

AI DAN KEAMANAN INFORMASI



Bijak Memanfaatkan Kecerdasan

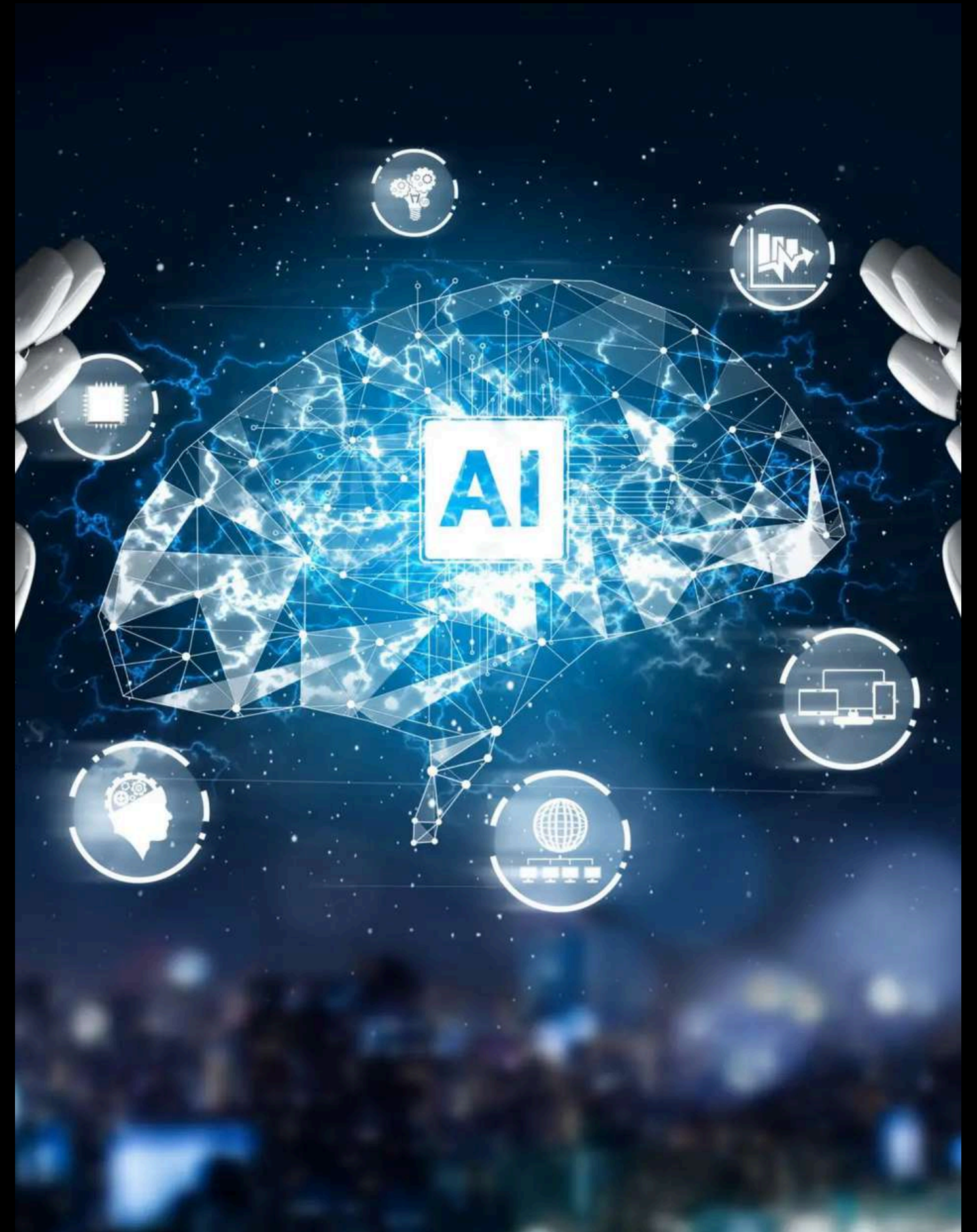
Buatan dalam Penggunaan Sehari-hari

BADAN SIBER DAN SANDI NEGARA
KETUA TIM LITERASI
RIKSON GULTOM., S.ST., M.KOM

APA ITU AI?

