

AI-richtlijnen voor je bedrijf

**Duidelijke regels. Zelfzekere medewerkers.
Verantwoord AI-gebruik op het werk.**

Een praktische leidraad om vast te leggen
hoe je team AI wel en niet mag gebruiken.

**Praktische AI.
Menselijk oordeel.**

A decorative graphic consisting of three concentric, partial rainbow arcs in yellow, teal, and dark teal, positioned on the right side of the dark teal background.

20 onderdelen voor de AI-richtlijnen van je bedrijf

Maak deze richtlijnen op maat

Goede AI-richtlijnen sluiten aan bij hoe jouw bedrijf in de praktijk werkt.

Kies wat relevant is voor jouw bedrijf

Elke organisatie gebruikt AI op haar eigen manier. Sommige onderdelen van dit werkboek zijn meteen relevant voor je team; andere spelen nauwelijks een rol in het dagelijkse werk. Je hoeft niet elke voorgestelde regel over te nemen of elk onderdeel in te vullen.

Gebruik deze leidraad gericht. Begin bij de onderwerpen die het belangrijkste zijn voor jouw bedrijf, de informatie waarmee je werkt en de manier waarop je medewerkers AI gebruiken. Pas de formuleringen aan, kies passende opties en voeg voorbeelden uit je eigen werkomgeving toe. Laat weg wat niet van toepassing is, maar zorg dat je richtlijnen je verantwoordelijkheden en risico's voldoende afdekken.

Kies voor duidelijke, bruikbare richtlijnen

Een gerichte set regels die medewerkers begrijpen en kunnen toepassen, is nuttiger dan een lang document dat moeilijk te volgen is. Bespreek je ontwerp met de betrokken personen in je organisatie voordat je het deelt.

Help medewerkers de regels te begrijpen

Duidelijke regels werken het best als mensen begrijpen waarom ze er zijn. Ready AI Go biedt verschillende praktische opleidingen waarmee medewerkers met meer vertrouwen AI leren gebruiken en de beperkingen en risico's leren herkennen.

De onderwerpen omvatten dagelijks AI-gebruik, prompts schrijven, privacy, AI-antwoorden controleren en dreigingen met AI herkennen. Combineer de opleidingen met je bedrijfsrichtlijnen, zodat medewerkers de regels ook in de praktijk kunnen toepassen.

Deel en onderhoud je richtlijnen digitaal

Zodra je richtlijnen vastliggen, kun je ze invoeren in Ready AI Go en digitaal beschikbaar maken voor iedereen in je bedrijf. Zo vinden medewerkers op één centrale plek de regels die gelden voor hun werk.

Door je richtlijnen in Ready AI Go te beheren, kun je ze eenvoudig delen en aanpassen wanneer je tools, werkwijzen of bedrijfsbehoeften veranderen. Kijk ze regelmatig na, zodat je team steeds over duidelijke, actuele richtlijnen beschikt.

Kies wat van toepassing is. Maak het duidelijk. Help je team ermee aan de slag.

Bepaal de richting

Een praktische leidraad om vast te leggen hoe medewerkers AI wel en niet mogen gebruiken op het werk.

Zo gebruik je dit werkboek

Stem de regels af op je organisatie, gegevens, tools en risicoprofiel. Vul de velden in en kies de opties die van toepassing zijn. Dit is een werksjabloon, geen afgewerkt beleid. Laat de tekst vóór publicatie nakijken door de verantwoordelijken voor juridische zaken, privacy, beveiliging en compliance.

01 Doel van deze richtlijnen

Leg uit waarom je AI-richtlijnen invoert. Help medewerkers AI verantwoord te gebruiken, met duidelijke grenzen en ruimte voor menselijk oordeel.

Onze organisatie staat medewerkers toe AI te gebruiken voor:

Voorbeelden: ideeën bedenken, documenten opstellen, samenvatten, teksten verbeteren, niet-gevoelige inhoud vertalen, goedgekeurde datasets analyseren, programmeren, onderzoek en repetitief werk automatiseren.

Vorgesteld uitgangspunt

Medewerkers mogen AI gebruiken zolang dit geen vertrouwelijke informatie blootlegt, onaanvaardbare risico's creëert, bedrijfsregels schendt of het vereiste menselijke oordeel vervangt.

