DOC-101 Beleidsverklaring Informatieveiligheid

Versie:	*1.0*
Datum:	22-07-2025
Status:	Definitief
Eigenaar:	Directie
Classificatie:	Publiek
Goedgekeurd door:	Directie

Wij begrijpen als geen ander dat de mentale gezondheid van medewerkers cruciaal is voor een bedrijf. Alleen als je 100% kunt bouwen op je medewerkers kun je als bedrijf elke uitdaging aan. Bij Fast Lane Vitality bieden we een uitgebreide aanpak om mentale klachten vroegtijdig te signaleren d.m.v. preventieve trainingen en effectieve individuele behandelingen.

Om onze clienten goed te ondersteunen is het van belang dat wij veilig en secuur om gaan met de data die wij verwerken. Dit waarborgen wij met een management systeem voor informatieveiligheid. Wij zien het als onze plicht om de privacy gevoelige gegevens en persoonlijke gezondheidsinformatie te beschermen.

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 de volgende aspecten te waarborgen:

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:

Naam: B.M.L. Caris