Modul 3: Penggunaan AI yang Aman

Panduan praktis menggunakan alat kecerdasan buatan secara aman, bertanggung jawab, dan sesuai kebijakan organisasi — tanpa membahayakan data pribadi maupun aset perusahaan.

Edy Susanto - Founder C-SIX Security

Gambaran Modul

Apa yang Akan Kita Pelajari?

Modul ini dirancang untuk membekali Anda dengan pemahaman mendalam tentang risiko penggunaan AI di lingkungan kerja dan cara menggunakannya secara aman.

01

Risiko Data & AI

Memahami bahaya membocorkan informasi sensitif ke platform AI

02

Shadow AI

Mengenali dan mengelola penggunaan AI tidak resmi di tempat kerja

03

Privasi & Perlindungan Data

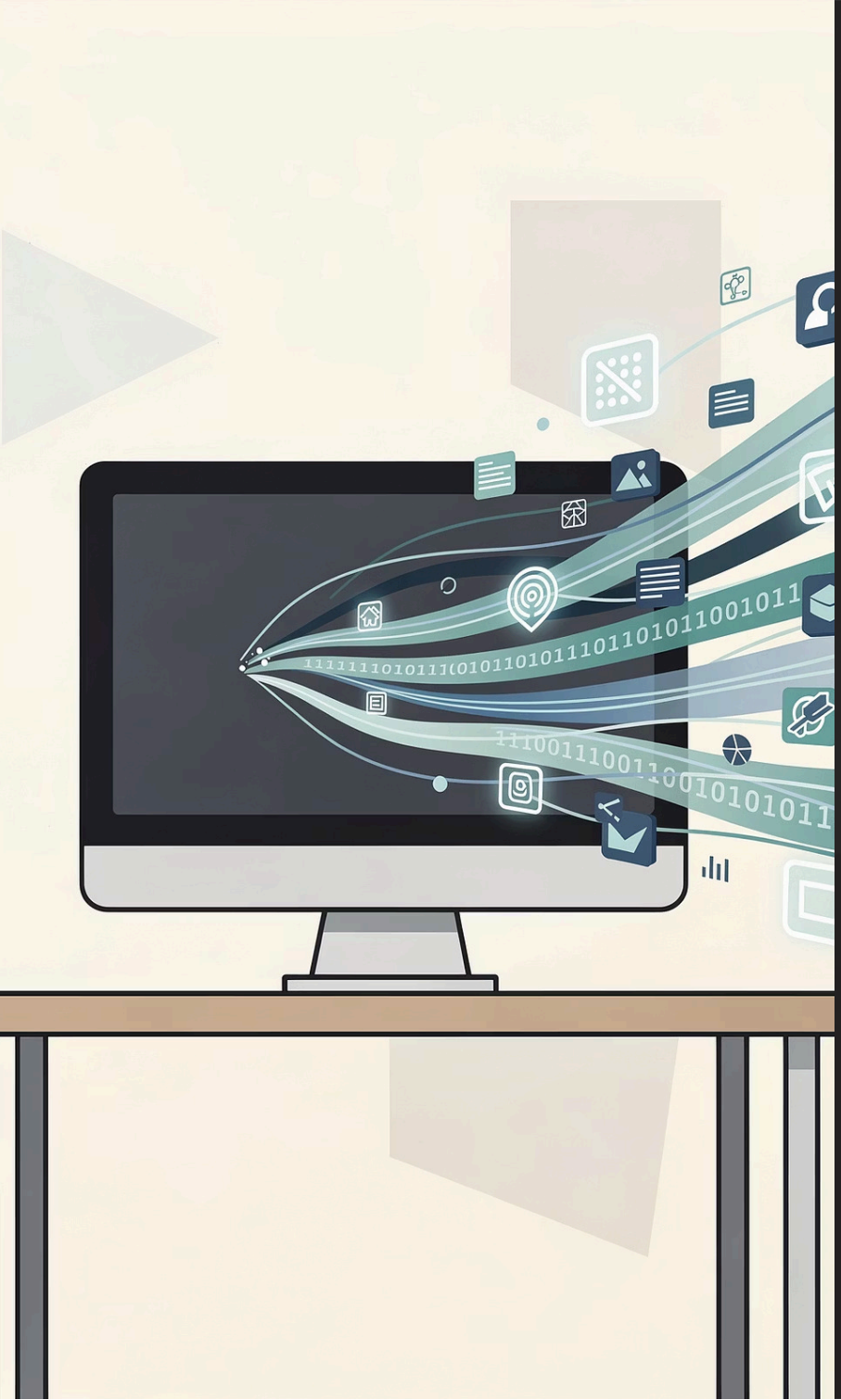
Prinsip dasar menjaga kerahasiaan data dalam interaksi dengan AI

