Inhoudsopgave

1 Onderwerp en toepassingsgebied

2 Normatieve wijzigingen

3 Termen en definities

4 Context van de organisatie

4.1 Inzicht verkrijgen in de organisatie en haar context

James Software B.V. ("Organisatie") is leverancier van een software voor paramedische praktijken. De software wordt ter beschikking gesteld als webbased applicatie en opslag van data in een private cloud (SAAS model). De belangrijkste functionaliteiten van de Webapplicatie zijn: agenda, patiënten, dossiers, facturatie / declaratie en patiënten portaal. In de Webapplicatie worden persoons- en gezondheidsgegevens van patiënten / cliënten van paramedische praktijken opgeslagen.

De Organisatie heeft 9 medewerkers die zich bezighouden met sales, projectmanagement, applicatie-ontwikkeling en support. Infrastructuurdiensten (virtuele servers, storage en back up) worden uitbesteed.

Het doel van de Organisatie is het maximaliseren van winst en aandeelhouderswaarde.

De Organisatie stelt de volgende onderwerpen vast die relevant zijn voor haar doelstelling en die tegelijk haar vermogen beïnvloeden om de beoogde resultaten van haar managementsysteem voor informatiebeveiliging te behalen:

- Interne factoren
  - Ontwikkelen Webapplicatie
  - Hosting Webapplicatie en opslag gezondheidsgegevens
  - Support leveren aan klanten
  - Insider threats t.a.v. informatiebeveiliging

  Externe factoren
  - De ontwikkeling van wet- en regelgeving in de gezondheidszorg, onder andere informatiebeveiliging en privacy
  - Outsider threats t.a.v. informatiebeveiliging

4.2 Behoeften en verwachtingen van belanghebbenden

De Organisatie heeft de volgende externe belanghebbenden: klanten, patiënten / cliënten van klanten en VECOZO. De Organisatie beheert persoons- en gezondheidsgegevens van patiënten en cliënten van haar klanten. De Organisatie van adequate informatiebeveiliging als samenhangend geheel van beschikbaarheid, integriteit en vertrouwelijkheid van persoons- en gezondheidsgegevens is voor ieder van deze partijen van belang. Bij patiënten / cliënten vloeit dit direct voort uit de Algemene verordening gegevensbescherming, bij de andere belanghebbenden is dit een contractuele eis. De Organisatie streeft hierbij continue naar verbetering van de informatiebeveiliging.

4.3 Toepassingsgebied managementsysteem

Het managementsysteem voor informatiebeveiliging is van toepassing op alle in paragraaf 1.1 genoemde interne en externe factoren alsmede op de behoeften en verwachtingen uit paragraaf 1.2 in relatie tot de persoons- en gezondheidsgegevens van derden die beheerd worden door de Organisatie. Meer specifiek ziet het managementsysteem op de activa en alle hiermee samenhangende processen van de Organisatie. De activa van de Organisatie bestaan uit: data, personeel, infrastructuur en applicaties. De processen betreffen onder andere het ontwikkelen van de Webapplicatie, de SAAS dienstverlening en veilig personeel. Het informatiebeveiligingsbeleid is ook van toepassing op de gegevensuitwisseling van de Organisatie met andere organisaties en personen. Het toepassingsgebied wordt nader uitgewerkt in de risicoanalyse.

4.4 Managementsysteem voor informatiebeveiliging

Het managementsysteem voor informatiebeveiliging omvat de volgende vijf stappen o.b.v. de Deming cirkel: *beleidsvorming -> risicoanalyse -> planvorming -> implementatie -> monitoring, evaluatie, controle (waarna de cirkel opnieuw begint met beleidsvorming, etc).*

De samenhang tussen deze vijf stappen en de Deming cirkel is als volgt:

- Plan : Beleidsvorming en Risicoanalyse
- Do : Planvorming en Implementatie
- Check : Monitoring, evaluatie en controle
- Act : Het verbeterproces

Het managementsysteem voor informatiebeveiliging wordt hieronder nader uitgewerkt.

4.4.1 Beleidsvorming

Zoals ook aangegeven in paragraaf 1, start het managementsysteem voor informatiebeveiliging met het opstellen van het informatiebeveiligingsbeleid. In dit beleid worden de doelstellingen en uitgangspunten voor informatiebeveiliging van de Organisatie vastgelegd. Hiermee vormt het beleid de leidraad voor de overige stappen van het managementsysteem.

