KD-5

Robi Się Samo
stan na XI 2026

# 7 zasad bezpiecznego AI

**Siedem zasad na każdy dzień z AI – w pracy i w domu.**




1. **AI to zdolny stażysta, nie wyrocznia.** AI szykuje, Ty podpisujesz. Liczby, nazwiska, daty, przepisy i cytaty sprawdzasz u źródła. Naczelny Sąd Administracyjny dostał już pisma z wyrokami, których nie ma albo które mówią co innego (2026).
2. **Zanim wkleisz – czyje to dane i jakie to konto?** Dane innych ludzi i dokumenty firmy nie trafiają do prywatnego czatu. Hasła nie trafiają nigdzie. Używasz tylko oficjalnej aplikacji producenta: OpenAI, Google, Anthropic albo Microsoft. Część głośnych wycieków rozmów z AI poszła przez nieoficjalne aplikacje i przycisk „udostępnij".
3. **Pośpiech + emocje + pieniądze = rozłącz się.** Oddzwaniasz na numer, który znasz. Z bliskimi ustalasz hasło rodzinne. Głos i twarz bliskiej osoby da się dziś podrobić z niewielu nagrań z internetu.
4. **Znana twarz obiecuje szybki zysk z inwestycji? Traktuj to jak oszustwo.** Nie klikasz. Zgłaszasz: SMS – przekaż na 8080; strona albo mail – incydent.cert.pl.
5. **Poproś AI o zdanie sceptyka, nie o pochwałę.** Napisz: „Wskaż trzy słabe punkty mojego planu". W badaniu z „Science" (2026) modele przyznawały ludziom rację prawie o połowę częściej niż inni ludzie.
6. **Agentowi daj klucz do jednej szuflady, nie do całego biura.** Agent AI to model, który dostał narzędzia i cel. Kolejne kroki robi sam, a ważne ruchy zatwierdzasz Ty. Trzy hamulce: najmniejsze dostępy · szkice zamiast wysyłki · Ty zatwierdzasz wysyłkę, płatność, usuwanie i publikację.
7. **Nie oddawaj AI całego myślenia – i odpowiadaj za wynik.** Ważne umiejętności ćwiczysz też bez AI. Realistyczne zdjęcie albo film z AI oznaczasz w publikacji. Cudzej twarzy i głosu nie używasz bez zgody. Ważne rozmowy o bliskich i emocjach prowadzisz z ludźmi. W kryzysie: 116 123, całą dobę.

**Wszystko, co musisz wiedzieć o AI** · Kompendium Robi Się Samo · Stan na XI 2026
Źródła: Policja i INTERPOL (2026) · CERT Polska · Ministerstwo Cyfryzacji · NSA (I FZ 104/26, I OSK 590/26) · „Science" (2026) · doniesienia o wyciekach (2025–2026) · 116sos.pl · wpisy KD.12–KD.18, KD.20 w „Skąd to wiemy"
Możesz wydrukować i przekazać bez zmian · CC BY-NC-ND 4.0 · **robisiesamo.pl/kompendium**

robisiesamo.pl/
kompendium