ROBOT YANG BISA MIKIR?

“MASALAH TERBESAR AI BUKAN BAHWA AI TAHU TERLALU BANYAK TENTANG KITA. MASALAHNYA ADALAH KITA MULAI TERLALU MUDAH MEMPERCAYAI SESUATU HANYA KARENA AI YANG MENGATAKANNYA.”



AI BISA MEMBUAT TEKS?

AI BISA MEMBUAT GAMBAR?

AI BISA MEMBUAT SUARA?

AI BISA MEMBUAT VIDEO?

AI BISA MELAKUKAN ANALISIS DOKUMEN?

AI BISA MENIRU GAYA KOMUNIKASI MANUSIA

AI BISA MEMBANTU MANUSIA MEMBUAT KEPUTUSAN?



KALAU SEBUAH INFORMASI DAPAT DIBUAT DALAM 10 DETIK, TETAPI MEMBUTUHKAN 10 MENIT
UNTUK MEMASTIKAN BAHWA INFORMASI ITU BENAR, APAKAH KITA SEDANG HIDUP DI ERA
INFORMASI... ATAU ERA KEBINGUNGAN?

DULU

IDE > MANUSIA > WAKTU > TULISAN > INFORMASI

INFORMASI YANG BANYAK RELATIF
MAHAL KETIKA DIPRODUKSI

DULU KITA KEKURANGAN INFORMASI

SEKARANG

IDE > PROMPT > AI > INFORMASI

INFORMASI YANG BANYAK SANGAT
MURAH UNTUK DIPRODUKSI

SEKARANG KITA BERISIKO
MENGALAMI SURPLUS INFORMASI
YANG TIDAK TERVERIFIKASI

AI MEMBUAT KITA LEBIH CEPAT, TETAPI BELUM TENTU LEBIH BENAR

BANYAK ORANG BERFIKIR KEAMANAN SIBER ADALAH :

- FIREWALL
- ANTIVIRUS
- PASSWORD
- MFA
- ENCRYPTION

COGNITIVE SECURITY

KEMAMPUAN MANUSIA MEMPERTAHANKAN KUALITAS BERPIKIR KETIKA BERHADAPAN DENGAN INFORMASI YANG DIHASILKAN ATAU DIMANIPULASI OLEH AI.

SERANGAN BERTUJUAN :

- MEMBUAT KITA PERCAYA,
- MEMBUAT KITA PANIK,
- MEMBUAT KITA TERBURU-BURU,
- MEMBUAT KITA MENGAMBIL KEPUTUSAN YANG SALAH

SERANGAN TERBESAR AI MUNGKIN BUKAN “DATA BREACH TAPI DECISION BREACH

KETIKA KITA DIHADAPKAN PADA KONDISI HARUS MEMILIH A ATAU B,
DULU KITA BISA MENGENALI GAYA BAHASA YANG ANEH (TIDAK
BIASA)

SEKARANG AI DAPAT MEMBANTU MENGHASILKAN:

- BAHASA YANG SANGAT NATURAL,
- SUARA YANG MENYERUPAI ATASAN,
- FOTO PROFIL YANG MEYAKINKAN,
- VIDEO YANG TAMPAK AUTENTIK

