Specialist in productiever samenwerken met Microsoft 365

Wij willen meer halen uit jouw bedrijf, onszelf en de technologie die Microsoft ons biedt. Grenzen verleggen, meesterschap, toewijding en teamgeest zijn kernwaarden bij CTB.

Scope

Informatiebeveiliging gerelateerd aan het ontwerpen, ontwikkelen en ondersteunen van software voor het automatiseren van governance en werkprocessen in Microsoft 365.

Visie

Microsoft 365, Teams voorop, biedt organisaties grote voordelen. Er kan veel tijd bespaard worden door efficiëntere communicatie en door niet meer te hoeven zoeken naar de juiste informatie. Maar ook hebben organisaties die Teams goed gebruiken meer grip op het werk; de centrale en open samenwerking zorgt voor minder fouten, miscommunicatie en vertraging. Zo wordt er beter werk geleverd aan klanten.

Echter om de vele functies van M365 goed in gebruik te nemen, compliance op orde te hebben en adoptie te maximaliseren is er software nodig voor het automatiseren van governance en de werkprocessen.

Missie

Wij helpen organisaties bij het op orde brengen van hun Microsoft Teams governance én bij de ondersteuning van werkprocessen in Teams. Dit doen wij door middel van de automatiseringsfuncties van onze cloudoplossing P365.

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 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 Security Officer worden gewijzigd om de blijvende levensvatbaarheid, toepasbaarheid en naleving van de wetgeving te waarborgen en om de informatiebeveiligingssystemen 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.

Ede, 28 juli 2026

Yuri Ramdhani
CEO