Beleid Informatiebeveiliging InfinitCare

Wijzigingshistorie

Versie	Wie	Wanneer	Wat
2021-V001	Han Laarhuis	2021-02-05	Tekstuele aanpassingen
2020-V001	Han Laarhuis	2020-03-04	Aanpassen aan nieuwe ISMS 2020

InfinitCare B.V.
Koningin Wilhelminalaan 8
3527 LD Utrecht

kvk 51152266
030-2040219
www.InfinitCare.com

Inleiding

InfinitCare ondersteunt GGZ zorgaanbieders 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: 2015 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: 2015 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:

InfinitCare B.V.
Koningin Wilhelminalaan 8
3527 LD Utrecht

kvk 51152266
030-2040219
www.InfinitCare.com

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. 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

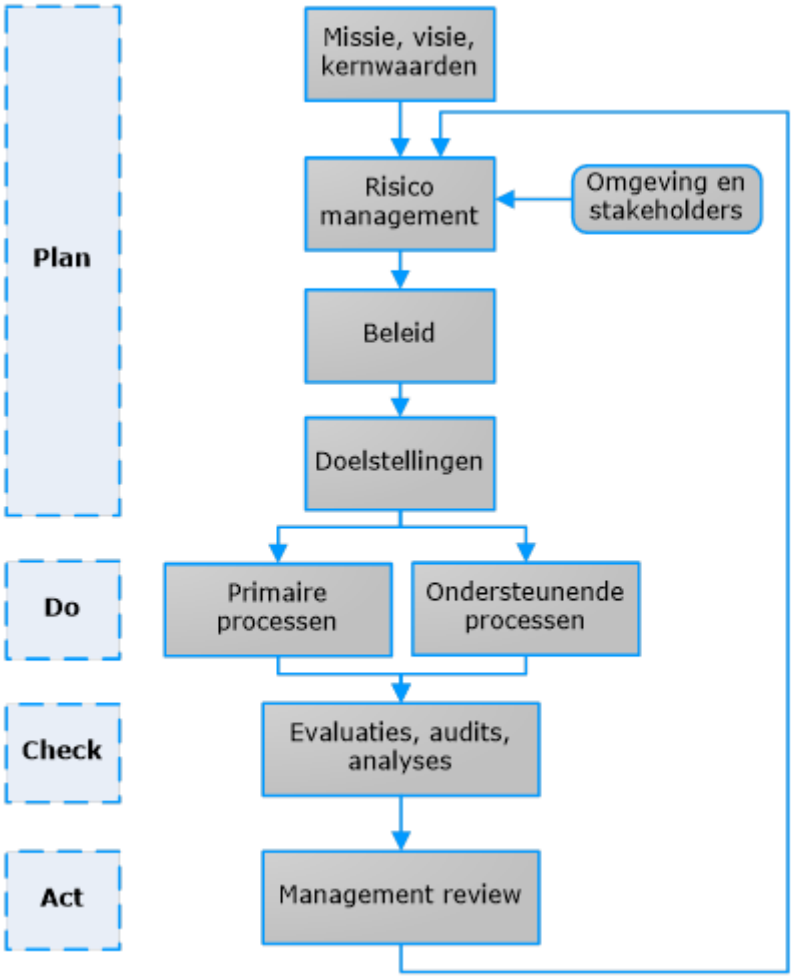
Ons managementsysteem (ISMS) is erop gericht zelf continu te verbeteren aan de hand van een Plan–Do–Check–Act-cyclus. Hierin wordt de gehele organisatie betrokken. In onderstaand overzicht staat procesmatig weergegeven op welke wijze aan deze PDCA-cyclus wordt vormgegeven.

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.

InfinitCare B.V.
Koningin Wilhelminalaan 8
3527 LD Utrecht

kvk 51152266
030-2040219
www.InfinitCare.com

Onderstaand is dit schematisch weergegeven.



InfinitCare B.V.
Koningin Wilhelminalaan 8
3527 LD Utrecht

kvk 51152266
030-2040219
www.InfinitCare.com

Beleidsuitgangspunten

Bij de verdere invulling van het beleid dienen de volgende door de directie vastgestelde uitgangspunten gehanteerd te worden. Tevens wordt bij deze beleidsuitgangspunten ook aangegeven op welke informatiebeveiligingsdoelstellingen ze betrekking hebben.

1	**Gecertificeerd blijven voor ISO 27001 en NEN 7510**
Nr	**Omschrijving**
1	Informatiebeveiliging is een belangrijk **bedrijfsrisico** voor InfinitCare. De directie stelt daarom het beleid vast, beoordeelt de risico's, stelt de maatregelen vast en laat periodiek de werking van het beleid en de naleving van deze maatregelen intern en extern beoordelen.
12	**Gegevensverstrekking** extern gebeurt op basis van 'need to know'. Intern is dit niet altijd wenselijk omdat kennisdeling essentieel is voor een kosteneffectieve dienstverlening aan klanten.
15	**Datatransport** is zodanig met beveiligingsmaatregelen omkleed, dat geen inbreuk kan worden gepleegd op de vertrouwelijkheid en de integriteit van deze gegevens.
16	Geautoriseerde medewerkers moeten ook **op afstand** een beveiligde toegang hebben tot de voor hun relevante productie omgevingen. Er worden geen vertrouwelijke gegevens buiten de productieomgeving opgeslagen. Onder condities kan hiervan afgeweken worden.
17	**Productie** omgevingen zijn gescheiden van andere omgevingen en hierin kunnen specifiek toegangsrechten worden verleend en is monitoring van de toegang mogelijk.
21	Er zijn calamiteitenplannen en -voorzieningen om de **continuïteit** van de informatievoorziening te waarborgen.
22	Genoemde beleidsuitgangspunten gelden voor die gegevensbewerkingen, waarvoor InfinitCare wettelijk en/of contractueel verantwoordelijk is.
23	Alle informatie die binnen InfinitCare gebruikt wordt, wordt **geclassificeerd** als vertrouwelijk.

