Informatiebeveiligingsbeleid

Document nummer	ISMS 2
Versie	1.4
Auteur	M. Konersmann
Goedgekeurd door	J. Meijer
Datum	30-08-2017
Classificatie	Openbaar

Versie	**Datum**	**Reden voor opmaak**	Aangepast door
1.0	21-02-2017	Ontwikkeling document	M. Konersmann
1.1	03-07-2017	Vernieuwen document	M. Konersmann
1.2	10-08-2017	Aanpassen scope	M. Konersmann
1.3	26-08-2017	Vernieuwen document	M. Konersmann
1.4	30-08-2017	Vernieuwen document	M. Konersmann

Versie	**Goedgekeurd door**	**Rol**	**Datum**
1.0	Jarno Meijer	Directeur	21-02-2017
1.1	Jarno Meijer	Directeur	03-07-2017
1.2	Jarno Meijer	Directeur	10-08-2017
1.3	Jarno Meijer	Directeur	26-08-2017
1.4	Jarno Meijer	Directeur	30-08-2017

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 van cliënten, behandelaren en zorginstellingen.

Therapieland wil groeien en professionaliseren. Goed georganiseerde processen rondom informatiebeveiliging horen bij een gezonde groei. Therapieland wil haar klanten en cliënten laten zien dat zij informatiebeveiliging serieus neemt.

Om de informatiebeveiliging te optimaliseren is gekozen om een traject op te zetten waarmee Therapieland zich laat certificeren voor de informatiebeveiligingsnormen NEN 7510 en ISO 27001.

Marjoleine Konersmann
Security Officer

Inhoudsopgave

1. Inleiding

Therapieland ontwikkelt online e-mental health applicaties voor onder andere de GGZ en voor de huisartsenzorg. Therapieland ontwikkelt zijn 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 2700. Voor meer informatie over de doelstellingen, visie en missie van Therapieland verwijzen wij naar het strategiedocument van Therapieland.

Dit document omschrijft 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.

1.1 Doelstelling

In 2017 wil Therapieland de informatiebeveiliging zo optimaliseren dat wij in aanmerking komen voor een ISO 27001 en NEN 7510 certificaat – Jarno Meijer en Marike de Haan.

1.2 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 voor de gebruiker.
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.

1.3 Gerelateerde documenten

- Strategie Therapieland
- ISO 27001 & NEN 7510
- Scope Therapieland, doc. nr.: ISMS 1
- Behoeften belanghebbenden
- Inventarisatie informatie en middelen

1.3 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.

2. 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**
Responsible	Jarno Meijer en Marike de Haan	Directeuren
Accountable	Marjoleine Konersmann	Security Officer, helpdesk en support
Informed en Consulted	Medewerkers Therapieland	Afdelingen: sales, content development, account management en training, ICT, onderzoek, video.

3. Scope

In de scope wordt gekeken waar de grenzen liggen van het informatiebeveiligingsbeleid van Therapieland. Het beleid is van toepassing op alle informatie die wordt ontvangen, verzonden en bewaard door Therapieland. Voor een overzicht van vormen van informatie wordt verwezen

naar het Excel-document: Inventarisatie Informatie en Middelen. Het beleid geldt voor alle werknemers van Therapieland.

Voor een uitgebreide beschrijving van de scope wordt verwezen naar het document: scope Therapieland, doc nr: ISMS 1.

De samenvatting van de scope is als volgt:

De scope van het ISMS heeft betrekking op de gehele organisatie van Therapieland, haar diensten en activiteiten. Onder deze diensten en activiteiten vallen het ontwikkelen en aanbieden van het platform met online programma's, implementatietrajecten bij klanten, helpdesk & support en het bewerken en verwerken van (patiënt)gegevens in overeenkomst met de verklaring van toepasselijkheid (Versie 1.0 , datum 26 augustus 2017).

4. Behoeften belanghebbende

Therapieland wordt in stand gehouden door haar belanghebbenden. Therapieland is afhankelijk van behandelaren die Therapieland inzetten en tevens ook van cliënten die een of meerdere programma's van Therapieland volgen. Dergelijke belanghebbenden zijn volledig in kaart gebracht in het bestand 'Behoeften belanghebbenden'. Therapieland wil naar haar belanghebbenden het signaal afgeven informatiebeveiliging serieus te nemen.

