8 april 2024

InfinitCare

Informatie beveiligingsbeleid 2024

Inhoud

Inleiding

InfinitCare ondersteunt GGZ zorgaanbieders en financiers (zorgverzekeraars, KiBG en gemeenten / regio's) om te gaan met de vele uitdagingen in een snel veranderende omgeving. In een sector die meer en meer met marktwerking te maken heeft is het van groot belang dat zorgaanbieders de kwaliteit van hun behandelingen aantonen en deze op een goede manier verbeteren (effectiever en efficiënter).

Met onze kennis, ervaring en applicatie SAM Zorgmonitor helpen we zorgaanbieders inzicht te krijgen in de effectiviteit en efficiëntie van hun behandelingen (zorgpaden).

Naast de interne kwaliteitsdoelstellingen zijn zorgaanbieders ook steeds vaker verplicht om zich ook te verantwoorden over de geleverde kwaliteit richting hun zorgfinanciers. M.b.v. ons Gemeenteportaal verzorgen we aan beide partijen een platform, waar het mogelijk is om de geleverde kwaliteit van dienstverlening met elkaar af te stemmen.

Om bovenstaande te bewerkstelligen heeft InfinitCare gevoelige zorg informatie nodig. De zorgaanbieders en hun patiënten stellen dan ook hoge eisen aan de beschikbaarheid, juistheid en vertrouwelijkheid van de informatieverwerking. Zeker in het kader van de nieuwe wet AVG is de focus op informatiebeveiliging en goed omgaan met privacy aspecten nog meer toegenomen.

Het inrichten van een ISMS voor InfinitCare zorgt er tevens voor dat de beleidsuitgangspunten van InfinitCare voor alle medewerkers duidelijk beschreven zijn. Alle aspecten betreffende informatiebeveiliging en privacy zijn beschreven en dienen voor de medewerkers als uitgangspunt hoe hun activiteiten uit te voeren. Daarnaast zorgt een goede beschrijving er tevens voor dat processen efficiënter worden uitgevoerd.

Bovenstaande zijn de redenen dat de directie van InfinitCare zich ten doel gesteld haar dienstverlening conform ISO-27001: 2017 en de NEN-7510:2017 in te richten en zich te certificeren, zodat aan die behoefte van klanten wordt voldaan. Ook de interne bedrijfsprocessen van InfinitCare worden getoetst op de norm van ISO-27001: 2017 en de NEN-7510:2017.

Verantwoordelijkheid en doelstelling

Gelet op de mogelijke impact van verstoringen op de bedrijfsvoering en continuïteit van InfinitCare en haar klanten berust eindverantwoordelijkheid voor het beleid inzake informatiebeveiliging bij de directie van InfinitCare.

Dit beleidsdocument Informatiebeveiliging (hierna te noemen beleid IB) maakt deel uit van het algehele beveiligingsbeleid van InfinitCare. De doelstelling van het beleid IB inzake de vertrouwelijkheid, integriteit en continuïteit van de geautomatiseerde informatievoorziening van de InfinitCare luidt:

'Het bieden van een raamwerk van beleidsuitgangspunten met betrekking tot de vertrouwelijkheid, integriteit en beschikbaarheid van de informatievoorziening, waarbinnen een evenwichtig (doeltreffend en doelmatig) stelsel van onderling samenhangende maatregelen ontwikkeld wordt, teneinde de informatievoorziening te beschermen tegen interne en externe bedreigingen'.

Alle leidinggevenden dienen ervoor zorg te dragen, dat aan de in dit beleid IB geformuleerde beleidsuitgangspunten wordt voldaan bij de inrichting van de organisatie, procedures, werkwijze en de daarbij gehanteerde informatiesystemen.

Dit 'grote' doel is verder uitgewerkt in de volgende specifieke doelstellingen:

1. Gecertificeerd blijven voor ISO 27001 en NEN 7510.
2. Penetratietesten op alle omgevingen van InfinitCare uitgevoerd met als resultaat geen issues met prioriteit "Blocker" of "Critical".
3. Voldoen aan alle wet en regelgeving en alle contractuele eisen.
4. Aantal informatiebeveiligingsissue met prioriteit "Critical" of hoger, maximaal 1 per 2 maanden.
5. Voor SAM Zorgmonitor geldt een minimale 99,5 % uptime tijdens werkdagen.
6. Voor alle partijen die onderdeel zijn van het leveringsproces van InfinitCare geldt dat zij minimaal ISO 27001 gecertificeerd zijn of aantoonbaar voldoen (door een onafhankelijke partij vastgesteld) aan een gelijkwaardig informatiebeveiligingssysteem en dat zij minimaal eens per jaar aangeven in welke mate voldaan wordt aan de verwerkersovereenkomst en de SLA.
7. Alle medewerkers en leveranciers van InfinitCare voldoen aan de gedefinieerde ethische code

Toepassingsgebied

Dit beleid is van toepassing op alle informatie die gecreëerd, ontvangen, verzonden of bewaard wordt in de dienstverlening van InfinitCare aan klanten en de daarmee samenhangende contractuele verplichtingen. Het beleid en de uitwerking hiervan gelden voor alle medewerkers van InfinitCare. Daarnaast dient het beleid ook uitgevoerd te worden door tijdelijk personeel en leveranciers die InfinitCare ondersteunen bij haar dienstverlening aan klanten.

