OZOverbindzorg
Wispelweg 2b
8105 AB Luttenberg

06 117 695 20
info@ozoverbindzorg.nl
www.ozoverbindzorg.nl

KvK: 56833849
Bank: NL 47RABO 01780.53.864
BTW: NL 852323372.B01

Beleid Informatiebeveiliging OZOverbindzorg

1 Inleiding

OZOverbindzorg heeft tot doel het (doen) verzekeren dat de complexe zorgvraag voor zorgbehoeftigen, waaronder, maar niet uitsluitend, kwetsbare ouderen, jongeren en gehandicapten, optimaal wordt verricht middels het daartoe door OZOverbindzorg op te richten en te onderhouden Virtuele Verzorgingshuis OZOverbindzorg, waarbij de cliënt centraal dient te staan, de regie kan voeren over zijn/haar eigen zorg, alsmede het verrichten van alle verdere handelingen, die met het vorenstaande in de ruimste zijn verband houden of daartoe bevorderlijk kunnen zijn. Daarbij stelt de stichting zich met name ten doel het bijdragen aan de welzijnsverbetering van kwetsbare mensen met chronische ziekten en het nastreven van alle daartoe behorende maatschappelijke doelen.

E-Health ontwikkelingen zullen elkaar in de komende jaren snel opvolgen. In dit “woud” van nieuwe mogelijkheden wil de Stichting een organiserende en coördinerende rol spelen binnen het sociaal medisch netwerk. Dit teneinde een infrastructuur te bieden, die (waar mogelijk) deze E-Health toepassingen voor de cliënt en alle zorgverleners laat aansluiten en/of integreren. Hierbij is het maatschappelijk doel “Meer voor Minder” leidend. Centraal daarbij: betere zorg en begeleiding met minder kosten en ten dienste van de cliënt.

De basis van de dienstverlening is een samenwerkingsplatform met als gebruikers cliënten, mantelzorgers, huisartsen, zorgverleners, gemeenten, verzekeraars en ziekenhuizen, gericht op afstemming en communicatie rond zorg en begeleiding van kwetsbaren in de thuissituatie, waarbij de cliënt centraal staat!

Om alle partijen (en financiers) het vertrouwen te geven, dat de data goed beveiligd zijn en dat OZOverbindzorg in control is, heeft de directie besloten dit aantoonbaar te maken middels het halen van zowel een ISO 27001 als een NEN 7510 certificaat.

2 Verantwoordelijkheid, doelstelling en doelgroep

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

Het Beleidsdocument Informatiebeveiliging (hierna te noemen beleid IB) heeft als doel de risico’s m.b.t. de vertrouwelijkheid, integriteit en continuïteit van de informatievoorziening binnen OZOverbindzorg te beheersen en definiëren we als volgt:
‘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 betrokkenen 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.

Intern wordt het beleid IB gecommuniceerd aan de Raad van Commissarissen, het managementteam en medewerkers via reguliere overleggen. Extern wordt het beleid gecommuniceerd via de website.

3 Toepassingsgebied

Dit beleid is van toepassing op alle informatie die gecreëerd, ontvangen, verzonden of bewaard wordt in de dienstverlening van OZOverbindzorg aan cliënten en de daarmee samenhangende contractuele verplichtingen en ondersteunende processen. Het beleid en de uitwerking hiervan gelden voor alle medewerkers van OZOverbindzorg. Afwijkingen hierop moeten gemeld worden, zodat het management systeem continu verbeterd kan worden. Daarnaast geldt beleid ook voor contractanten, die OZOverbindzorg ondersteunen bij haar dienstverlening aan cliënten. Onlosmakelijk onderdeel van dit beleid is de ethische code, waaraan ook alle medewerkers, contractanten en stagiaires zich dienen te houden. Zoveel mogelijk wordt gestreefd naar het kiezen van beveiligingsmaatregelen gebaseerd op logische principes, omdat deze kosteneffectief en duurzaam zijn. Deze principes zijn:

- Data, die je niet hebt of die niet vertrouwelijk zijn, hoef je ook niet te beveiligen
- Niet slepen met informatie (dus niet kopiëren).
- Scheiden van informatie

