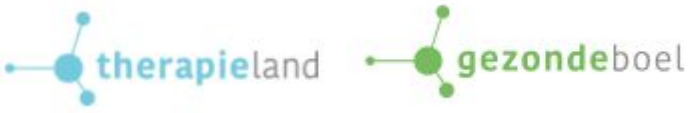
Informatiebeveiligingsbeleid



Auteur	Marjoleine Konersmann
Goedgekeurd door	Jarno Meijer
Datum	Juli 2018
Classificatie	Openbaar

Voorwoord

Informatiebeveiliging speelt een steeds belangrijkere rol in de samenleving. De wereld digitaliseert snel en veel bedrijven en organisaties beheren veel gegevens online. Dit geldt ook voor Therapieland. Ook wij werken met meerdere gegevens, waaronder die van cliënten, behandelaren en zorginstellingen. Therapieland wil groeien en professionaliseren. Goed georganiseerde processen rondom informatiebeveiliging horen bij een gezonde groei.

Therapieland is ISO 27001 en NEN 7510 gecertificeerd. Therapieland laat zich jaarlijks auditen door een externe audit partij.

Marjoleine Konersmann
Security Officer

Inhoudsopgave

Inleiding

Therapieland ontwikkelt online e-mental health applicaties voor onder andere de GGZ en voor de huisartsenzorg. Therapieland ontwikkelt haar applicaties (ook wel programma's of modules genoemd) altijd vanuit de behoefte van de cliënt. Om de cliënt alsook de andere betrokken partijen (denk aan zorginstellingen en behandelaren) het vertrouwen te geven dat Therapieland serieus omgaat met informatie en '*in control'* is, heeft het management, bestaande uit Jarno Meijer en Marike de Haan, besloten het informatiebeveiligingssysteem van Therapieland zo in te richten dat het voldoet aan de eisen van de normen NEN 7510 en ISO 27001.

Dit document beschrijft het informatiebeveiligingsbeleid van Therapieland B.V. (voortaan: Therapieland). Dit document dient als uitgangspunt voor het inrichten van de informatiebeveiliging en is geschreven om de werknemers en belanghebbenden van Therapieland op de hoogte te stellen van voorgenomen processen aangaande informatiebeveiliging. Intern zal het beleid gecommuniceerd worden aan de werknemers via de e-mail. Extern zal het beleid gecommuniceerd worden op de website van Therapieland.

Doelstelling

In 2020 wil Therapieland het informatiebeveiligingsysteem continu verbeteren in overeenstemming met de normen ISO 27001 en NEN 7510.

Definitie informatie

Informatiebeveiliging is een breed begrip. Om dit begrip meer inhoud te geven gaan wij uit van de onder beschreven definities.

Definitie	**Betekenis**
Beschikbaarheid	De mate waarin informatie beschikbaar is.
Integriteit	De mate waarin informatie volledig en juist is ten opzichte van de gebruiker.
Vertrouwelijkheid	De mate waarin de toegang tot informatie beperkt is en alleen toegankelijk is voor gebruikers die daar recht toe hebben.

Gedefinieerde termen

ISMS	Informatiebeveiligingssysteem Information Security Management System.
ISO 27001	De norm specificeert eisen voor het vaststellen, implementeren, uitvoeren, controleren, beoordelen, bijhouden en verbeteren van een gedocumenteerd Information Security Management System (ISMS) in het kader van de algemene bedrijfsrisico's voor de organisatie.
NEN 7510	Informatiebeveiligingsnorm specifiek voor de zorg.
PDCA	De PDCA-cyclus staat voor Plan, Do, Check en Act-cyclus en wordt aangehouden bij het inrichten van het ISMS.
SO	Security officer

Verantwoordelijkheden

Een belangrijk onderdeel van het organiseren van informatiebeveiliging is het vastleggen van rollen en verantwoordelijkheden. Iedereen die werkzaam is voor Therapieland, is verantwoordelijk voor de informatiebeveiliging zoals is vastgelegd in contracten. Echter is het management van Therapieland uiteindelijk hoofdverantwoordelijk. De verantwoordelijkheden zijn vastgelegd middels het RACI-model.

RACI	Persoon	Rol
Accountable	Jarno Meijer en Marike de Haan	Directie/management
Responsible	Marjoleine Konersmann	Security Officer
Informed en Consulted	Medewerkers Therapieland	Afdelingen: Sales, Content Development, Account Management en Training, ICT, Onderzoek en Media.

Scope

In de scope wordt gekeken naar waar de grenzen liggen van het informatiebeveiligingsbeleid van Therapieland.

De samenvatting van de scope is als volgt:

Het ontwikkelen en aanbieden van de online platformen van Therapieland met applicaties voor psychologische ondersteuning die toegankelijk is voor gebruikers die kunnen inloggen met hun persoonlijke account, het verzorgen van de implementatie bij de afnemer, en het leveren van helpdesk & support, in overeenstemming met de verklaring van toepasselijkheid (1.0, datum 27-09-2019).