02 Voor wie gelden deze richtlijnen?

Deze richtlijnen gelden voor:

- | | |
|---|---|
| ☐ Alle medewerkers | ☐ Externe opdrachtnemers |
| ☐ Freelancers | ☐ Stagiairs |
| ☐ Externe partners | ☐ Alleen bepaalde afdelingen |

Ze gelden bij AI-gebruik:

- | | |
|---|---|
| ☐ Op bedrijfstoestellen | ☐ Op privét toestellen voor het werk |
| ☐ Via bedrijfsaccounts | ☐ Via persoonlijke AI-accounts voor het werk |
| ☐ In contact met klanten | ☐ Voor intern werk |

Andere personen, afdelingen of situaties:

Kies je AI-tools

Geef medewerkers een duidelijke lijst met toegestane tools, toepassingen en beperkingen.

Wees concreet. 'Gebruik betrouwbare AI-tools' laat te veel ruimte voor interpretatie.

03 Welke AI-tools mogen medewerkers gebruiken?

Tool / account	Toegestaan gebruik	Beperkingen

Mogelijke beperkingen: alleen beheerde bedrijfsaccounts; alleen de bedrijfsomgeving; geen gratis of publieke versie; geen koppelingen met derden; alleen niet-vertrouwelijke informatie; alleen goedgekeurde afdelingen.

Tools waarvoor toestemming nodig is

Verantwoordelijke persoon / team:

Tools en voorwaarden waarvoor toestemming nodig is:

Verboden tools

Deze AI-tools mogen niet voor het werk worden gebruikt:

Leg de grens vast
Medewerkers mogen geen nieuwe AI-tool invoeren in bedrijfsprocessen zonder toestemming van de hieronder vermelde persoon of het team.

Wie geeft toestemming?

Bepaal welke gegevens in AI mogen

Medewerkers hoeven niet telkens ingewikkelde privacy- en beveiligingsafwegingen te maken wanneer ze een AI-tool openen.

04 Welke informatie mag worden ingevoerd?

GROEN / Toegestane informatie

Informatie die medewerkers in goedgekeurde AI-systemen mogen invoeren. Voorbeelden: openbare informatie, gepubliceerde webteksten, productbeschrijvingen, marketingmateriaal, algemene vragen, fictieve voorbeelden en specifiek goedgekeurde, niet-gevoelige interne informatie.

Onze GROENE informatie omvat:

ORANJE / Informatie met beperkingen

Alleen gebruiken in specifiek goedgekeurde tools of onder vastgelegde voorwaarden. Voorbeelden: interne documenten, processen, vergadernotities, bedrijfsresultaten, broncode, onderzoek en geanonimiseerde klantgegevens.

Onze ORANJE informatie omvat:

ORANJE: goedgekeurde tools en vereiste voorwaarden:

ROOD / Nooit in publieke of niet-goedgekeurde AI

Voorbeelden: wachtwoorden, API-sleutels, inloggegevens, vertrouwelijke klant- of persoonsgegevens, medische of bankgegevens, personeelsdossiers, contracten, bedrijfsgeheimen, strategie, eigen datasets, beveiligingsarchitectuur, niet-openbare financiële informatie en gevoelige intellectuele eigendom.

Onze RODE informatie omvat:

RODE informatie mag alleen worden ingevoerd als zowel het systeem als de specifieke toepassing uitdrukkelijk is goedgekeurd.

Uitzonderingen voor ROOD mogen alleen worden goedgekeurd door:

Bescherm mensen en bedrijfsdata

Leg duidelijke regels vast voor informatie over medewerkers, klanten, potentiële klanten, partners en je organisatie.

05 Persoonsgegevens en klantinformatie

Voor persoonsgegevens geldt:

- | | |
|---|---|
| ☐ Nooit invoeren in AI-systemen | ☐ Alleen invoeren in goedgekeurde systemen |
| ☐ Alleen gebruiken na correcte anonimisering | ☐ Alleen gebruiken in goedgekeurde situaties |

Andere voorwaarden / goedgekeurde situaties:

Persoonsgegevens die medewerkers nooit mogen invoeren:

Twijfel je of informatie persoonlijk of gevoelig is? Upload ze niet. Vraag eerst advies aan de hieronder vermelde persoon of het team.

Contactpersoon voor privacy:

06 Vertrouwelijke bedrijfsinformatie

Informatie in een AI-chat kopiëren kan betekenen dat je ze met een ander systeem of een andere aanbieder deelt. Bepaal wat jouw organisatie als vertrouwelijk beschouwt.