04

Kebijakan AI Organisasi

Memahami aturan dan panduan resmi penggunaan AI di perusahaan

Edy Susanto - Founder C-SIX Security



Risiko Membocorkan Data ke AI

Setiap kali Anda mengetikkan teks ke dalam platform AI seperti ChatGPT, Gemini, atau Copilot, data tersebut berpotensi dikirim ke server eksternal, diproses, dan dalam beberapa kasus, digunakan untuk melatih model AI.

📤 Data Terkirim ke Server Luar

Teks yang Anda masukkan dapat disimpan di infrastruktur milik pihak ketiga, di luar kendali organisasi Anda.

🔁 Digunakan untuk Pelatihan Model

Beberapa platform AI menggunakan input pengguna untuk menyempurnakan modelnya, sehingga data Anda bisa "tersimpan" di sistem mereka.

⚖️ Risiko Kepatuhan & Hukum

Kebocoran data pelanggan atau informasi internal dapat melanggar regulasi seperti UU PDP, GDPR, atau kebijakan internal perusahaan.

Edy Susanto - Founder C-SIX Security

Batasan Konten

Informasi yang Tidak Boleh Dibagikan ke AI

Tidak semua informasi aman untuk dimasukkan ke dalam platform AI. Berikut adalah kategori data yang harus dihindari saat menggunakan alat AI eksternal:

Data Pribadi

NIK, nomor KTP, tanggal lahir, alamat rumah, dan informasi identitas karyawan maupun pelanggan

Data Keuangan

Laporan keuangan internal, anggaran belum dipublikasi, data akun bank, dan informasi transaksi sensitif

Rahasia Bisnis

Strategi perusahaan, rencana produk, kontrak klien, dan informasi kompetitif yang belum dipublikasikan

Kredensial & Akses

Password, API key, token autentikasi, dan segala bentuk informasi login sistem internal

⚠ Ingat: Sekali data dikirim ke platform AI eksternal, Anda tidak memiliki kendali penuh atas bagaimana data tersebut diproses atau disimpan.

Edy Susanto - Founder C-SIX Security

Shadow AI di Tempat Kerja

Shadow AI adalah penggunaan alat kecerdasan buatan oleh karyawan tanpa sepengetahuan atau persetujuan resmi dari departemen TI maupun manajemen. Fenomena ini semakin meluas seiring mudahnya akses ke berbagai platform AI gratis di internet.

Mengapa Ini Terjadi?

- Tekanan produktivitas yang tinggi
- Kurangnya alat AI resmi yang disediakan perusahaan
- Minimnya kesadaran tentang risiko keamanan
- Kemudahan akses platform AI gratis

Risiko yang Ditimbulkan

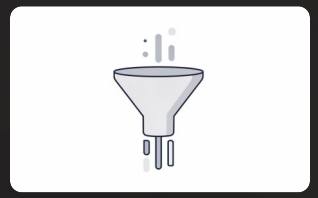
- Data sensitif bocor ke pihak ketiga tanpa audit
- Pelanggaran kebijakan keamanan informasi
- Potensi sanksi hukum dan regulasi
- Sulit dilacak dan dikendalikan oleh tim TI

Edy Susanto - Founder C-SIX Security

Perlindungan Data

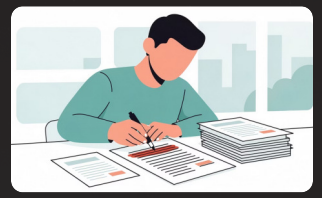
Privasi dalam Penggunaan AI

Menjaga privasi bukan hanya kewajiban hukum — ini adalah bentuk tanggung jawab profesional terhadap pelanggan, rekan kerja, dan organisasi Anda. Berikut prinsip-prinsip yang harus selalu diterapkan:



Minimalisasi Data

Hanya masukkan informasi yang benar-benar diperlukan. Hindari menyertakan detail yang tidak relevan dengan tugas yang ingin diselesaikan.