KEAMANAN TIDAK LAGI HANYA TENTANG MENJAGA KERAHASIAAN DATA.
KEAMANAN JUGA TENTANG MENJAGA INTEGRITAS KEPUTUSAN

DEEPPFAKE BUKAN MASALAH TEKNOLOGI, AI INI ADALAH MASALAH KEPERCAYAAN

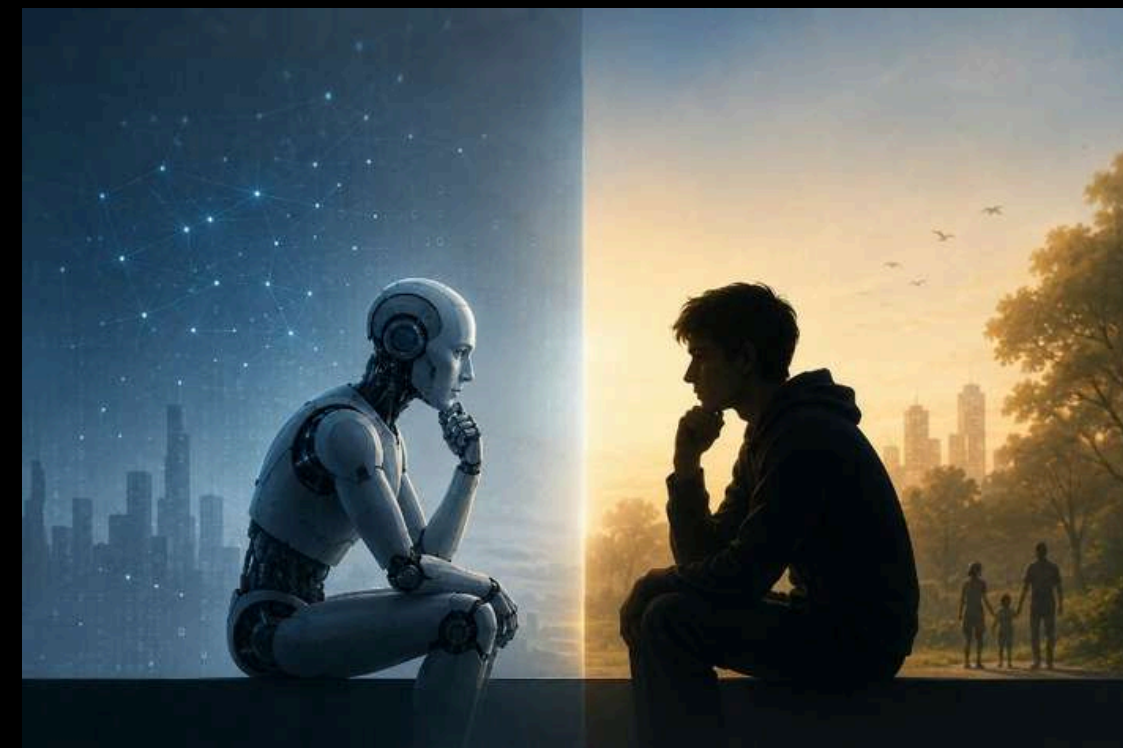
KETIKA BUKTI DAPAT DIPALSUKAN, APA YANG TERJADI DENGAN KEPERCAYAAN?

DULU, SEEING IS BELIEVING
SEKARANG, SEEING IS EVIDENCE, BUT NOT NECESSARILY TRUTH

IDENTITAS TIDAK BOLEH LAGI DIVERIFIKASI HANYA BERDASARKAN APA YANG
TERLIHAT ATAU TERDENGAR.

APA SOLUSINYA?

BE HUMAN!



“JANGAN PERNAH MEMBERIKAN DATA KE AI” (TELALU KLASIK!)

PEGAWAI PASTI AKAN MENGGUNAKAN AI
MASYARAKAT AKAN MENGGUNAKAN AI

PERTANYAANNYA BUKAN APAKAH BOLEH MENGGUNAKAN AI?”
TETAPI, INFORMASI SEPERTI APA YANG BOLEH DIGUNAKAN AI, UNTUK TUJUAN
APA, DENGAN RISIKO APA, DAN DENGAN KONTROL APA?

AI DATA CLASSIFICATION, MISALNYA:

-  PUBLIK
-  INTERNAL
-  SENSITIF
-  SANGAT SENSITIF

BUKAN “AI BOLEH ATAU TIDAK BOLEH”.
YANG BENAR ADALAH “DATA APA, DIGUNAKAN PADA AI APA,
UNTUK TUJUAN APA, DAN DENGAN PENGAMANAN APA.”

PROMPT ADALAH PERINTAH, TETAPI JUGA JEJAK DIGITAL

BANYAK ORANG MENGANGGAP PROMPT HANYA PERTANYAAN.

PADAHAL PROMPT DAPAT MENGANDUNG:

- NAMA,
- IDENTITAS,
- DOKUMEN,
- KONDISI ORGANISASI,
- INFORMASI INTERNAL,
- DATA PELANGGAN,
- STRATEGI,
- KONTEKS PEKERJAAN.