Dit mag niet worden ingevoerd in niet-goedgekeurde AI-systemen:

- | | |
|--|---|
| ☐ Interne financiële informatie | ☐ Strategie- of bestuursdocumenten |
| ☐ Contracten | ☐ Klantinformatie |
| ☐ Personeelsinformatie | ☐ Intellectuele eigendom |
| ☐ Productplannen | ☐ Interne e-mails |
| ☐ Broncode | ☐ Beveiligingsinformatie |
| ☐ Inloggegevens of toegangssleutels | ☐ Ongepubliceerd onderzoek |

Andere vertrouwelijke informatie / voorbeelden uit ons bedrijf:

De mens blijft verantwoordelijk

AI mag medewerkers ondersteunen. Zij blijven verantwoordelijk voor hun werk en de beslissingen die ze nemen.

07 Controleer informatie die AI genereert

Beschouw AI-antwoorden niet automatisch als feitelijk juist. Controleer belangrijke informatie voordat je erop vertrouwt.

Controleer feiten, cijfers, citaten, bronnen, verwijzingen, klantinformatie en zakelijke aanbevelingen. Wees extra zorgvuldig met juridische, financiële, medische, technische en beveiligingsinformatie.

Voordat AI-gegenereerd werk extern wordt gebruikt, moeten medewerkers:

- | | |
|---|--|
| ☐ Het zelf nakijken | ☐ Belangrijke feitelijke claims controleren |
| ☐ Vermelde bronnen controleren | ☐ Een collega laten meekijken |
| ☐ Toestemming van hun leidinggevende krijgen | ☐ Bestaande kwaliteitscontroles volgen |

Aanvullende controlevereisten:

08 Menselijke verantwoordelijkheid

AI mag niet zelfstandig definitieve beslissingen nemen over:

- | | |
|--|---|
| ☐ Aanwerving of ontslag | ☐ Beoordeling van medewerkers |
| ☐ Promotie of verloning | ☐ Of klanten in aanmerking komen |
| ☐ Krediet of financiële zaken | ☐ Juridische zaken |
| ☐ Veiligheidskritieke situaties | ☐ Medische zaken |
| ☐ Beveiligingsincidenten | ☐ Anders: _____ |

Toegestaan AI-gebruik bij deze activiteiten:

- | | |
|--|--|
| ☐ Geen AI-gebruik | ☐ Alleen ondersteuning bij de voorbereiding |
| ☐ Voorstellen; een mens beslist | ☐ Alleen volgens een goedgekeurde procedure |

Aanvullende regels / wie moet de beslissing nemen?

Stel regels voor externe content

Bepaal wat medewerkers mogen maken, publiceren of naar klanten sturen, en welke controles vooraf nodig zijn.

09 AI-content voor klanten

AI-gegenereerde content voor klanten:

- | | |
|--|---|
| ☐ Is toegestaan na menselijke controle | ☐ Vereist toestemming van een leidinggevende |
| ☐ Is beperkt tot bepaalde soorten content | ☐ Mag niet worden gebruikt |

Toegestane soorten content / andere voorwaarden:

AI-gegenereerde content mag niet worden gebruikt voor:

Vóór publicatie of externe verzending moeten medewerkers:

10 AI-gegenereerde beelden, audio en video

Medewerkers mogen generatieve AI gebruiken voor:

- | | |
|--|---|
| ☐ Marketingbeelden | ☐ Interne presentaties |
| ☐ Conceptontwikkeling | ☐ Audio |
| ☐ Video | ☐ Stemgeneratie |

Medewerkers mogen niet:

- ☐ Zich voordoen als bestaande personen
- ☐ Misleidende content of valse klantgetuigenissen maken
- ☐ Gegenereerde media voorstellen als bewijs van iets dat niet is gebeurd
- ☐ Iemands beeltenis gebruiken zonder de nodige toestemming

Andere toegestane toepassingen / aanvullende mediaregels:

Bescherm intellectuele eigendom

Behandel creatief werk en code die met AI tot stand komen even zorgvuldig als ander bedrijfswerk.