Anonimisasi

Ganti nama, nomor ID, atau detail identitas dengan placeholder seperti "Pelanggan A" atau "Perusahaan X" sebelum memasukkan ke AI.

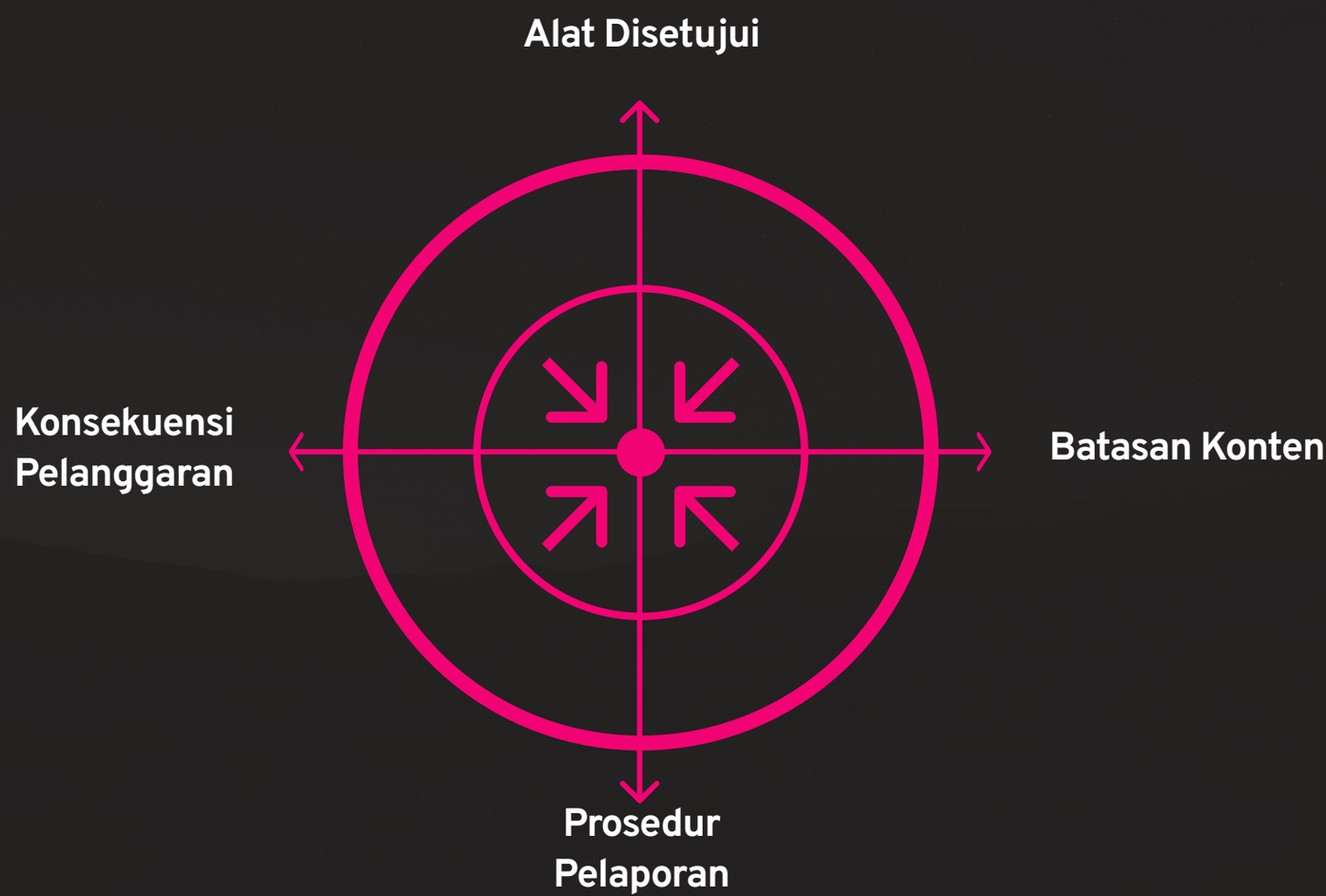
Review Sebelum Kirim

Selalu periksa ulang teks yang akan Anda kirim ke AI. Pastikan tidak ada data sensitif yang tersisip secara tidak sengaja.

Edy Susanto - Founder C-SIX Security

Memahami Kebijakan Penggunaan AI

Setiap organisasi memiliki kebijakan yang mengatur bagaimana AI boleh dan tidak boleh digunakan. Memahami dan mematuhi kebijakan ini adalah tanggung jawab setiap karyawan.



Kebijakan AI yang baik mencakup daftar platform yang disetujui, panduan konten yang boleh diproses, mekanisme pelaporan insiden, serta konsekuensi jika terjadi pelanggaran. Segera konsultasikan dengan tim TI jika Anda tidak yakin tentang suatu alat AI.

Edy Susanto - Founder C-SIX Security

Studi Kasus

Skenario: Apa yang Harus Dilakukan?

Kemampuan mengevaluasi situasi nyata adalah kunci penggunaan AI yang aman. Perhatikan skenario berikut dan identifikasi tindakan yang tepat:

1

Skenario 1: Laporan Keuangan

Rekan Anda meminta bantuan meringkas laporan keuangan Q3 menggunakan ChatGPT. **Apa yang seharusnya dilakukan?** Gunakan alat AI yang telah disetujui perusahaan, atau anonimkan angka sebelum memproses.

2

Skenario 2: Data Pelanggan

Anda ingin membuat email pemasaran dan berniat memasukkan nama serta email pelanggan ke AI. **Apa risikonya?** Data pelanggan adalah PII yang dilindungi — gunakan data contoh atau placeholder.

3

Skenario 3: Kode Internal