Behoeften belanghebbende

Een belangrijk onderdeel van de bedrijfsvoering zijn de belanghebbenden. Om zo goed mogelijk in te spelen op de behoeften van de belanghebbenden heeft Therapieland deze in kaart gebracht.

Methode inrichten ISMS

Het ISMS

De normen stellen dat er een Information Security Management System (ISMS) moet worden ingericht. Het management systeem is een raamwerk van processen, procedures, werkwijzen en documenten dat weergeeft hoe een organisatie de taken kan vervullen die nodig zijn om haar doelstellingen omtrent informatiebeveiliging te bereiken *(praktijkboek Informatiebeveiliging in de zorg, Werken met NEN 7510, 2016).*

Overbrengen van belang

Om een goed ISMS in te richten, is het essentieel dat de medewerkers van Therapieland begrijpen waarom informatiebeveiliging van belang is. Zij zijn tenslotte een groot onderdeel van het ISMS en moeten daarom het belang inzien van een goedwerkend informatiebeveiligingssysteem, mede omdat het hun werkzaamheden beïnvloedt. Om het bewustzijn van de werknemers te vergroten worden periodiek activiteiten georganiseerd om de informatiebeveiliging onder de aandacht te brengen.

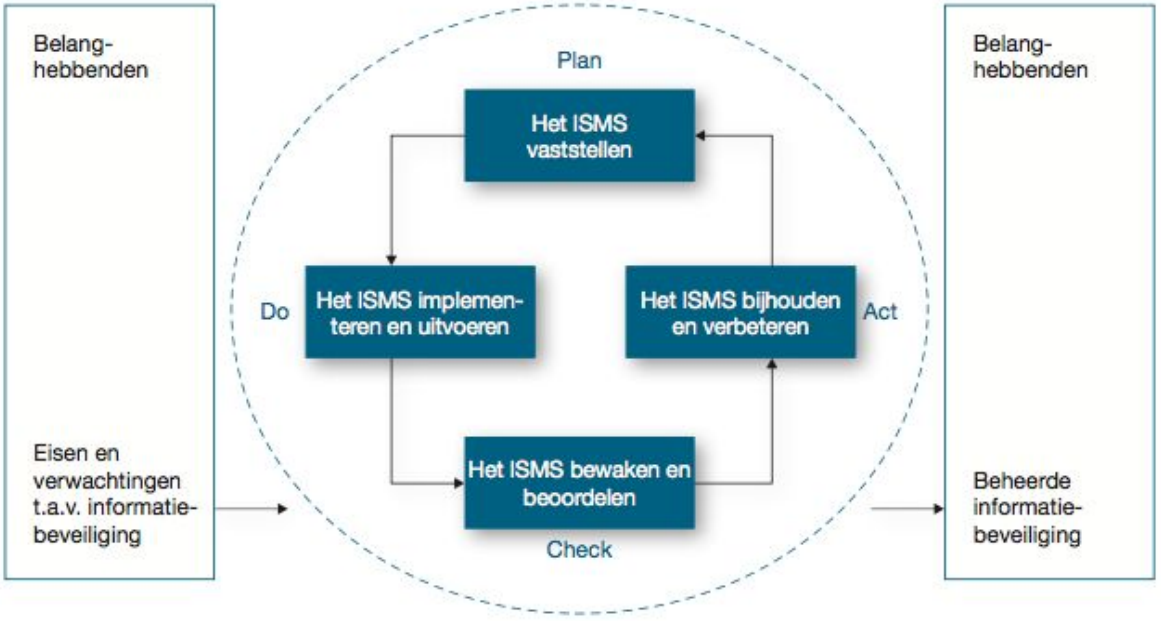
Het aanstellen van de juiste mensen

Om een goed werkend ISMS in te onderhouden is het van belang om de juiste mensen daarvoor aan te wijzen. Het management van Therapieland heeft een Security Officer aangesteld die het ISMS vormgeeft en monitort volgens de richtlijnen van de ISO27001 en de NEN7510 normen. Therapieland streeft naar een platte organisatie, wat betekent dat het management altijd direct betrokken wordt in de uitvoering van het ISMS. Deze sturing wordt direct door het management overgedragen aan de medewerkers.

PDCA Cyclus

Het inrichten van een ISMS is een continu proces. Om echter niet te verzaken in maatregelen en processen wordt de PDCA-cyclus aangehouden. Deze cyclus geeft structurering in het proces en draagt zorg voor meetbare resultaten.

Het raamwerk voor het ISMS bestaat uit de PDCA-cyclus (*Plan, Do, Check, Act*). Dit is een cyclus die continu moet worden doorlopen. Kort gezegd bestaat de cyclus uit het opstellen van een plan voor informatiebeveiliging, het implementeren van het plan, het controleren en evalueren van het plan en uiteindelijk het verbeteren van het ISMS. Zie figuur 1 voor een visuele weergaven. Dit geschreven beleid is ook onderdeel van het ISMS.



Figuur 1 Visuele weergave PDCA-cyclus op ISMS. (Bron: *Praktijkboek Informatiebeveiliging in de zorg, Werken met NEN 7510, 2016).*

Het beleid concretiseren – Plan

In deze fase moet worden gekeken welke processen moeten worden ingericht om het ISMS continue te verbeteren.

