Over ons

Hermac ontzorgt u op het gebied van ICT: Wij bieden transparante, betaalbare automatiseringsdiensten voor de zakelijke markt. Deskundig, betrouwbaar, flexibel en innovatief. Deze ondernemingskenmerken verwoorden de essentie van onze werkwijze en vormen ons bestaansrecht binnen de uiterst dynamische ICT branche.

Missie & Visie

De missie: Hermac biedt transparante, betaalbare automatiseringsdiensten voor de zakelijke markt. Deze diensten dienen naadloos aan te sluiten bij de behoefte van elke individuele en unieke organisatie en aantoonbaar meerwaarde te bieden. Deskundig, betrouwbaar, flexibel en innovatief. Deze ondernemingskenmerken verwoorden de essentie van de Hermac werkwijze en vormen daarmee het bestaansrecht binnen de uiterst dynamische ICT branche.

De visie: Professioneel maar ongedwongen, collegiaal, integer en betrouwbaar werken. De tevreden relatie als middelpunt van al onze activiteiten. Steeds net dat stapje extra zetten, zowel voor elkaar als ook voor onze partners.

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 dienen informatiemiddelen te worden beschermd om te zorgen voor:

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 Information Security Manager.

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.

Plaats, datum: Scherpenzeel, 19-10-2026

Naam: Mike Niekerk - Directeur

Handtekening: Mike Niekerk

Dit publieke document is vanuit cybersecurity oogpunt niet voorzien van een originele handtekening.

Het originele document is getekend op **19-10-2026** en op verzoek toonbaar.