DE FORENSISCHE ZORGSPECIALISTEN

Willem Dreeslaan 2
3515 GB Utrecht
Postbus 174
3500 AD Utrecht

Tel. 030-275 82 75
info@dfzs.nl
www.dfzs.nl

Samenvatting Informatiebeveiliging

Openbaar | Documentversie 6 | Laatst bijgewerkt 22-10-2026

De Forensische Zorgspecialisten werkt dagelijks met persoonlijke, medische en bedrijfsgevoelige informatie. Een zorgvuldige omgang met deze informatie is essentieel voor de privacy en veiligheid van onze patiënten, cliënten en medewerkers, maar ook voor de kwaliteit en continuïteit van onze dienstverlening.

Informatiebeveiliging gaat voor ons niet alleen over digitale dreigingen. Het gaat ook over het voorkomen van fouten, verlies van informatie, onbevoegde toegang en uitval van systemen of diensten. Daarom beschermen wij informatie tegen risico's die de beschikbaarheid, juistheid en vertrouwelijkheid ervan kunnen aantasten.

Onze uitgangspunten

Bij de inrichting van informatiebeveiliging hanteren wij de volgende uitgangspunten:

- Informatie is beschikbaar wanneer deze nodig is voor onze zorgverlening en bedrijfsvoering.
- Informatie is betrouwbaar, juist en actueel.
- Vertrouwelijke informatie is alleen toegankelijk voor personen die deze voor hun werkzaamheden nodig hebben.
- Persoonsgegevens en medische gegevens worden zorgvuldig en rechtmatig verwerkt.
- Informatiebeveiliging maakt onderdeel uit van beleid, besluitvorming, projecten en veranderingen binnen de organisatie.
- Risico's worden tijdig herkend, beoordeeld en waar nodig teruggebracht tot een aanvaardbaar niveau.
- Incidenten en verbeterpunten worden onderzocht en gebruikt om onze werkwijze verder te verbeteren.

Deze uitgangspunten worden risicogestuurd en praktisch toegepast. Daarbij zoeken we steeds naar een passende balans tussen veiligheid, kwaliteit van zorg en werkbaarheid.

Verantwoordelijkheid en bewustwording

Informatiebeveiliging is een gezamenlijke verantwoordelijkheid. De Raad van Bestuur, directie en het management geven richting aan het beleid en zorgen voor de benodigde mensen en middelen. Medewerkers worden geïnformeerd over hun verantwoordelijkheden en krijgen training om veilig met informatie en systemen om te gaan.

Van medewerkers wordt verwacht dat zij zorgvuldig omgaan met informatie, alleen toegang gebruiken die nodig is voor hun werkzaamheden en mogelijke incidenten of onveilige situaties melden. Ook leveranciers en andere samenwerkingspartners moeten voldoen aan passende eisen op het gebied van informatiebeveiliging en privacy.

Risicobeheersing

Wij brengen risico's voor informatie, systemen en dienstverlening periodiek in beeld. Bij nieuwe of gewijzigde processen, systemen, samenwerkingen en leveranciers wordt beoordeeld welke beveiligings- en privacyrisico's kunnen ontstaan.

Op basis van deze risico's nemen wij passende organisatorische, fysieke en technische maatregelen. Kritische leveranciers worden periodiek beoordeeld en bij de selectie van leveranciers die toegang hebben tot medische informatie worden aantoonbare eisen gesteld aan privacy en informatiebeveiliging.

Privacy

Informatiebeveiliging en privacy zijn nauw met elkaar verbonden. Persoonsgegevens worden alleen verwerkt wanneer daarvoor een geldige grondslag bestaat en alleen voor het doel waarvoor ze zijn verzameld. We verzamelen niet meer gegevens dan noodzakelijk en bewaren deze niet langer dan nodig.

Bij de inrichting van nieuwe processen en systemen houden we vanaf het begin rekening met gegevensbescherming. Voor persoonsgegevens en medische informatie treffen we aanvullende maatregelen wanneer de gevoeligheid of risico's daartoe aanleiding geven.

Incidenten en verbetering

Ondanks alle voorzorgsmaatregelen kan zich een beveiligingsincident of datalek voordoen. Medewerkers worden gestimuleerd om verdachte situaties, incidenten en mogelijke verbeterpunten zo snel mogelijk te melden. Meldingen worden beoordeeld en opgevolgd. Waar nodig nemen we maatregelen om schade te beperken en herhaling te voorkomen.

Informatiebeveiliging is een continu proces. Ons beleid, onze risico's en de werking van maatregelen worden periodiek beoordeeld. Daarbij maken we gebruik van interne controles, onafhankelijke audits, evaluaties en managementbeoordelingen. Het beleid wordt minimaal jaarlijks herzien en eerder wanneer ontwikkelingen of ernstige incidenten daar aanleiding toe geven.

Normen en wetgeving

De Forensische Zorgspecialisten richt informatiebeveiliging en kwaliteitsmanagement in als een samenhangend managementsysteem. Daarbij houden wij rekening met toepasselijke wet- en regelgeving, contractuele verplichtingen en relevante normen voor de zorgsector, waaronder NEN 7510. Het managementsysteem wordt onafhankelijk getoetst aan ISO 9001 en NEN 7510.