Developer ingin menggunakan Copilot untuk men-debug kode yang mengandung logika bisnis rahasia. **Apa tindakan aman?** Periksa apakah enterprise version dengan data protection aktif tersedia.

Panduan Praktis: Checklist Penggunaan AI Aman

Gunakan checklist ini setiap kali Anda hendak menggunakan alat AI untuk pekerjaan. Jadikan ini kebiasaan sehari-hari:

✅ Sebelum Menggunakan AI

- ▢ Pastikan platform AI sudah disetujui perusahaan
- ▢ Periksa apakah konten mengandung data sensitif
- ▢ Anonimkan informasi pribadi atau rahasia bisnis
- ▢ Baca kebijakan privasi platform yang akan digunakan

✅ Saat & Setelah Menggunakan AI

- ▢ Hindari copy-paste dokumen internal secara langsung
- ▢ Verifikasi output AI sebelum digunakan secara resmi
- ▢ Laporkan penggunaan AI yang mencurigakan ke tim TI
- ▢ Dokumentasikan alat AI yang digunakan untuk audit

Edy Susanto - Founder C-SIX Security

Ringkasan & Outcome Pembelajaran

Setelah menyelesaikan Modul 3 ini, Anda kini memiliki pemahaman yang lebih baik untuk menggunakan AI secara aman dan bertanggung jawab di lingkungan kerja.

🎯 Anda Mampu

Mengidentifikasi risiko keamanan data saat menggunakan platform AI eksternal

🛡️ Anda Terlindungi

Menerapkan praktik terbaik untuk menjaga privasi data pribadi dan organisasi

📋 Anda Patuh

Memahami dan mengikuti kebijakan resmi penggunaan AI di perusahaan Anda

Ingat: AI adalah alat yang powerful — keamanannya bergantung pada bagaimana kita menggunakannya. Jadilah pengguna AI yang cerdas dan bertanggung jawab!

Edy Susanto - Founder C-SIX Security