4.4.2 Risicoanalyse

De tweede stap van het managementsysteem voor informatiebeveiliging bestaat uit risicoanalyse. Het analyseren van de risico's heeft tot doel:

- Inzicht te krijgen in de kwaliteit en de effectiviteit van de bestaande beveiligingsmaatregelen.
- Inzicht te krijgen in de risico's die de realisatie van het gewenste beveiligingsniveau in gevaar kunnen brengen.
- Het gewenste niveau van informatiebeveiliging vast te stellen in de vorm van een classificatie van bedrijfsprocessen, informatiesystemen en gegevensverzamelingen.
- Keuzes te kunnen maken voor het beheersen van risico's.
- Prioriteiten te bepalen voor de verbetering van de bestaande situatie.

4.4.3 Planvorming

Op basis van de uitkomsten van de risicoanalyse wordt een verbeterplan opgesteld. In dit plan worden de verbeteractiviteiten voor de realisatie van het gewenste beveiligingsniveau op projectmatige wijze vastgelegd.

4.4.4 Implementatie

Aan de hand van het verbeterplan wordt de implementatie van de aanvullende beveiligingsmaatregelen ter hand genomen. Dit betekent onder andere het opstellen van richtlijnen en procedures voor informatiebeveiliging, het invoeren van beveiligingshulpmiddelen en het voorlichten en opleiden van medewerkers.

4.4.5 Monitoring, evaluatie en controle

De laatste stap van het managementsysteem voor informatiebeveiliging bestaat uit monitoring, evaluatie en controle. Monitoring betreft het continu bewaken van het niveau van informatiebeveiliging binnen de Organisatie. Daar waar dit niveau in gevaar komt door het optreden van bedreigingen treedt incidentmanagement in werking om het gewenste beveiligingsniveau te waarborgen of zo snel mogelijk te herstellen.

4.4.6 Het verbeterproces

Het managementsysteem voor informatiebeveiliging omvat een continu en cyclisch proces. Dit betekent dat op basis van de uitkomsten van evaluaties en controles of door nieuwe ontwikkelingen de noodzaak aanwezig kan zijn het informatiebeveiligingsbeleid aan te passen, een nieuwe risicoanalyse uit te voeren, extra maatregelen te treffen of de implementatie hiervan aan te passen. Ook is het mogelijk dat nieuwe ontwikkelingen, zoals de introductie van nieuwe bedrijfsprocessen of informatiesystemen, aanleiding geven om het informatiebeveiligingsbeleid te heroverwegen.

5 Leiderschap

5.1 Leiderschap en betrokkenheid

De directie;

- Implementeert een managementsysteem voor informatiebeveiliging
- Formuleert het informatiebeveiligingsbeleid en -doelstellingen
- Kent rollen en verantwoordelijkheden voor de informatiebeveiliging toe
- Benoemt een Security Officer en een externe auditor
- Bevordert het informatiebeveiligingsbewustzijn van het personeel
- Voert een risicoanalyse uit en stelt een verbeterplan op
- Zorgt voor de middelen nodig voor de uitvoering van het verbeterplan
- Zorgt voor meten van prestaties, evaluatie en een volgend verbeterplan

5.2 Informatiebeveiligingsbeleid van James Software B.V.

5.2.1 Doelstelling en toepassingsgebied

Informatiebeveiliging wordt als volgt gedefinieerd:
Het samenhangend stelsel van maatregelen dat zich richt op het blijvend realiseren van een optimaal niveau van beschikbaarheid, integriteit en vertrouwelijkheid van persoonsgegevens van derden (waaronder gezondheidsgegevens).

Beschikbaarheid, integriteit en vertrouwelijkheid worden als volgt gedefinieerd:
- *Beschikbaarheid*, de informatie moet op de gewenste momenten beschikbaar zijn;
- *Integriteit*, de informatie moet juist en volledig zijn en de informatiesystemen moeten juiste en volledige informatie opslaan en verwerken;
- *Vertrouwelijkheid*, de informatie moet alleen toegankelijk zijn voor degene die hiervoor bevoegd is.