PROMPT ADALAH BENTUK BARU DARI INPUT DATA

JIKA KITA MEMASUKKAN SESUATU KE AI:

KITA BUKAN HANYA SEDANG BERTANYA.

KITA SEDANG:

“MEMBERIKAN KONTEKS”

SEMAKIN BANYAK KONTEKS YANG DIBERIKAN,
SEMAKIN BESAR PULA POTENSI INFORMASI
SENSITIF YANG IKUT TERBAWA.

AI TIDAK HARUS BERBOHONG UNTUK MEMBUAT KITA SALAH

AI BISA MENGHASILKAN JAWABAN YANG SALAH TANPA MEMILIKI NIAT UNTUK MENIPU.

MISINFORMATION
INFORMASI SALAH TANPA HARUS ADA NIAT JAHAT.

DISINFORMATION
INFORMASI SALAH YANG SENGAJA DIBUAT UNTUK MENYESATKAN.

AI-GENERATED MISINFORMATION
INFORMASI SALAH YANG DIHASILKAN AI, BAHKAN TANPA MANUSIA BERMAKSUD MELAKUKAN PENIPUAN.

KEMUDIAN PERTANYAAN:
“KALAU MESIN MENGHASILKAN KESALAHAN DENGAN BAHASA YANG SANGAT MEYAKINKAN, APAKAH MANUSIA MASIH MAMPU MEMBEDAKAN ANTARA CONFIDENT DAN CORRECT?”



“HALUSINASI” BUKAN SEKADAR ERROR

“Mengapa manusia begitu mudah mempercayai halusinasi AI?”

**AI menjawab seperti seseorang yang:
lancar, percaya diri, sistematis, argumentatif.**

**Problemnya:
Semakin lancar sebuah jawaban, semakin mudah
manusia menganggapnya benar.**

**Padahal:
Kelancaran bahasa bukan bukti kebenaran.**



“AI LITERACY” SEBENARNYA BUKAN KEMAMPUAN MEMBUAT PROMPT

AI Literacy = tahu kapan menggunakan AI, tahu kapan tidak menggunakan AI, tahu informasi apa yang boleh diberikan, tahu bagaimana memverifikasi hasil, tahu kapan harus mempertanyakan hasil, tahu konsekuensi ketika AI salah.

Jadi:

Prompt engineering adalah skill teknis.

Judgment engineering adalah skill manusia.

“HUMAN IN THE LOOP” HARUS BERUBAH MENJADI “HUMAN WITH RESPONSIBILITY”

Manusia seperti apa?

Kalau manusia hanya “copy → paste → approve”

maka sebenarnya manusia hanya menjadi rubber stamp

Jadi prinsip yang lebih kuat:

Human-in-the-loop tidak berarti manusia sekadar berada di akhir proses.

Manusia harus memahami, memverifikasi, dan bertanggung jawab atas keputusan yang dihasilkan dengan bantuan AI.



AI SEHARUSNYA MENAMBAH “AUGMENTATION”, BUKAN MENGHILANGKAN “JUDGMENT”

