Informatiebeveiligings-beleid

De ZorgSpecialist
Thuis in alle zorg

Jens Jansma – 12-07-2022 – versie 1.1

Documenthistorie

Versie	Datum	Auteur(s)	Opmerkingen
1.0	25-08-2021	J. Jansma	Vastgesteld in ST van 20-09-2021
1.1	12-07-2022	J. Jansma	Update relevante gerelateerde stukken

Inhoud

1. Inleiding

De ZorgSpecialist staat voor goede en persoonlijke zorgverlening met deskundig en betrokken personeel. Met een toenemende afhankelijkheid van informatie en technologie, is het van belang dat er zorgvuldig met deze informatie omgegaan wordt. In dit informatiebeveiligingsbeleid wordt beschreven hoe De ZorgSpecialist maatregelen neemt tegen kwetsbaarheden en risico's die gepaard gaan met deze toenemende afhankelijkheid.

De ZorgSpecialist heeft de ambitie om met behulp van dit beleid de informatiebeveiliging continu te blijven verbeteren.

1.1 Geldigheid

Het informatiebeveiligingsbeleid is van toepassing op alle medewerkers binnen De ZorgSpecialist en alle externen die op enige wijze toegang krijgen tot informatiesystemen die in gebruik zijn binnen De ZorgSpecialist. Daarnaast geldt het beleid voor alle devices waarmee geautoriseerde toegang tot deze systemen verkregen kan worden.

2. Doelen

Het informatiebeveiligingsbeleid heeft als primaire doel om de continuïteit van zorg en bedrijfsvoering te waarborgen, beveiligingsincidenten zo veel als mogelijk te voorkomen en potentiële schade ten gevolge van incidenten zo veel mogelijk te beperken.

2.1 Uitgangspunten

We hebben verschillende uitgangspunten gedefinieerd die Er zijn enkele uitgangspunten gedefinieerd, die de realisatie van het primaire doel.

2.1.1 Informatiebeveiliging als proces

Om de informatiebeveiliging continu te blijven verbeteren, wordt deze als proces ingericht conform de PDCA-cyclus. Ook het informatiebeveiligingsbeleid wordt jaarlijks herzien.

2.1.2 Risico en praktijk gebaseerde maatregelen

De ZorgSpecialist neemt maatregelen op basis van een risicoanalyse voor informatiebeveiliging. Hierin wordt duidelijk welke risicowaarde bij verschillende kritieke processen en middelen hoort. Het gaat hier om alle mogelijke bedreigingen, zoals: gebrek aan bewustwording, foutief gebruik van applicaties, cybercriminaliteit, brand, wateroverlast, stroomstoringen, etc.

De risicowaarde is afhankelijk van de waarschijnlijkheid en de impact. Op basis van de risicowaarde wordt bepaald welke maatregelen prioriteit krijgen. Deze risicoanalyse wordt minimaal eens per jaar uitgevoerd.

Daarnaast is er aandacht voor informatiebeveiliging in de praktijk. Ontwikkelingen en best practices vanuit de zorgsector kunnen worden gebruikt om snel en effectief te werk te gaan.

2.1.3 Beschikbaarheid, integriteit en vertrouwelijkheid

Beveiligingsmaatregelen worden genomen om de drie belangrijkste eigenschappen van goede informatievoorziening te waarborgen:

- Beschikbaarheid: informatie moet beschikbaar en toegankelijk zijn voor eindgebruikers.
- Integriteit: informatie moet overeenkomen met de werkelijkheid. De informatie is juist, volledig en actueel.
- Vertrouwelijkheid: informatie moet enkel toegankelijk zijn voor bevoegden.

2.1.4 Normen en wetten

De ZorgSpecialist streeft ernaar aantoonbaar te voldoen aan de NEN 7510. Deze norm is speciaal ontwikkeld voor de informatiebeveiliging in de zorgsector in Nederland. Daarnaast streeft De ZorgSpecialist ernaar te voldoen aan de relevante wetgeving.

2.1.5 Maatregelen en beleid

Getroffen maatregelen worden vastgelegd en verwijzen naar relevant beleid, richtlijnen en procedures. Deze worden geactualiseerd wanneer nodig. Procedures en richtlijnen worden op passende wijze binnen de organisatie ingevoerd en gecommuniceerd met aandacht voor de doelgroep.

2.1.6 Gebruiksvriendelijkheid

Bij het invoeren van maatregelen ten behoeve van informatiebeveiliging wordt rekening gehouden met de gebruiksvriendelijkheid van informatiesystemen.

3. Rollen en verantwoordelijkheden

- De directie is eindverantwoordelijk voor informatiebeveiliging binnen De ZorgSpecialist en stelt het beleid en de maatregelen vast.
- Het beleid wordt samengesteld in samenwerking met de privacyfunctionarissen. Zij zien toe op de naleving ervan.

- De ICT-afdeling is verantwoordelijk voor controle van de status van de beveiliging van applicaties en volgt functionele ontwikkelingen die de beveiliging kunnen verbeteren.
- Er wordt naar gestreefd om iedereen binnen de organisatie deelgenoot te maken van de verantwoordelijkheid. Iedereen is verantwoordelijk voor het naleven van het beleid. Leidinggevenden en coördinatoren hebben een belangrijke rol in naleving van het beleid door hun teamleden.

4. Naleving en bewustwording

Beleid en maatregelen alleen kunnen nooit voor een geschikte informatiebeveiliging zorgen. In de praktijk blijkt dat menselijke fouten vaak het grootste risico vormen. Daarom wordt voldoende aandacht besteed aan bewustwording. Het betreft zowel aandacht specifiek voor nieuwe medewerkers, als terugkerende aandacht voor bestaand personeel.

Opzettelijke overtreding en misbruik wordt gemeld bij de HR-afdeling en de leidinggevende. Overtreding van het informatiebeveiligingsbeleid en ondersteunende richtlijnen kan leiden tot arbeidsrechtelijke gevolgen.

5. Gerelateerde stukken

Hieronder staat een overzicht van enkele relevante beleidsstukken en documenten, gerelateerd aan het informatiebeveiligingsbeleid.

- Gedragscode verantwoord ICT-gebruik
  De gedragscode geeft aan hoe binnen De ZorgSpecialist met ICT dient te worden omgegaan.
- Risicoanalyse
  De risicoanalyse, zoals bedoeld in hoofdstuk 2.1.1
- ICT- beleid
  Omschrijft de wijze waarop ICT binnen De ZorgSpecialist wordt georganiseerd.
- Jaarplan ICT
  Beschrijft de geplande activiteiten voor de afdeling ICT, waaronder informatiebeveiliging.