11 Auteursrecht en intellectuele eigendom

Ga er niet van uit dat AI-gegenereerd materiaal zomaar commercieel bruikbaar is. Controleer vooraf:

- ☐ Is er materiaal van derden overgenomen?
- ☐ Komen er logo's, merken of auteursrechtelijk beschermde personages in voor?
- ☐ Wordt vertrouwelijke intellectuele eigendom van het bedrijf gedeeld?
- ☐ Zijn er licentievoorwaarden van toepassing?
- ☐ Mag het resultaat wettelijk voor het beoogde doel worden gebruikt?

Onze regels voor AI-gegenereerde intellectuele eigendom:

12 AI bij softwareontwikkeling

Goedgekeurde programmeerassistenten / omgevingen:

Ontwikkelaars mogen dit niet invoeren:

- | | |
|--|---|
| ☐ Inloggegevens van productiesystemen | ☐ API-sleutels |
| ☐ Klantgegevens | ☐ Bedrijfseigen broncode |
| ☐ Beveiligingsgevoelige code | ☐ Interne architectuurinformatie |

AI-gegenereerde code moet:

- | | |
|--|--|
| ☐ Door een ontwikkelaar worden nagekeken | ☐ Bestaande testprocedures doorstaan |
| ☐ Beveiligingscontroles doorstaan | ☐ Op licentievoorwaarden worden gecontroleerd |
| ☐ De gebruikelijke codecontrole doorlopen | ☐ Anders: _____ |

Aanvullende beperkingen of ontwikkelregels:

Herken dreigingen. Stel grenzen.

AI kan oplichting overtuigender maken. Geef medewerkers een duidelijke controleprocedure en heldere grenzen.

13 Oplichting met AI en verdachte content

Controleer ongewone verzoeken over overschrijvingen, betaalgegevens, gewijzigde bankrekeningen, wachtwoordherstel, inloggegevens of vertrouwelijke bestanden. Wees alert bij onverwachte verzoeken van leidinggevenden of klanten, ook bij overtuigende stemmen en beelden.

Bij een verdacht verzoek volgt de medewerker deze stappen:

1.

2.

3.

Meld vermoedelijke fraude met AI aan:

14 Waarvoor medewerkers AI nooit mogen gebruiken

- ☐ Verboden bedrijfsinformatie uploaden
- ☐ Klant informatie uploaden zonder toestemming
- ☐ Beveiligingsmaatregelen omzeilen
- ☐ Schadelijke software genereren
- ☐ Frauduleuze of misleidende content maken
- ☐ Zich voordoen als een andere medewerker of klant
- ☐ Zonder toestemming geautomatiseerde beslissingen nemen
- ☐ AI-resultaten versturen zonder de vereiste controle
- ☐ Niet-goedgekeurde AI-tools gebruiken voor het werk
- ☐ AI-onderzoek zonder controle als vaststaand feit voorstellen

Andere verboden toepassingen in ons bedrijf:

1.

2.

3.

Maak vragen stellen en melden eenvoudig

Goed beleid geeft medewerkers een duidelijke volgende stap bij twijfel of wanneer er iets misgaat.

15 Wat doen medewerkers bij twijfel?

Weet je niet zeker of informatie in een AI-systeem mag worden ingevoerd? Voer ze pas in nadat je dit hebt nagevraagd.

Vragen: naam / team en e-mailadres / kanaal:

Vraag toestemming vóór je een nieuwe tool gebruikt, gevoelige gegevens invoert, een belangrijke beslissing automatiseert, AI met een ander bedrijfssysteem koppelt of een nieuw AI-proces voor klanten invoert. Vraag advies als je twijfelt of een toepassing aan de regels voldoet.

16 Fouten en incidenten melden

Meld onbedoelde uploads van vertrouwelijke of klantinformatie, gelekte inloggegevens, vermoedelijke fraude met AI, extern gebruikte schadelijke of misleidende AI-resultaten en niet-goedgekeurde AI-koppelingen.

Neem bij een incident onmiddellijk contact op met:

Vermeld in de melding	Details
Gebruikte AI-tool	
Gedeelde informatie	
Datum en tijdstip	
Mogelijk getroffen personen	
Reeds ondernomen actie	

Moedig snelle melding aan
Fouten kunnen gebeuren. Medewerkers moeten onbedoeld verkeerd gebruik snel melden en mogen het niet proberen te verbergen.

Maak van richtlijnen een gewoonte

Duid een verantwoordelijke aan, leg de regels uit en plan regelmatige herzieningen.