5. 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).*

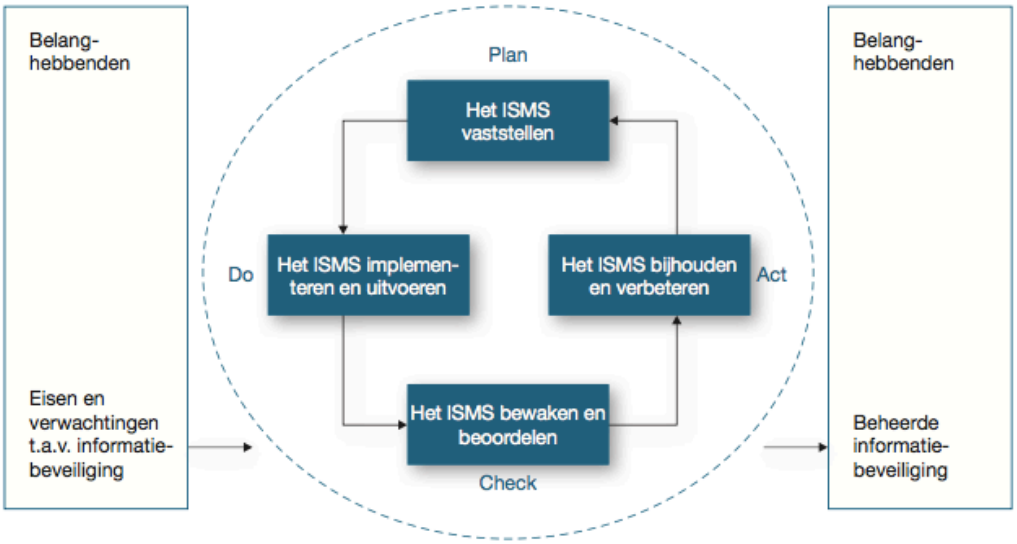
Overbrengen van belang
Om een goed ISMS in te richten, is het essentieel dat de medewerkers van Therapieland ook begrijpen waarom informatiebeveiliging van belang is. Zij zijn tenslotte een groot onderdeel van het ISMS en moeten daarom het belang inzien van een goedwerkend informatiebeveiligingssysteem, ook als dat betekent dat het hun werkzaamheden zal beïnvloeden. Om het bewustzijn van de werknemers te vergroten zal een bewustwordingscampagne worden opgezet.

Het aanstellen van de juiste mensen
Om een optimaal ISMS in te richten is het van belang om de juiste mensen daarvoor aan te wijzen. Het management van Therapieland heeft een Security Officer aangesteld die het ISMS zal inrichten. Therapieland is vooralsnog een platte organisatie, wat betekent dat in het jaar 2017 geen managers zijn aangesteld die de sturing van het beleid op zich nemen. Deze

sturing wordt direct door het management overgedragen aan de medewerkers.

Resultaat garanderen
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.

PDCA Cyclus
Het raamwerk voor het ISMS bestaat uit de PDCA-cyclus (Plan, Do, Check, Act). Dit is een cyclus die continu moet worden doorlopen. Kortgezegd 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 wordt gekeken wat er allemaal nodig is voor het inrichten van een ISMS. Een Security Officer zal worden aangesteld, de behoeften van belanghebbenden van de organisatie worden onderzocht en beschreven, de scope wordt opgesteld, verantwoordelijkheden worden vastgelegd en er wordt een methode beschreven voor het uitvoeren van een integrale risicoanalyse.

Het beleid implementeren en uitvoeren – Do
Het beleid uit de planfase wordt in zijn werking gezet en de integrale risico analyse 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.

6. 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.

7. Beleidsuitgangspunten

Therapieland stelt zich ten doel om op een verantwoorde en lucratieve manier haar bedrijf uit te oefenen in de zorgsector en op gelijknamige wijze te werken aan haar missie, namelijk het bieden van de beste e-Healthoplossingen voor de huisartsenzorg, de GGZ, de bedrijfsgezondheidszorg en daarnaast voor mensen die aan de slag willen met online zelfhulp. Bij al onze werkzaamheden laten wij ons leiden door onze gemeenschappelijke kernwaarden van professionaliteit, enthousiasme, integriteit en innovatie. Ten grondslag aan onze kernwaarden ligt het uitgangspunt om altijd secuur om te gaan met gevoelige en persoonlijke informatie volgens het privacy-beleid wat in al onze werkzaamheden wordt gewaarborgd.

