disimpan di lokasi berbeda dan aman.

5. Perlindungan Data Saat Dikirimkan (Data in Transit)

Gunakan HTTPS/TLS 1.2+, VPN untuk akses luar. Dilarang kirim data sensitif tanpa enkripsi.

6. Akses & Autentikasi

Gunakan login kuat dan 2FA. Terapkan kontrol akses berbasis peran. Audit log dicatat dan ditinjau rutin.

7. Pemantauan & Logging

Semua aktivitas dicatat dengan sistem logging terpusat. Log disimpan minimal 12 bulan.

8. Pencegahan Kebocoran Data (DLP)

Gunakan software DLP, blokir USB/email tidak sah, larang penggunaan cloud pribadi.

9. Penghapusan Data

Data yang tidak terpakai harus dihapus secara aman. Media digital di-wipe, fisik dihancurkan.

10. Tanggung Jawab Pengguna

Setiap karyawan bertanggung jawab menjaga data yang diakses. Wajib lapor pelanggaran ke tim IT.

11. Kepatuhan dan Audit

Akan dilakukan audit rutin. Pelanggaran dapat diberi sanksi sesuai tingkat kesalahan.

12. Contoh Implementasi

- Enkripsi database PostgreSQL menggunakan TDE
- Transfer file klien via SFTP
- Backup terenkripsi otomatis ke cloud
- Pemakaian BitLocker untuk laptop kerja
- Email dengan enkripsi PGP
- Google Workspace dengan DLP rules aktif

13. Pernyataan Kepatuhan

Saya memahami dan akan mematuhi Data Security Protocol ini:

Nama: _____

Jabatan: _____

Tanda Tangan: _____

Tanggal: _____