AI

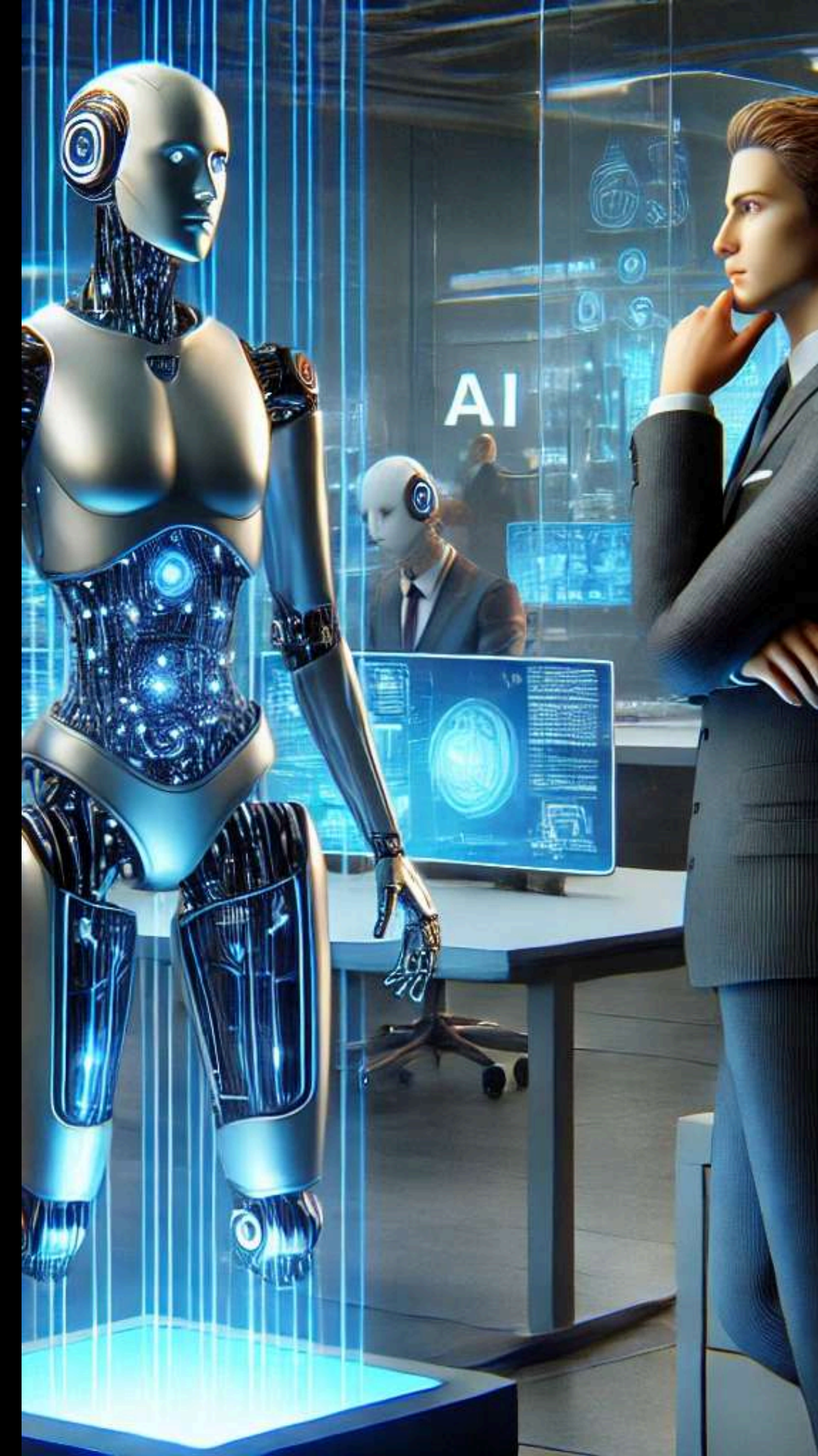


MEMBANTU MENCARI POLA, MEMBANTU
MERINGKAS, MEMBANTU MENGHASILKAN
ALTERNATIF, MEMBANTU SIMULASI



MANUSIA, MEMAHAMI KONTEKS, MEMERIKSA
FAKTA, MEMPERTIMBANGKAN DAMPAK,
MENGAMBIL KEPUTUSAN, MEMIKUL TANGGUNG
JAWAB

“AI BOLEH MEMBANTU BERPIKIR.
TETAPI AI TIDAK BOLEH MENGAMBIL ALIH TANGGUNG JAWAB BERPIKIR”



UNTUK PEGAWAI PEMERINTAH: “PUBLIC DATA + AI $\neq$ AUTOMATICALLY SAFE”



Informasi yang tersedia secara publik belum tentu aman untuk diproses sembarangan. Karena konteks dapat mengubah risiko.

Misalnya satu informasi “Nama pejabat X.” mungkin publik, tetapi jika digabung dengan jadwal, lokasi, struktur organisasi, kebiasaan, dokumen internal, kontak, pola perjalanan, maka terbentuk information mosaic yaitu potongan informasi kecil dapat menghasilkan gambaran yang sangat sensitif ketika digabungkan.