Het informatiebeveiligingsbeleid is van toepassing op de Organisatie en de gegevensuitwisseling van de Organisatie met externe partijen.

Informatiebeveiliging heeft tot doel het optreden van bedreigingen die bovenstaande aspecten van de informatievoorziening kunnen schaden, te voorkomen en/of te beperken.

5.2.2 Informatiebeveiligingsdoelstellingen

1. De Organisatie implementeert een managementsysteem om informatiebeveiligingsrisico's te beheersen
2. De Organisatie voert een risico-analyse uit met betrekking tot de beschikbaarheid, integriteit en vertrouwelijkheid van persoonsgegevens van derden (waaronder gezondheidsgegevens)
3. Teneinde informatiebeveiligingsrisico's te elimineren / mitigeren implementeert de Organisatie beheersmaatregelen op de volgende terreinen:
    - Personeel
    - Bedrijfsmiddelen
    - Toegang tot informatiesystemen en data
    - Cryptogafie
    - Fysieke beveiliging
    - Beveiliging van de bedrijfsvoering
    - Communicatiebeveiliging
    - Ontwikkeling en onderhoud van informatiesystemen
    - Leveranciersrelaties
    - Beheer van informatiebeveiligingsincidenten
    - Informatiebeveiligingsaspecten van bedrijfscontinuïteitsbeheer
    - Naleving van relevante wet- en regelgeving
4. Het informatiebeveiligingsbeleid en de implementatie hiervan door de Organisatie voldoen aan van toepassing zijnde wetgeving zoals AVG, Wet BSN in de Zorg en contractuele afspraken met klanten

5.3 Rollen en verantwoordelijkheden

5.3.1 Directie

De directie is eindverantwoordelijk voor het informatiebeveiligingsbeleid en heeft dit beleid vastgesteld door middel van dit document. De directie is ook enige verantwoordelijke met betrekking tot de uitvoering van het beleid en de planning. De directie voert het autorisatiebeheer m.b.t. de toegang tot informatiesystemen.

5.3.2 Security Officer

De Security Officer heeft de volgende taken:

- Het voorbereiden van de beleidsvorming m.b.t. informatiebeveiliging
- Het coördineren van de implementatie van beveiligingsmaatregelen
- Het monitoring en controle van informatiebeveiligingsmaatregelen binnen de Organisatie (interne auditor rol)
- Het signaleren van tekortkomingen in de naleving van het informatiebeveiligingsbeleid
- Het voorlichten en stimuleren van het beveiligingsbewustzijn bij alle betrokkenen
- Evaluatie en advies, het adviseren van de directie over informatiebeveiliging
- Het uitvoeren van een risico-analyse
- Het opstellen en coördineren van een verbeterplan m.b.t. informatiebeveiliging
- Het uitvoeren en coördineren van de implementatie van beveiligingsmaatregelen
- Het centraal registreren van ICT-beveiligingsincidenten
- Het analyseren en beoordelen van ICT-beveiligingsincidenten
- Het centraal informeren van gebruikers over (potentiële) ICT-beveiligings-incidenten
- Het coördineren van de uitvoering van preventieve en herstelacties.
- De Security Officer heeft geen andere bevoegdheden dan de hier genoemde en rapporteert aan de directie

5.3.3 Auditor

De Organisatie maakt gebruik van een externe auditor die iedere 3 jaar een audit uitvoert m.b.t. het niveau van de informatiebeveiliging. De auditor rapporteert aan de directie.

6. Planning

6.1 Maatregelen om risico's te beperken en kansen te benutten

6.1.1. Algemeen

De directie dient te bewerkstelligen dat het managementsysteem zijn beoogde resultaten behaald, ongewenste effecten te voorkomen / beperken, continu verbetering te bereiken. Voorts dient de directie maatregelen te plannen risico's te beperken en de doeltreffendheid hiervan te meten en te evalueren.

6.1.2 Risicobeoordeling van informatiebeveiliging

6.1.2.1 Doelstelling risicoanalyse en -methode

Het uitvoeren van een risicoanalyse heeft tot doel de gevolgen van bedreigingen, waaraan een bedrijfsproces, een informatiesysteem of informatie van de Organisatie blootstaat te analyseren en op grond hiervan een passend beveiligingsniveau te bepalen.

