

Informatiebeveiligingsbeleid TrusTool



TrusTool B.V. houdt zich bezig met het ontwerpen, ontwikkelen en onderhouden van een softwareapplicatie ten behoeve van vertrouwenspersonen.

TrusTool heeft een applicatie ontwikkeld om de werkwijze van de vertrouwenspersoon te professionaliseren. Ons platform kan worden ingezet om:

- a. de vertrouwenspersoon veilig en laagdrempelig te bereiken;
- b. een beschermde omgeving te bieden voor logboekbeheer door de vertrouwenspersoon, waarbij interne en/of externe vertrouwenspersonen kunnen samenwerken;
- c. eenvoudig data te genereren voor een management samenvatting van de bevindingen door de vertrouwenspersoon (inclusief tijdregistratie).

Onze klanten bestaan enerzijds uit organisaties die interne en/of externe vertrouwenspersonen hebben aangesteld en anderzijds uit externe vertrouwenspersonen die met de applicatie willen werken.

TrusTool is ontwikkeld vanuit de praktijk: van en voor de vertrouwenspersoon.

Met ontwikkeling vanuit de kennis en ervaring in de praktijk streven wij ernaar te voorzien in de behoeften van vertrouwenspersonen. Wij blijven continu ons product door ontwikkelen. Daarbij is uitgangspunt dat de applicatie veilig en eenvoudig in gebruik moet blijven.

Doelstellingen van ons Informatiebeveiligingsbeleid

- Beschermen van alle bedrijfsinformatie en informatie die door TrusTool wordt verwerkt tegen ongeautoriseerde toegang, verlies of schade.
- Voldoen aan relevante wet- en regelgeving, inclusief AVG
- Bevorderen van veilig gedrag en gebruik van IT-middelen door alle medewerkers

Extern openbaar – Versie 1.1

TrusTool B.V.

KvK 89206320

- Een kader voor continue verbetering van onze bedrijfsvoering

Toepassingsgebied

Dit beleid is van toepassing op:

- Alle medewerkers, inclusief tijdelijke krachten, stagiairs en externe partijen;
- Alle informatie en informatiesystemen van TrusTool, ongeacht locatie of drager (digitaal of fysiek).

Principes voor informatiebeveiliging

TrusTool hanteert de volgende kernprincipes:

- **Vertrouwelijkheid:** Informatie is alleen toegankelijk voor geautoriseerde personen.
- **Integriteit:** Informatie is juist, volledig en up-to-date.
- **Beschikbaarheid:** Informatie en systemen zijn beschikbaar wanneer nodig.
- **Naleving:** De organisatie handelt conform toepasselijke wet- en regelgeving, contractuele verplichtingen en normen.
- **Risicomangement:** Beveiligingsmaatregelen worden gekozen op basis van risico's en proportionaliteit.
- TrusTool heeft een beleid voor leveranciersbeoordeling. Leveranciers met toegang tot informatie of systemen worden beoordeeld op beveiliging.

Rollen en Verantwoordelijkheden

- **De Directie** is eindverantwoordelijk voor informatiebeveiliging, stelt het beleid vast en zorgt voor middelen, beheert, controleert en actualiseert het beleid. Zij evalueert periodiek resultaten en incidenten.
- **Het TrusTool medewerker team** handelt volgens beleid (o.a. gedragscode) en meldt incidenten. Eenieder dient actief bij te dragen aan een veilige informatiecultuur.

Toegangsbeveiliging

- Toegang tot informatie is geregeld via rollen en rechten. Toegang wordt verleend op basis van *need-to-know* en functie.
- Gebruik van sterke wachtwoorden en multifactor-authenticatie (MFA) is verplicht.
- Onbevoegd gebruik van informatiebronnen is verboden
- Accounts en toegangsrechten worden gedeactiveerd bij uitdiensttreding

Fysieke Beveiliging

- Toegang tot kantoorruimten is beperkt tot geautoriseerde personen.
- Apparatuur moet worden vergrendeld wanneer deze onbeheerd wordt achtergelaten.

Netwerk- en Systeembeveiliging

- Relevante systemen worden gemonitord op verdachte activiteiten.

Extern openbaar – Versie 1.1

TrusTool B.V.

KvK 89206320

TRUSTOOL

- Systeemupdates en beveiligingspatches zijn verplicht.
- Gebruik van goedgekeurde antivirus- en anti malwaresoftware.
- Back-ups worden periodiek gemaakt, getest en veilig opgeslagen.

Incidentmanagement

- Medewerkers melden beveiligingsincidenten direct bij de Directie of Security Officer
- Incidenten worden geregistreerd en geëvalueerd.
- Herstelmaatregelen worden zo snel mogelijk uitgevoerd.

Bewustwording en Training

- Verplichte security-awareness training voor alle medewerkers.
- Informatiebeveiliging regelmatig onderwerp bij werkoverleg en IB-overleg

Audit en Evaluatie

- Jaarlijkse risicoanalyse en evaluatie en zo nodig aanpassing van het informatiebeveiligingsbeleid
- Interne audits waar nodig en jaarlijks een onafhankelijke audit

Wijzigingen van het Beleid

Het beleid wordt jaarlijks geëvalueerd, maar kan eerder worden aangepast wanneer significante wijzigingen in processen, systemen of wetgeving dit vereisen.