Het beleid implementeren en uitvoeren – Do

Het beleid uit de planfase wordt in zijn werking gezet en de integrale risicoanalyse wordt uitgevoerd. Uit deze analyse komen maatregelen voort die worden geïmplementeerd. Tevens wordt de bewustwordingscampagne opgezet.

Het beleid evalueren – Check

In deze fase wordt onderzocht of de ingevoerde maatregelen effect hebben gehad. Dit wordt gemeten aan de hand van een interne audit waarbij de Security Officer nagaat waar het ISMS verbeterd kan worden.

Het beleid verbeteren en actueel houden – Act

In deze laatste fase worden de verbeterpunten uit de interne audit doorgevoerd. Daarna zal de cyclus opnieuw worden doorlopen.

Controle werking en naleving van het beleid

Controle medewerkers

De Security Officer controleert of de medewerkers van Therapieland het beleid naleven.

Controle Security Officer

Het management van Therapieland controleert of de Security Officer het ISMS inricht, uitvoert, evalueert en verbetert zoals beschreven in de methodiek.

Controle Therapieland

Een externe audit-organisatie zal Therapieland toetsen op de eisen van de normen.

Beleidsuitgangspunten

Therapieland heeft als doel psychologische kennis en expertise middels it oplossingen dicht bij mensen te krijgen. Hierbij streeft Therapieland ernaar om de eigen regie van gebruikers te vergroten, inspirerende en effectieve interventies aan te bieden en om gebruikers een sociaal en/of professioneel netwerk rondom zichzelf te laten organiseren.

Therapieland heeft als doel 1 miljoen mensen te helpen. Het helpen van deze mensen moet op een veilige wijze waarbij rekening wordt gehouden met privacy en security.

Bij alle werkzaamheden laten de medewerkers van Therapieland zich leiden door de kernwaarden. Deze zijn: bevlogen, betrouwbaar, nieuwsgierig, samen, ondernemend.

Informatiebeveiliging is van essentieel belang binnen Therapieland en dient in alle bedrijfsprocessen meegenomen te worden. Therapieland wil ten alle tijden secuur, integer en verantwoordelijk omgaan met de informatie die klanten aan Therapieland toevertrouwen.

Doelen

Omdat bewustwording een belangrijk onderdeel is van het beleid omtrent informatiebeveiliging zal de kennis die nodig is om de informatiebeveiliging te waarborgen onder werknemers worden gedeeld, geactiveerd en periodiek worden getest door middel van interne audits.

Het ISMS focust zich op de domeinen beschikbaarheid, integriteit en vertrouwelijkheid door de in het ISMS vastgelegde beheersmaatregelen te implementeren in de processen, handelingen en systemen van Therapieland.

Therapieland heeft een beleid omtrent informatiebeveiliging waarin alle normen zijn meegenomen en waarin ook wordt benoemd hoe lering wordt getrokken uit incidenten voor continue verbetering van het ISMS

Therapieland zal in zijn beleid de rollen en verantwoordelijkheden voor het waarborgen van integriteit, beschikbaarheid en vertrouwelijkheid in het ISMS benoemen zodat de rollen en verantwoordelijkheden altijd duidelijk zijn en opgevangen kunnen worden.

Therapieland heeft een ISMS geïmplementeerd welke de risico's mitigeert naar een acceptabel risiconiveau.

Therapieland zal belanghebbenden wijzen op het beleid en de daarin relevante content zodat ook zij op de hoogte zijn van het ISMS.

Therapieland conformeert zich met betrekking tot de informatiebeveiliging aan de relevante wetgeving en de contractuele afspraken met belanghebbenden.

Therapieland hanteert het wederkerigheidsprincipe naar medewerkers en belanghebbenden met betrekking tot vertrouwen. Therapieland gaat ervan uit dat zij afspraken nakomen met betrekking tot integriteit, vertrouwelijkheid en continuïteit van informatievoorziening.

Therapieland heeft een HR beleid mede gericht op het verbeteren van integriteit, vertrouwelijkheid en beschikbaarheid.

Therapieland heeft de fysieke omgeving van gegevens dusdanig ingericht dat de vertrouwelijkheid, integriteit en beschikbaarheid van gegevens wordt gewaarborgd.

Therapieland heeft met haar belanghebbenden afspraken omtrent een samenwerking waarin wordt meegenomen dat de vertrouwelijkheid, integriteit en beschikbaarheid van de informatievoorziening niet wordt aangetast.

Therapieland beschikt over calamiteitenplannen en -voorzieningen om de continuïteit van de informatievoorzieningen te waarborgen.

De toegangsbeveiliging van Therapieland zorgt ervoor dat ongeautoriseerde personen of processen geen toegang krijgen tot de informatiesystemen en gegevensbestanden van Therapieland.

In het geval van uitzonderlijke noodsituaties zal Therapieland mogelijk afwijken van de standaardprocedures die gebaseerd zijn op het ISMS. Wel zal Therapieland haar uiterste best doen in deze situaties om alsnog volgens protocol te handelen.