“AI MENGUBAH NILAI DATA: DATA KECIL BISA MENJADI INFORMASI BESAR”

Dulu: Data kecil → dampak kecil

Sekarang: Data kecil + AI + data lain → insight besar

AI mampu menggabungkan, mengelompokkan, mencari korelasi, menemukan pola, menyimpulkan. Sehingga risiko bukan hanya pada data yang kita berikan, tetapi juga pada apa yang dapat disimpulkan dari data tersebut.



“AI PERSONALIZATION” PUNYA SISI GELAP

Semakin AI mengenal kita:

AI semakin tahu cara kita bekerja, cara kita menulis, apa yang kita cari, apa yang kita sukai, bagaimana kita mengambil keputusan.

Personalisasi membuat AI lebih berguna, tetapi semakin personal AI, semakin besar pula konsekuensi jika konteks personal tersebut disalahgunakan atau bocor.

Jadi:

**Convenience ↔ Privacy
Selalu ada trade-off.**

AI DAN SOCIAL ENGINEERING: SERANGAN MENJADI PERSONAL

Dulu phishing bunyinya “Dear customer...” tetapi sekarang AI memungkinkan pesan yang jauh lebih personal. Misalnya “Pak Budi, terkait rapat koordinasi yang kemarin...”

AI memungkinkan penyerang membuat serangan yang lebih personal, lebih kontekstual, lebih persuasif, lebih cepat, lebih murah. Maka AI menurunkan biaya melakukan social engineering.



“THE NEW FIREWALL IS NOT SOFTWARE, IT IS SKEPTICISM”

Firewall melindungi jaringan, antivirus melindungi perangkat, encryption melindungi data.

Tetapi siapa yang melindungi keputusan manusia?

Jawabannya:

Critical thinking + verification + healthy skepticism

Bukan curiga kepada semua hal.



BUAT “5 PERTANYAAN SEBELUM PERCAYA PADA AI”

P

P — Purpose
Untuk apa AI digunakan?

A

A — Accuracy
Bagaimana memastikan jawabannya benar?

U

U — User/Data
Data siapa yang saya masukkan?

S

S — Security
Apa risikonya jika informasi ini bocor atau disalahgunakan?

E

E — Effect
Apa dampaknya jika jawaban AI salah?