8. Doelen

In 2017 heeft Therapieland een bewustwordingscampagne opgezet bestaande uit: een training voor medewerkers, een online bewustwordingstool en ontwikkeling van posters.

In 2017 kunnen de medewerkers van Therapieland voorbeelden noemen van hoe zij in hun werkzaamheden de vertrouwelijkheid, beschikbaarheid en integriteit van gegevens kunnen waarborgen.

In 2017 weten de werknemers van Therapieland waar zij documenten aangaande informatiebeveiliging kunnen vinden.

In 2017 weten de werknemers van Therapieland hoe zij moeten handelen na het signaleren van een incident omtrent informatiebeveiliging.

In 2017 heeft Therapieland maatregelen doorgevoerd die ervoor zorgen dat informatie op de domeinen beschikbaarheid, integriteit en vertrouwelijkheid worden gewaarborgd.

In 2017 wil Therapieland zijn risico's in kaart brengen middels een integrale risicoanalyse. De kansen, gevolgen en maatregelen zullen hiervoor gedefinieerd worden.

In 2017 wil Therapieland beleid hebben ontwikkeld dat zal vormgeven hoe Therapieland omgaat met incidenten, hoe deze beheerd worden en hoe er lering wordt getrokken uit incidenten voor verder beleid.

In 2017 zal Therapieland een interne audit uitvoeren waarin aan de hand van interviews wordt getest of het geïmplementeerde beleid bij de medewerkers wordt opgevolgd.

In 2017 zal beleid worden aangepast aan de hand van de verbeterpunten uit de interne audit.

In 2017 zal Therapieland een Security Officer aanwijzen die verantwoordelijk is voor het vormgeven van het ISMS.

In 2017 zal de Security Officer maandelijks met het management overleg hebben om het ISMS vorm te geven. Daarnaast zal informatiebeveiliging een terugkerend onderdeel zijn in maandoverleggen.

In 2017 zal Therapieland zijn belanghebbenden in kaart hebben gebracht.

In 2017 zal Therapieland de soorten informatie samen met de bedrijfsmiddelen die zij beheert, inclusief de toegang daartoe, in kaart hebben gebracht.

In 2017 zal Therapieland hebben vormgegeven hoe zij het beleid communiceren naar belanghebbenden.

In 2017 heeft Therapieland zijn fysieke omgeving (pand) volledig in kaart gebracht.

In 2017 heeft Therapieland een duidelijk beeld van het toepassingsgebied van het ISMS. Dit zal beschreven worden in een scope.

In 2017 heeft Therapieland de toegang tot systemen en middelen van Therapieland afgedekt middels een wachtwoordbeleid.

In 2017 heeft Therapieland bij het in- en uit dienst treden van medewerkers protocollen opgesteld die doorlopen moeten worden zodat de informatie kan worden beveiligd.

In 2017 zal Therapieland met belanghebbenden eenmaal per jaar overleggen over de informatiebeveiliging.

In 2017 zal controle op de bovengenoemde doelen plaatsvinden door het management.

Bijlagen A – Bronnen

Praktijkboek NEN 7510 herzien, B. Franken & J.W.Schoemaker (2016).

Bijlagen B:

Verklaring van betrokkenheid management

Hierbij verklaart het management betrokken te zijn geweest bij het vormgeven van het beleidsdocument informatiebeveiliging van Therapieland. Het management onderschrijft daarmee de opgestelde doelen en geeft de Security Officer de middelen en de ruimte het informatiebeveiligingssysteem optimaal in te richten, ook als daar financiële middelen voor nodig zijn. Het management verbindt zich met het beleid door zich te houden aan onderstaande eisen:

- Het management is betrokken doordat zij maandelijks overleg hebben met de Security Officer omtrent informatiebeveiliging;
- Het management geeft de Security Officer toestemming objectief te handelen;
- Het management voorziet het beleid en de ingevoerde maatregelen van feedback zodat het ISMS continu verbeterd kan worden;
- Het management draagt zorg voor de betrokkenheid onder werknemers door deze betrokkenheid contractueel vast te leggen;
- Het management controleert of het beleid wordt uitgevoerd en of verbeterpunten continu worden doorgevoerd.

Handtekening:

Datum: ../.../…/