Beleidsverklaring

iWize bouwt privacyvriendelijke software die het digitale leven makkelijker maakt. iWize levert veilige en privacyvriendelijke software die gebruikers in staat stelt persoonlijke gegevens op een eenvoudige manier te verzamelen, te beheren en te delen.

Goede informatiebeveiliging is hierbij randvoorwaardelijk. Niet alleen voor de eigen bedrijfsvoering, maar vooral voor gebruikers van de iWize software: consumenten en bedrijven. Zij moeten ervan uit kunnen gaan dat het verzamelen, beheren en delen van gegevens op een veilige manier gebeurt en dat eventuele risico's geminimaliseerd zijn.

Het doel van Informatiebeveiliging is het waarborgen van de bedrijfscontinuïteit en het minimaliseren van bedrijfsschade door het voorkomen en minimaliseren van de impact van beveiligingsincidenten. Met name moeten informatiemiddelen worden beschermd om een hoog niveau te halen op de volgende onderwerpen;

1. Beschikbaarheid waar en wanneer nodig voor het realiseren van de bedrijfsdoelstellingen
2. Integriteit, d.w.z. bescherming tegen ongeoorloofde of accidentele wijziging
3. Vertrouwelijkheid, d.w.z. bescherming tegen ongeoorloofde openbaarmaking.

Om alle gebruikers van de iWize software zekerheid te geven over de wijze waarop iWize de informatiebeveiliging geregeld heeft, voldoet iWize aan de ISO 27001 norm. Hiervoor gebruikt iWize een ISMS dat periodiek, minimaal jaarlijks, door een onafhankelijk certificeringsbureau beoordeeld wordt. Zo wordt jaarlijks bevestigd dat systemen, processen en organisatie van iWize voldoen aan de ISO 27001 norm. Het is daarmee voor de interne organisatie, alle gebruikers van de iWize software en voor externe auditors mogelijk om te beoordelen of en hoe iWize aan de ISO 27001 norm voldoet.

Verantwoordelijkheden:

1. De directie heeft dit Informatiebeveiligingsbeleid goedgekeurd;

2. De dagelijkse verantwoordelijkheid voor en de contacten met externe organisaties voor de naleving van de wettelijke eisen, met inbegrip van de bescherming van gegevens, berusten bij de Security Officer.

3. Alle werknemers of dienstverleners namens de organisatie hebben de plicht om de middelen, inclusief locaties, hardware, software, systemen of informatie, die zij onder hun hoede hebben, te beschermen en elke vermoede inbreuk op de beveiliging onmiddellijk te melden.

4. Het naleven van informatiebeveiligingsprocedures zoals uiteengezet in de beleids- en richtlijnstukken wordt geaccepteerd als onderdeel van de standaardwerkwijzen binnen de organisatie. Niet-naleving leidt tot disciplinaire maatregelen.

5. Aan alle wettelijke en reglementaire vereisten wordt voldaan en regelmatig op wijzigingen gecontroleerd.

6. Er is een bedrijfscontinuïteitsplan. Dit wordt onderhouden, getest en regelmatig herzien.

7. Dit informatiebeveiligingsbeleid wordt regelmatig herzien en kan door de directie worden gewijzigd om de blijvende levensvatbaarheid, toepasbaarheid en naleving van de wetgeving te waarborgen en om de informatiebeveiliging systemen voortdurend te verbeteren.

8. De directie stuurt erop aan dat er wordt voldaan aan de geldende wet- en regelgeving en dat middels het Informatiebeveiligingsmanagementsysteem continue verbetering wordt bewerkstelligd binnen de organisatie.

De scope conform het informatiebeveiligingsmanagementsysteem ISO 27001 is bepaald als:

“Informatiebeveiliging in relatie tot het ontwikkelen, beheren en onderhouden van software voor het verzamelen, delen en beheren van data’

Eindhoven, 19 januari 2024

J. de Bruijne

Algemeen Directeur