Uitwerking van dit beleid

Op basis van dit beleid worden risico analyses uitgevoerd en wordt een set van maatregelen en controles gedefinieerd als basisbeveiligingsniveau (BBN), dat geldt als minimum voor de dienstverlening aan klanten. Er is beleid gedefinieerd voor de volgende aspecten:

- Mobiele apparatuur - A.6.2.1
- (Logische) toegangsbeveiliging - A.9.1.1

- Cryptografie - A.10.1.1
- Clear desk / clear screen - A.11.2.9
- Backup en restore- A.12.3.1
- Informatietransport - A.13.2.1
- Beveiligd ontwikkelen - A.14.2.1
- Leveranciers - A.15.1.1

Hiermee wordt de continuïteit van de informatie en de informatievoorziening gewaarborgd en de eventuele gevolgen van beveiligingsincidenten tot een acceptabel, vooraf bepaald niveau beperkt.

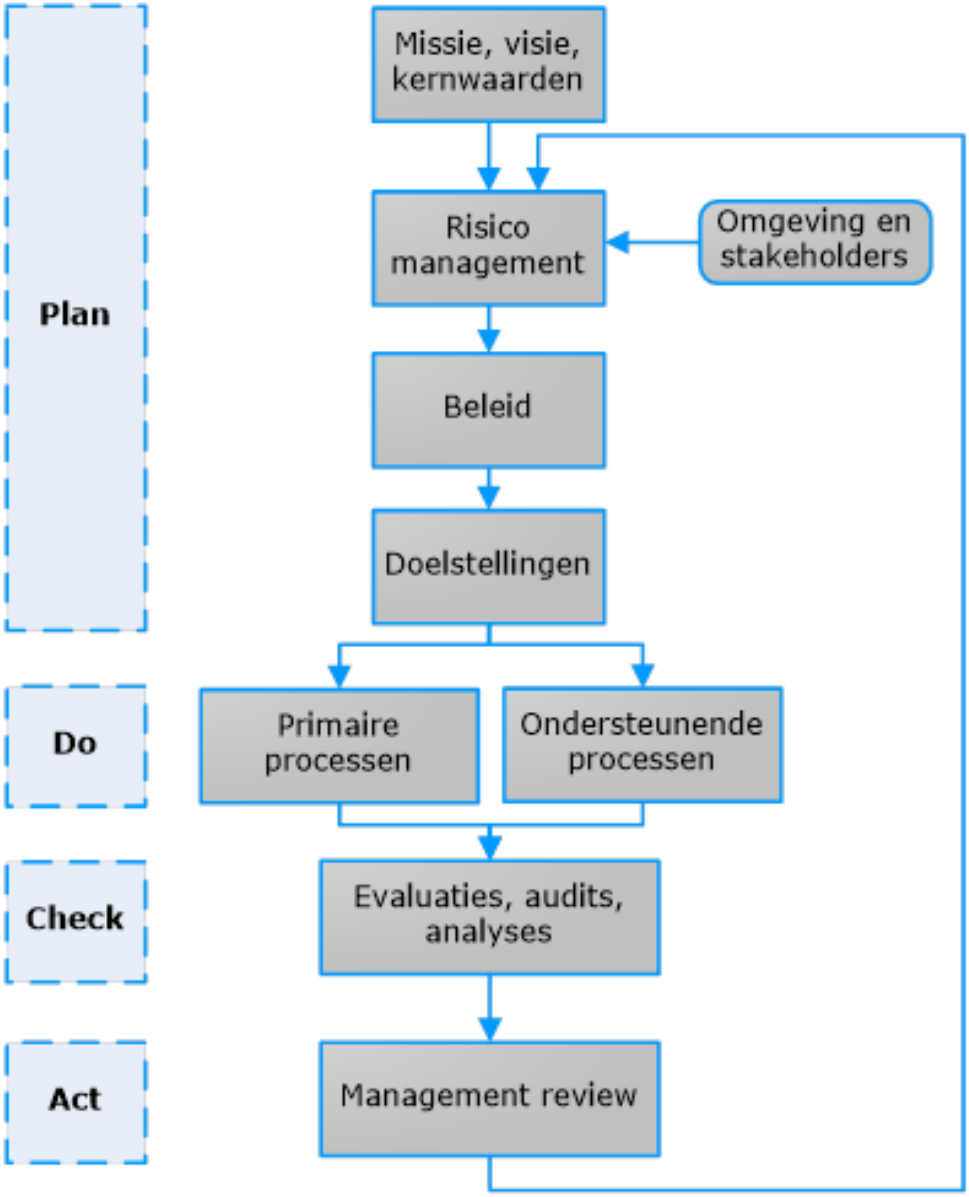
Onder de bescherming van informatie verstaan we het geheel van preventieve-, repressieve- en herstelmaatregelen, alsmede procedures welke de beschikbaarheid, integriteit en vertrouwelijkheid van alle vormen van informatie garanderen.

Om dit te realiseren stelt de directie middelen ter beschikking in de vorm van geld, tijd en voorzieningen voor onder andere interne opleidingen, penetratietesten, externe en interne ondersteuning.

Controle werking en naleving van het beleid

Ons managementsysteem (ISMS) is erop gericht zelf continu te verbeteren aan de hand van een Plan–Do–Check–Act-cyclus. Hierin wordt de gehele organisatie betrokken. In onderstaand overzicht staat procesmatig weergegeven op welke wijze aan deze PDCA-cyclus wordt vormgegeven.

Halfjaarlijks wordt de werking en de naleving van het beleid intern geëvalueerd en hierover wordt gerapporteerd aan de directie. Onderdeel van deze evaluatie zijn het opnieuw beoordelen van risico's en een impact analyse van nieuwe wet- en regelgeving. Onderdeel van deze rapportage is ook een plan met verbetervoorstellen. De directie beoordeelt de rapportage, keurt voorstellen al dan niet goed en kent budget toe voor de realisatie van de voorstellen. Onderstaand is dit schematisch weergegeven.



Namens de directie van InfinitCare

Han Laarhuis

Johan Kerssies