De risicoanalysemethode van de Organisatie omvat de volgende stappen:

1. Scope en business impact analyse
2. Object van analyse, bedreigingen en reeds genomen maatregelen
3. Score risico(klassen), aanvaardbare restrisico's en aanvullende maatregelen

6.1.2.2 Scope en business impact analyse

Het vaststellen van de scope van de risicoanalyse betreft het bepalen welke objecten (fysiek bedrijfsmiddel, bedrijfsproces, informatiesysteem of informatie) wel en niet onderdeel zijn van de risicoanalyse. Door middel van een business impact analyse wordt bepaald of een

object een kernobject van de organisatie is. Alleen kernobjecten worden in de risicoanalyse betrokken. Voor het uitvoeren van de business impact analyse worden de criteria “voortgang primair proces”, “voldoen aan de AVG” en “imago” in relatie gebracht met de impact op beschikbaarheid, integriteit en vertrouwelijkheid. De impact kan hoog, middel of laag zijn. Als een object op één van de criteria een impactscore “Hoog” heeft wordt het object als kernobject geclassificeerd.

In onderstaande tabel worden de criteria voor het uitvoeren van de business impact analyse vastgesteld.

Criterium	Context	Hanteren
Lichamelijke schade of overlijden van patiënten	De klanten van de Organisatie zijn voornamelijk paramedische praktijken. Het is niet waarschijnlijk dat het niet beschikbaar zijn van patiënteninformatie zal lijden tot lichamelijke schade of overlijden van een patiënt	Nee
Voortgang van het primaire bedrijfsproces	Dit is een belangrijk criterium bij de Organisatie en/of haar klanten.	Ja
Voldoen aan de wet bescherming persoonsgegevens	In de systemen van de Organisatie zijn gegevens opgeslagen, privacy is erg belangrijk	Ja
Financiële gevolgen	Beperkte financiële gevolgen hebben veelal geen impact en grote financiële gevolgen zijn meer verbonden met imagoschade	Nee
Imago schade	Voor de groei en continuïteit van de Organisatie is dit een cruciaal criterium om te managen	Ja
Verlies van unieke middelen	Zijnde gegevens, dossiers en archieven. Dit is hetzelfde als permanent niet beschikbaarheid. In de BIA is niet beschikbaarheid een scenario en daarom is het niet logisch om dit ook als criterium te hanteren	Nee
Gevolgen voor de kwaliteit van het bedrijfsproces	Dit criterium heeft teveel overlap met de voortgang van het primaire bedrijfsproces om voldoende onderscheidend te zijn	Nee

In onderstaande tabel wordt de impact per criterium vastgesteld naar laag, middel, hoog.

Criterium	Laag	Middel	Hoog
Voortgang primair proces (operatie)	De Web-applicatie is maximaal 15 minuten niet beschikbaar. Of verlies van maximaal 40 uur werk aan bedrijfsdocumenten.	De Web-applicatie is minimaal 15 en maximaal 60 minuten niet beschikbaar. Of verlies van min. 40 uur en maximaal 400 uur werk aan bedrijfsdocumenten.	De Web-applicatie is meer dan 60 minuten niet beschikbaar. Of verlies van min. 400 uur en max 4000 uur werk aan bedrijfsdocumenten.
Voldoen aan AVG	Er heeft zich een beveiligingsincident voorgedaan	N.v.t	Er zijn bij de inbreuk persoonsgegevens verloren gegaan en / of kan niet redelijkerwijs worden uitgesloten dat er persoonsgegevens onrechtmatig zijn verwerkt.
Imago James Software	Enkele klanten verliezen het vertrouwen in de Organisatie	Meerdere klanten verliezen het vertrouwen in de Organisatie en maken dit kenbaar via social media	Veel klanten stappen over naar concurrenten en prospects haken af vanwege de Organisatie

6.1.2.3 Object van analyse, bedreigingen en reeds genomen maatregelen

Afhankelijk van de vraagstelling van de risicoanalyse kan het object van analyse verschillen. In het algemeen kan een risicoanalyse worden uitgevoerd voor een fysiek bedrijfsmiddel, een bedrijfsproces, een informatiesysteem of voor informatie (gegevensverzameling, database, document) en personeel.