17 Opleidingsvereisten

Alle medewerkers moeten deze opleidingen volgen:

- | | |
|---|---|
| ☐ Basiskennis van AI | ☐ AI en privacy |
| ☐ Prompts schrijven | ☐ Veilig omgaan met AI |
| ☐ Oplichting met AI herkennen | ☐ AI-hallucinaties herkennen |
| ☐ AI-opleiding voor de eigen functie | ☐ Anders: _____ |

De opleiding moet worden gevolgd:

- | | |
|---|--|
| ☐ Bij indiensttreding | ☐ Vóór het gebruik van AI-tools |
| ☐ Jaarlijks | ☐ Via doorlopende korte opleidingen |
| ☐ Bij belangrijke wijzigingen in het AI-beleid | ☐ Anders: _____ |

18 Wie is verantwoordelijk voor het AI-beleid?

Verantwoordelijke voor het AI-beleid — naam / afdeling:

Deze persoon is verantwoordelijk voor:

- | | |
|--|--|
| ☐ De lijst met goedgekeurde tools bijhouden | ☐ Deze richtlijnen actualiseren |
| ☐ Nieuwe AI-toepassingen beoordelen | ☐ AI-incidenten afhandelen |
| ☐ Opleidingen voor medewerkers coördineren | ☐ AI-ontwikkelingen opvolgen |

Andere verantwoordelijkheden:

19 Herzie je richtlijnen regelmatig

Herzie de richtlijnen:

- | | |
|--|--|
| ☐ Om de 3 maanden | ☐ Om de 6 maanden |
| ☐ Jaarlijks | ☐ Bij invoering van een belangrijk AI-systeem |
| ☐ Bij gewijzigde vereisten of wetgeving | ☐ Na een AI-gerelateerd incident |

Laatst herzien: _____ **Volgende herziening:** _____

Verantwoordelijke voor de herziening:

Jouw AI-richtlijnen in één oogopslag

Vul deze pagina in zodra je beleid vastligt. Deel ze met medewerkers als praktisch overzicht dat ze in twee minuten kunnen lezen.

Organisatie: _____ Versie / datum: _____

Onze medewerkers mogen AI gebruiken voor:

01 Welke tools mag ik gebruiken?

Je mag deze tools gebruiken:

02 Welke informatie mag ik in AI invoeren?

Je mag dit invoeren:

03 Welke informatie mag nooit in AI?

Voer dit nooit in:

04 Wat moet ik controleren?

Controleer altijd / vereiste beoordelaar:

05 Wat doe ik bij twijfel?

Vraag het aan — naam / team en contactgegevens:

Twijfel je? Vraag eerst advies voordat je iets uploadt.

Klaar om ermee aan de slag te gaan?

Controleer vóór publicatie of je richtlijnen de belangrijkste vragen beantwoorden.

- ☐ Weten medewerkers welke AI-tools zijn toegestaan?
- ☐ Weten medewerkers welke AI-tools verboden zijn?
- ☐ Is duidelijk welke informatie nooit in AI mag worden ingevoerd?
- ☐ Zijn er regels voor persoonsgegevens en klantgegevens?
- ☐ Begrijpen medewerkers dat AI fouten kan maken?
- ☐ Is menselijke controle bij belangrijke beslissingen verplicht?
- ☐ Zijn er regels voor externe AI-resultaten en klantcommunicatie?
- ☐ Weten medewerkers hoe ze een fout met AI moeten melden?
- ☐ Is iemand verantwoordelijk voor het beheer van deze richtlijnen?
- ☐ Hebben medewerkers een opleiding over de regels gevolgd?
- ☐ Is er een datum vastgelegd om de richtlijnen opnieuw te bekijken?

Is het antwoord meermaals 'nee'? Dan volstaat een beleid alleen waarschijnlijk niet. Medewerkers moeten begrijpen waarom de regels er zijn en hoe ze die in concrete situaties toepassen.

Van AI-beleid naar de praktijk

Richtlijnen opstellen is de eerste stap. Medewerkers helpen om ze te begrijpen en na te leven, is de volgende.

Ready AI Go vertaalt AI-regels naar praktische kennis met korte, doorlopende opleidingen over AI-gebruik, prompts schrijven, privacy, hallucinaties, dreigingen met AI en verantwoord gedrag.

Stel je bedrijf in.

Voeg je medewerkers toe.

Wijs hun opleidingen toe.

Gratis voor bedrijven met maximaal 15 medewerkers.