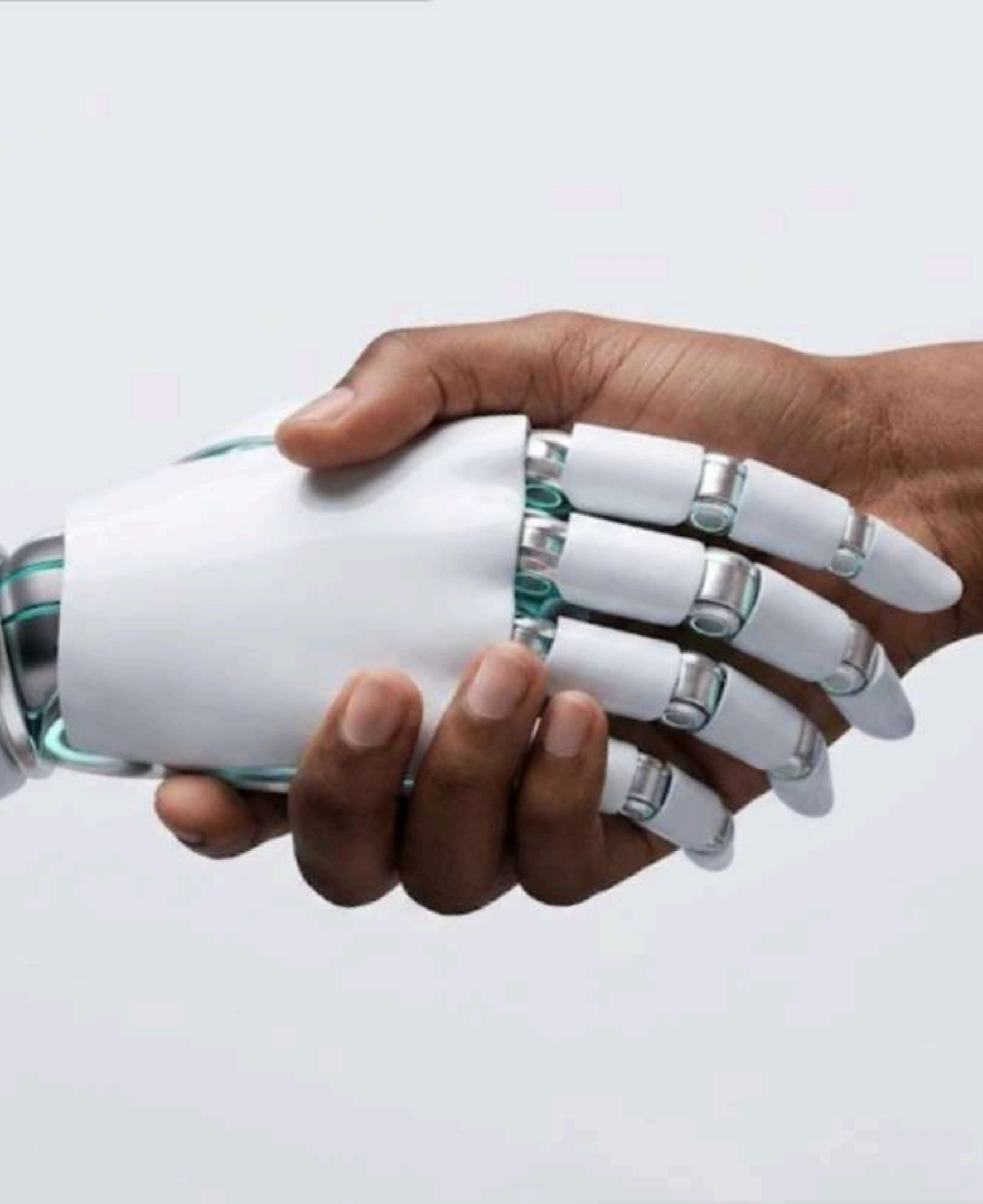
“JANGAN TANYAKAN APA YANG BISA AI LAKUKAN”

“Apa yang seharusnya tidak kita serahkan kepada AI?”

Misalnya:

keputusan yang membutuhkan empati, keputusan yang memiliki konsekuensi hukum, keputusan yang menyangkut hak seseorang, keputusan berdasarkan data yang belum diverifikasi, keputusan yang membutuhkan akuntabilitas manusia.





MASALAH BESAR MASA DEPAN BUKAN “AI MENGGANTIKAN MANUSIA”

**Bukan:
AI vs Human**

**Tetapi:
Human with AI vs Human without AI**

**“Manusia seperti apa yang akan muncul ketika AI
menjadi partner berpikir sehari-hari?”**

**Apakah manusia menjadi lebih kritis? lebih cepat?
lebih kreatif?**

**Atau justru lebih malas memeriksa? lebih
bergantung? kehilangan kemampuan menulis?
kehilangan kemampuan mengambil keputusan?**

PENUTUP

“KITA TIDAK PERLU MENJADI TAKUT PADA AI”

AI bukan sesuatu yang harus kita takuti. AI adalah sesuatu yang harus kita pahami.

USE AI. Gunakan AI untuk meningkatkan kemampuan.

VERIFY AI. Periksa apa yang AI hasilkan.

OWN THE DECISION. Manusia tetap bertanggung jawab atas keputusan.



“AI BOLEH TERLIHAT LEBIH CERDAS DARI KITA DALAM BANYAK HAL. TETAPI TANGGUNG JAWAB ATAS APA YANG KITA LAKUKAN TETAP BERADA DI TANGAN KITA. DI ERA KETIKA MESIN DAPAT MENGHASILKAN INFORMASI DALAM HITUNGAN DETIK, KEMAMPUAN PALING BERTHARGA MANUSIA BUKAN LAGI SEKADAR MENGETAHUI LEBIH BANYAK, MELAINKAN MENGETAHUI APA YANG LAYAK DIPERCAYA.”

CONTACT US



KOTA BOGOR

Email

rikson.gultom@bssn.go.id

Instagram

[@rikson.gultom.bssn](https://www.instagram.com/rikson.gultom.bssn)

THANK YOU