Beleidsverklaring

ISO27001/NEN7510

handsonict

Wijzigingen in dit document:

Auteur	Versie	Datum	Opmerkingen
William van de Rotten	1.0	`1-02-2022	Definitief

Over de organisatie
Met ICT-oplossingen die naadloos aansluiten op jouw ambities, zorgen wij ervoor dat jij kunt uitblinken in jouw business. Jouw doelstellingen en mensen staan bij ons altijd centraal. Want de beste ICT-oplossingen zijn die waardoor jouw mensen nóg efficiënter kunnen werken. En dat zie je terug in je resultaten.

Onze 125 specialisten staan dagelijks klaar om ervoor te zorgen dat de werkplekken van jouw mensen van alle gemakken voorzien zijn. Met 3 locaties in Nederland zijn we altijd dichtbij en snel op locatie. Als businesspartner begeleiden we jouw organisatie in de voortdurende digitale transitie.

Missie en Visie
Kwaliteit en informatiebeveiliging is voor Hands on ICT belangrijk. Zowel in de keuze voor de producten en diensten als voor de inrichting van onze organisatie. Hierbij kijken we ook naar industrie standaarden zoals Prince2 (voor projectuitvoering), ITIL (voor beheer), ISO27001 & NEN7510 (Informatiebeveiliging).

Het portfolio van Hands On ICT bestaat uit meerdere diensten waardoor we altijd de best mogelijke oplossing kunnen bieden. Door de juiste inzet van deze diensten en bovendien de kennis van onze medewerkers, zorgen we ervoor dat elke ICT-omgeving optimaal beschikbaar en veilig te gebruiken is. Deze diensten zijn onderverdeeld in:

- Workspace
- Security
- Cloud Ready
- Cloud densten
- Office 365
- Beheer

Informatiebeveiliging
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 ervoor te zorgen:

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

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 Privacy 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 informatiebeveiligingsmanager 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.