



Met de opkomst van artificiële intelligentie (AI, ook kunstmatige intelligentie genoemd), is het belangrijk om bij te blijven. Volg onderstaande tips om veilig met AI om te gaan.

1 ➤ **IMPLEMENTEER EEN ACCEPTABEL GEBRUIKERSBELEID VOOR AI**

Maak afspraken over het gebruik van AI, zoals chatbots. Leg vast welke informatie wel/niet gedeeld mag worden met AI. Zorg dat medewerkers dit beleid steeds kunnen raadplegen. Deel bijvoorbeeld geen PII (persoonlijk identificeerbare informatie), gevoelige bedrijfsinformatie, wachtwoorden, Intellectueel eigendom (IP), financiële gegevens en sourcecode.

2 ➤ **BEN EN BLIJF OP DE HOOGTE VAN RELEVANTE WET- EN REGELGEVING**

Wet- en regelgeving, zoals de Cyberbeveiligingswet en de Europese AI Act, bevatten regels die bepalen hoe organisaties gegevens verzamelen, verwerken en beschermen, vooral bij AI-toepassingen.

3 ➤ **KIES BETROUWBARE AI-OPLOSSINGEN**

Gebruik AI-tools van gerenommeerde bedrijven. Dit vermindert de kans op fouten, datalekken en andere veiligheidsrisico's. Voorbeelden zijn: ChatGPT (OpenAI), Claude (Anthropic), Gemini (Google) en Copilot (Microsoft). Copilot kan nooit zomaar data inzien waartoe de individuele gebruiker zelf ook geen toegang heeft. Een Europees alternatief is Mistral.

4 ➤ **BEPERK TOEGANG**

Zorg ervoor dat alleen geautoriseerde gebruikers toegang hebben tot AI-systemen. Implementeer sterke authenticatiemethoden, zoals tweefactorauthenticatie, om de beveiliging te versterken.

5 ➤ **TRAIN MEDEWERKERS IN HET VEILIGE GEBRUIK VAN AI**

Train medewerkers regelmatig om veilig met AI om te gaan. Houd hen op de hoogte van de nieuwste dreigingen. Volg hiervoor bijvoorbeeld NCSC advisories, CISA advisories, Security.nl, Tweakers.net, BleepingComputer.com.

6 ➤ **IMPLEMENTEER CONTINUE MONITORING**

Zet systemen op voor continue monitoring van AI-toepassingen om ongewone activiteiten te detecteren die een veiligheidsrisico kunnen vormen.



Meer informatie over dit onderwerp deelt Cyber Weerbaarheidscentrum Brainport met haar participanten. Ook lid worden van deze stichting zonder winstoogmerk? Bezoek www.cwbrainport.nl of mail naar info@cwbrainport.nl.

Met dank aan