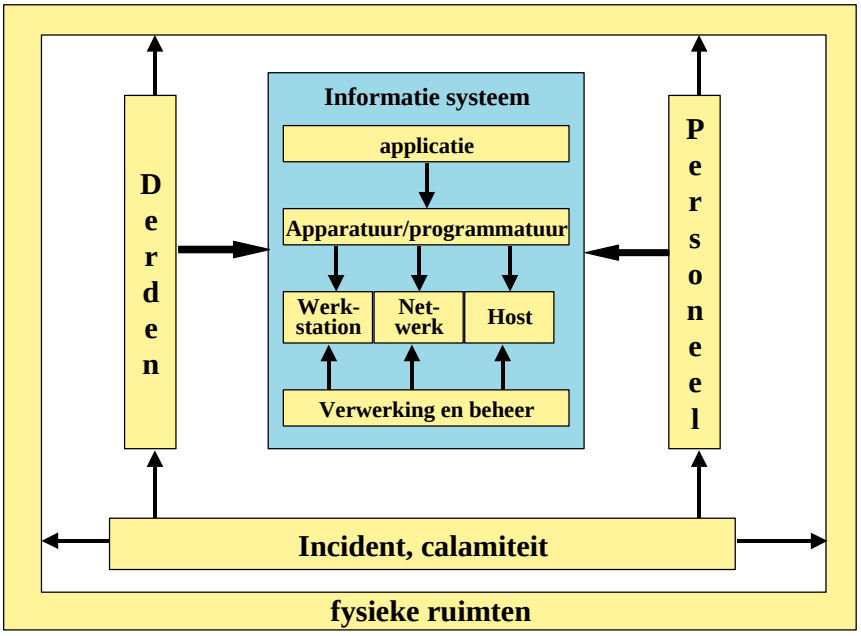
Alle medewerkers worden geacht deze principes in de praktijk te brengen.

3.1 HOUDERSCHAP EN REIKWIJDTE VAN HET BELEID

OZOverbindzorg is dus verantwoordelijk voor het beschikbaar stellen van haar dienst met voldoende beveiligingsopties, zodat haar cliënten kunnen voldoen aan de voor haar geldende IB-normen en andere wet- en regelgeving. Ook voldoet de hosting en het beheer van de software aan deze eisen.

De directie is eindverantwoordelijk voor het betreffende systeem, inclusief het bepalen van bij het systeem te onderkennen risico's, het classificeren van het systeem en de daarbij behorende gegevens en het (laten) ontwikkelen van adequate beveiligingsmiddelen en interne controle-maatregelen.

Naast de applicatie betreft dit ook de juiste inzet van de infrastructurele componenten (werkstations, servers en het interne en externe netwerk), de juiste verwerking, het adequate beheer, het goed functioneren van het personeel, het maken van afspraken met derden, fysieke beveiliging en voorzieningen om incidenten en calamiteiten te voorkomen of af te handelen. In figuur op de volgende pagina zijn alle genoemde deelgebieden van een informatiesysteem opgenomen.



Er wordt gesproken over eindverantwoordelijk omdat een aantal aspecten van het informatiesysteem uitbesteed worden aan andere houders zoals CGM. Hierbij wordt niet een maximaal beveiligingsniveau nagestreefd, maar een optimaal niveau, zodat OZOverbindzorg haar diensten kan bieden tegen een acceptabele kosten.

3.2 UITWERKING VAN DIT BELEID

Op basis van dit beleid worden risico analyses uitgevoerd en wordt een set van maatregelen en controls gedefinieerd als interne norm, dat geldt als minimum voor de dienstverlening aan cliënten. In overleg kan een hoger niveau van beveiliging met een cliënt worden afgesproken.

3.3 CONTROLE WERKING EN NALEVING VAN HET BELEID

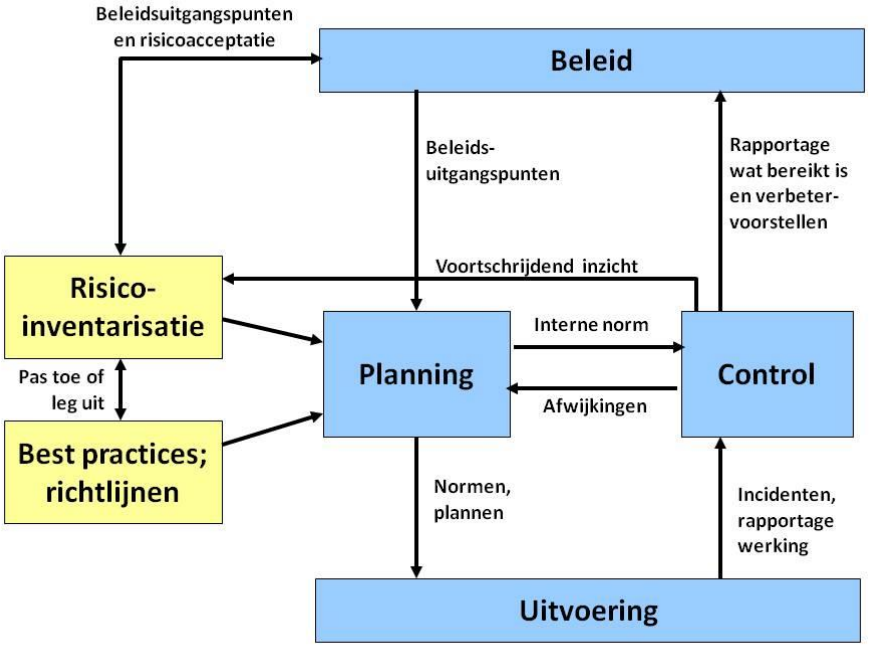
In de directiebeoordeling wordt de werking en de naleving van het beleid intern geëvalueerd en zo nodig aangepast.