Op basis van een selectie uit de standaardlijst van bedreigingen (Threat taxonomy 2016) van de European Union Agency for Cyber Security worden de relevante bedreigingen voor het object van analyse bepaald.

De maatregelen die reeds zijn genomen worden afgezet tegen de bedreigingen.

6.1.2.4 Score risico(klassen), aanvaardbare restrisico's en aanvullende maatregelen

Aan de hand van een bedreiging en de reeds genomen tegenmaatregelen wordt de kans geschat dat een informatiebeveiligingsincident optreedt. De kans van optreden wordt uitgedrukt in Laag, Hoog, Middel. In de tabel hieronder wordt aangegeven wat deze kwalificaties inhouden.

Kans / Klasse	Laag	Middel	Hoog
Keren per jaar	0,03 - 0,3 /jr	0,3 - 3 / jr	3 - 30 /jr

Vervolgens wordt de impact van een bedreiging op de criteria beschikbaarheid, integriteit en vertrouwelijkheid bepaald. De impact wordt ook uitgedrukt in Hoog, Middel, Laag zoals hierboven in 3.1.2 bepaald.

Voor de bepaling van het risico wordt de formule K x I = R gebruikt, waarbij K = kans, I = impact en R = risico. In totaal zijn er 9 risicoklassen, welke variëren van LL tot HH. Risico's in de volgende klassen moeten worden gemitigeerd: HH, MH en MM.

Kans / Impact	Laag	Middel	Hoog
Laag	LL	LM	LH
Middel	ML	MM	MH
Hoog	HL	MM	HH

Met betrekking tot scores in de risicoklassen MM, MH en HH moet de Organisatie aanvullende maatregelen treffen. Scores in de risicoklassen LL, ML, HL, LM en LH worden beschouwd als aanvaarbare restrisico's.

6.1.3 Behandeling van informatiebeveiliginsrisico's

De verklaring van toepasselijkheid is geïntegreerd in het document 'Beheersmaatregelenen verklaring van toepasselijkheid'. Op van de reeds geïmplementeerde beheersmaatregelen en de uitkomsten van de risico-analyse neemt de Organisatie aanvullende beheersmaatregelen.

6.2. Informatiebeveiligingsdoelstellingen en de planning om ze te bereiken

De planning van de aanvullende beheersmaatregelen om de beveiligingsdoelstellingen te bereiken en de periodieke meting van de werking van beheersmaatregelen is vastgelegd in het document 'Planning verbeterpunten en controle'. De interne communicatie is onderdeel van de planning. De Security Officer is verantwoordelijk voor de uitvoering van de planning.

De planning, realisatie en werking van de geïmplementeerde maatregelen worden besproken in het informatiebeveiligingsoverleg tussen de directie en de Security Officer.

7 Ondersteuning

7.1 Middelen

De directie stelt de middelen beschikbaar die benodigd zijn voor het inrichten, implementeren, onderhouden en continu verbeteren van het managementsysteem voor informatiebeveiliging.

7.2 Competentie

De Security Officer is bewezen competent om het informatiebeveiligingsbeleid namens de directie operationeel te implementeren. Het gedocumenteerde bewijs betreft de implementatie en third party mededeling NEN7510:2017
De externe audito moet ingeschreven staan in het register van Norea.

7.3 Bewustzijn

Het is van groot belang dat het informatiebeveiligingsbeleid en de hieruit volgende principes en richtlijnen bekend zijn bij alle betrokkenen binnen de Organisatie. De Security Officer is verantwoordelijk voor de communicatie van het beleid. Het bevorderen van het beveiligingsbewustzijn bij management en medewerkers vormt een belangrijk aandachtspunt bij deze communicatie. Eventuele corrigerende maatregelen met betrekking tot personeel dat zich niet conformeert aan het informatiebeveiligingsbeleid zijn beschreven in het document 'Beheersmaatregelen en verklaring van toepasselijkheid'. Jaarlijks krijgen alle medewerkers een bewustzijns training. In de procedure veilig personeel is beschreven welke maatregelen worden genomen in het geval van non-compliance door medewerkers.