2	**Penetratietesten op alle omgevingen van InfinitCare uitgevoerd met als resultaat geen issues met prioriteit "Blocker" of "Critical"**
Nr	**Omschrijving**
4	InfinitCare beschouwt **computercriminaliteit** als een ongewenst maatschappelijk probleem en ziet het slechts als haar taak om passende maatregelen te nemen om schade ten gevolge van criminele activiteiten zoveel mogelijk te beperken.
11	**Toegangsbeveiliging** zorgt ervoor, dat ongeautoriseerde personen of processen geen toegang krijgen tot de informatiesystemen, gegevensbestanden en programmatuur van InfinitCare.

InfinitCare B.V.
Koningin Wilhelminalaan 8
3527 LD Utrecht

kvk 51152266
030-2040219
www.InfinitCare.com

3	Voldoen aan alle wet en regelgeving en alle contractuele eisen
Nr	**Omschrijving**
2	InfinitCare conformeert zich m.b.t. de informatiebeveiliging aan de van toepassing zijnde **wetgeving en eisen**.
3	De doelstellingen en beheersmaatregelen van de norm **NEN-ISO/IEC 27001** en de privacy richtsnoeren van het **AP** vormen, voor zover zij bijdragen aan de informatiebeveiliging van InfinitCare en passen op de activiteiten die InfinitCare voor klanten uitvoert, het uitgangspunt voor de te definiëren maatregelen.
10	Bij de verwerking en het gebruik van gegevens worden maatregelen getroffen om de **privacy** van klanten, medewerkers en andere betrokkenen te waarborgen.
14	Input van klanten die vertrouwelijke data bevat, wordt na verwerking op korte termijn **gearchiveerd** of vernietigd.

4	Aantal informatiebeveiligingsissue met prioriteit "Critical" of hoger, maximaal 1 per 2 maanden
Nr	**Omschrijving**
20	Er is een proces om **incidenten** adequaat af te handelen en hier 'lessons learned' uit te trekken.

5	Voor SAM Zorgmonitor geldt een minimale 99,5 % uptime tijdens werkdagen
Nr	**Omschrijving**
18	Het **beheer** en de opslag van gegevens in productie omgevingen zijn zodanig, dat geen informatie verloren kan gaan tenzij er sprake is van overmacht.

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
Nr	**Omschrijving**
7	De fysieke en logistieke beveiliging van de **gebouwen** en de ruimtes daarin zijn zodanig, dat de vertrouwelijkheid, integriteit en beschikbaarheid van de gegevens en gegevensverwerking gewaarborgd zijn.
8	Aanschaf, installatie en onderhoud van **informatie- en communicatiesystemen**, alsmede inpassing van nieuwe technologieën, moeten zo nodig met aanvullende maatregelen worden uitgevoerd, dat hiermee geen afbreuk wordt gedaan aan de informatiebeveiliging.

InfinitCare B.V.
Koningin Wilhelminalaan 8
3527 LD Utrecht

kvk 51152266
030-2040219
www.InfinitCare.com

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**
9	Opdrachten aan **derden** voor het uitvoeren van werkzaamheden worden zodanig omgeven met maatregelen, dat er geen inbreuk op de vertrouwelijkheid, integriteit en continuïteit van de informatievoorziening kan ontstaan.
13	InfinitCare en haar medewerkers treffen maatregelen om te **voorkomen**, dat **vertrouwelijke informatie** in handen van derden terechtkomt.
18	Het **beheer** en de opslag van gegevens in productie omgevingen zijn zodanig, dat geen informatie verloren kan gaan tenzij er sprake is van overmacht.
19	Er zijn **functiescheidingen** aangebracht tussen de ontwikkel-, beheer- en gebruikersorganisatie. Voorts wordt functiescheiding toegepast waar dat mogelijk en wenselijk is.
26	Alle leveranciers, die cruciaal zijn voor het leveringsproces van InfinitCare dienen ISO 27001 gecertificeerd te zijn.

7	**Alle medewerkers en leveranciers van InfinitCare voldoen aan de gedefinieerde ethische code**
Nr	**Omschrijving**
5	**Vertrouwen** is voor InfinitCare een groot goed en zij hanteert naar medewerkers, klanten, leveranciers en andere stakeholders het wederkerigheidsprincipe. InfinitCare gaat er vanuit, dat zij afspraken nakomen m.b.t. integriteit, vertrouwelijkheid en continuïteit van de informatievoorziening.
6	Het **HRM-beleid** is mede gericht op het verbeteren van de integriteit, vertrouwelijkheid en continuïteit van de informatievoorziening bij medewerkers.
24	Door alle medewerkers is een **geheimhoudingsverklaring** ondertekend.
25	Door alle leveranciers is een **geheimhoudingsverklaring** ondertekend.

InfinitCare B.V.
Koningin Wilhelminalaan 8
3527 LD Utrecht

kvk 51152266
030-2040219
www.InfinitCare.com