Jaarlijks wordt een interne audit gehouden. Onderdeel van deze interne audit zijn het opnieuw beoordelen van risico's en een beoordeling van nieuwe contracten en 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. Op de volgende pagina is dit schematisch weergegeven.

Daarnaast wordt jaarlijks een audit uitgevoerd op de werking van het IB management systeem door een onafhankelijke derde partij, die hiertoe bevoegd en deskundig is. De rapportage hiervan is beschikbaar voor (potentiële) cliënten.

Bij een beveiligingsincident wordt het beleid opnieuw door de directie beoordeeld en waar nodig aangepast.



4 Beleidsuitgangspunten/doelstelling IB

In deze beleidsuitgangspunten/doelstellingen IB geeft de directie aan, op welke wijze zij wil dat de informatiebeveiliging vorm gegeven wordt, die past bij OZOverbindzorg. Bij de verdere invulling van dit beleid dienen de volgende uitgangspunten/doelstellingen IB gehanteerd te worden:

1. Informatiebeveiliging is een belangrijk bedrijfsrisico voor OZOverbindzorg. 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 om te borgen dat het IB-managementsysteem blijvend adequaat werkt en waar nodig verbeterd wordt.
2. OZOverbindzorg conformeert zich m.b.t. de informatiebeveiliging aan de relevante wetgeving en de contractuele afspraken met cliënten en business partners.
3. OZOverbindzorg streeft er naar om haar dienstverlening aan cliënten continu te verbeteren.
4. De doelstellingen en beheersmaatregelen van de norm NEN-ISO/IEC 27001 en de privacy richtsnoeren van de AP vormen, voor zover zij bijdragen aan de informatiebeveiliging van OZOverbindzorg, zijn het uitgangspunt voor de te definiëren maatregelen. Dit is vooral een bedrijfseconomische afweging.
5. OZOverbindzorg 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.
6. Vertrouwen is voor OZOverbindzorg een groot goed en zij hanteert naar medewerkers, cliënten, leveranciers en andere stakeholders het wederkerigheidsprincipe. OZOverbindzorg gaat er vanuit, dat zij afspraken nakomen m.b.t. integriteit, vertrouwelijkheid en continuïteit van de informatievoorziening.

7. Het HRM-beleid is mede gericht op het verbeteren van de integriteit, vertrouwelijkheid en continuïteit van de informatievoorziening bij medewerkers. Tijdens een jaarlijkse evaluatie wordt dit aan de orde gesteld.
8. 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.
9. 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.
10. 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.
11. Bij de verwerking en het gebruik van gegevens worden maatregelen getroffen om de privacy van cliënten, medewerkers en andere betrokkenen te waarborgen.
12. Toegangsbeveiliging zorgt ervoor, dat ongeautoriseerde personen of processen geen toegang krijgen tot de informatiesystemen, gegevensbestanden en programmatuur van OZOverbindzorg.
13. Gegevensverstrekking extern gebeurt op basis van 'need to know'. Intern is dit niet altijd wenselijk omdat kennisdeling essentieel is voor een kosteneffectieve dienstverlening aan cliënten.
14. OZOverbindzorg en haar medewerkers treffen maatregelen om te voorkomen, dat vertrouwelijke informatie in handen van derden terechtkomt.
15. Input van cliënten die vertrouwelijke data bevat, wordt na verwerking op korte termijn gearchiveerd of vernietigd.
16. Datatransport is zodanig met beveiligingsmaatregelen omkleed, dat geen inbreuk kan worden gepleegd op de vertrouwelijkheid en de integriteit van deze gegevens.
17. 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.
18. Productie omgevingen zijn gescheiden van andere omgevingen en hierin kunnen specifiek toegangsrechten worden verleend en is monitoring van de toegang mogelijk.
19. Het beheer en de opslag van gegevens in productie omgevingen zijn zodanig, dat geen informatie verloren kan gaan tenzij er sprake is van overmacht.
20. Er zijn functiescheidingen aangebracht tussen de ontwikkel-, beheer- en gebruikersorganisatie. Voorts wordt functiescheiding toegepast waar dat mogelijk en wenselijk is.
21. Er is een proces om incidenten adequaat af te handelen en hier 'lessons learned' uit te trekken.
22. Er zijn calamiteitenplannen en -voorzieningen om de continuïteit van de informatievoorziening te waarborgen.
23. Bij uitbesteding van gegevensverwerking kan de directie besluiten om tijdelijk af te wijken van deze beleidsuitgangspunten en de risico's hiervan tijdelijk te accepteren.
24. Genoemde beleidsuitgangspunten gelden voor die gegevensbewerkingen, waarvoor OZOverbindzorg wettelijk en/of contractueel verantwoordelijk is.