7.4 Communicatie

De Organisatie publiceert het informatiebeveiligingsbeleid met externe stakeholders door publicatie op de website www.james-software.nl direct nadat dit is vastgesteld door de directie. De volledige documentatie van de opzet van de norm NEN7510 zal eveneens direct ter beschikking worden gesteld aan het personeel van de Organisatie en worden behandeld in een bijeenkomst met het voltallige personeel. De Security Officer is verantwoordelijk voor de communicatie.

7.5 Gedocumenteerde informatie

7.5.1. Algemeen

De documentatie bestaat uit dit document en de volgende documenten:

- Beheersmaatregelen en verklaring van toepasselijkheid
- Inventarisatie en classificatie van bedrijfsmiddelen
- Aanvaardbaar gebruik bedrijfsmiddelen en informatiebeveiligingsincidenten
- Risico-analyse
- Planning verbeterpunten en controles
- Directiebesluiten
- Bewijsdocumentatie uitvoering planning
- Evaluatie en verbeterplan

- Extern audit rapport

7.5.2 Creëren en actualiseren
De auteur van alle documenten (welke voorzien zijn van versienummers) is de Security Officer.

7.5.3 Beheer van gedocumenteerde informatie
De documentatie wordt bewaard in een digitale kluis in een mappenstructuur die alleen toegankelijk is voor de directie en de Security Officer. Op de documentatie is versiebeheer van toepassing. De directie en de Security Officer zijn bevoegd om wijzigingen aan te brengen in de documentatie. Oude versies van documenten worden bewaard in een aparte map van de digitale kluis.

8 Uitvoering
8.1 Operationele planning en beheersing
De Security Officer is verantwoordelijk voor het documenteren van (verbeter)planning, het documenteren van de uitvoering van de planning en deze documentatie ter beschikking van de directie te stellen. Het beheren van uitbestede processen is de verantwoordelijkheid van de Security Officer.

8.2 Risicobeoordeling van informatiebeveiliging
De Organisatie voert jaarlijks een risico-beoordeling uit en vaker indien de omstandigheden dit vereisen. De risico-beoordeling wordt gedocumenteerd door de Security Officer.

8.3 Informatiebeveiligingsrisico's behandelen
Zie punt 8.1 hierboven.

9 Evaluatie van prestaties
9.1 Monitoren, meten, analyseren en evalueren
De Security Officer is verantwoordelijk voor het leveren van de gedocumenteerde bewijsvoering van de implementatie van de verbeterpunten (behandeling van risico's). Daarnaast is de Security Officer verantwoordelijk voor het uitvoeren / initiëren van en de bewijsvoering met betrekking tot onder andere:

- Risico-analyse (jaarlijks of indien noodzakelijk vaker)
- Verbeterplanning (continu proces)
- Het uitvoeren van periodieke controles

De Security Officer is verantwoordelijk om de uitkomsten die uit bovenstaande periodieke controles naar voren komen eens per 3 maanden met de directie te evalueren / analyseren (indien noodzakelijk vaker) en de met de directie afgesproken verbeterplanning uit te voeren. De Security Officer is verantwoordelijk om controles te documenteren als bewijs van uitvoering.

9.2 Interne audit

De Organisatie heeft onvoldoende mankracht om naast de reeds geïmplementeerde maatregelen en de periodieke controles uit paragraaf 9.1 een interne audit uit te voeren. De In plaats hiervan laat de Organisatie iedere 3 jaar een externe audit uitvoeren door een Norea geaccrediteerde auditor. Daarnaast voert de Organisatie ieder jaar een risico-analyse uit.

9.3 Directiebeoordeling

Iedere 3 maanden beoordeeld de directie in het informatiebeveiligingsoverleg met de Security Officer de voortgang van de uitvoering van de verbeterplanning en periodieke controles en neemt indien nog corrigerende of aanvullende maatregelen teneinde de goede werking van het managementsysteem te bevorderen en de informatiebeveiligingsdoelstellingen te behalen.

10 Verbetering

10.1 Afwijkingen en corrigerende maatregelen

Zie paragraaf 9.3. Corrigerende maatregelen moeten passend zijn om de opgetreden afwijkingen te mitigeren. Na implementatie van de corrigerende maatregelen wordt gecontroleerd of deze doelstelling is bereikt.

10.2 Continu verbetering

Zie paragraaf 9.3