Informatiebeveiligingsbeleid

Inhoudsopgave

1 Goedkeuring informatiebeveiligingsbeleid en distributie (BH1)

De directie behoort een beleidsdocument voor informatiebeveiliging goed te keuren, te publiceren en kenbaar te maken aan alle werknemers en relevante externe partijen.

2 Inleiding

2.1 Toelichting

Dit document beschrijft het beleid van James Software B.V. ("Organisatie") met betrekking tot de beveiliging van informatie. De informatievoorziening is van essentieel belang voor de continuïteit van de bedrijfsvoering van de Organisatie en haar klanten. Zowel op papier als geautomatiseerd zijn wij en onze klanten bij ons dagelijks werk afhankelijk van de beschikbaarheid van betrouwbare informatie. Onze Organisatie en onze informatievoorziening wordt blootgesteld aan een groot aantal bedreigingen, al dan niet opzettelijk van aard. Deze bedreigingen maken het noodzakelijk om gerichte maatregelen te treffen om de risico's tot een aanvaardbaar niveau te reduceren. Het proces van informatiebeveiliging begint met het definiëren van een beleid op dit punt. Dit beleid is vastgelegd in het onderhavige document en door de directie vastgesteld.

2.2 Definitie van informatiebeveiliging

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 informatie en informatiesystemen.

Opgemerkt wordt dat informatiebeveiliging een *samenhangend stelsel* van maatregelen omvat. Dit betekent dat de verschillende maatregelen die tezamen de informatiebeveiliging vormen, niet los van elkaar worden getroffen, maar in onderlinge relatie met elkaar staan.

Het stelsel van beveiligingsmaatregelen heeft tot doel een *blijvend niveau van beveiliging* te realiseren. Door een zorgvuldige borging wordt bereikt dat het gewenste niveau van beveiliging ook op langere termijn wordt gehandhaafd.

Informatiebeveiliging is gericht op het realiseren van een *optimaal niveau van beveiliging.* Dit optimum wordt bereikt door een zorgvuldige afweging van kosten en baten.

2.3 Samenhang tussen informatiebeveiliging en privacybescherming

Privacybescherming richt zich op de zorgvuldige omgang met persoonsgegevens. Dit kunnen bijvoorbeeld gegevens van patiënten of van medewerkers zijn. Informatiebeveiliging richt zich op de beveiliging van vertrouwelijke gegevens, waaronder persoonsgegevens. De maatregelen die in het kader van informatiebeveiliging worden getroffen, leveren dus een bijdrage aan de bescherming van privacygevoelige gegevens. Binnen de Organisatie is de

Security Officer verantwoordelijk voor de coördinatie van alle activiteiten die betrekking hebben op informatiebeveiliging.

2.4 Samenhang tussen informatiebeveiliging en risicomanagement

Risicomanagement richt zich op het analyseren en beheersen van risico's waaraan de Organisatie en haar klanten bloot staan gesteld. Deze risico's kunnen op velerlei terreinen betrekking hebben, zoals financiële risico's en de beschikbaarheid en inzet van personeel. Informatiebeveiliging heeft betrekking op de risico's die samenhangen met de informatievoorziening en de omgang met vertrouwelijke informatie. De coördinatie van risicomanagement is de verantwoordelijkheid van de Security Officer van de Organisatie.

2.5 Doelstelling informatiebeveiligingsbeleid

Het opstellen van het informatiebeveiligingsbeleid heeft tot doel de doelstellingen en uitgangspunten met betrekking tot informatiebeveiliging binnen de Organisatie vast te stellen en vast te leggen. Hiermee vormt het beleid de leidraad voor alle betrokkenen bij informatiebeveiliging binnen de Organisatie. De directie acht de doelstellingen, uitgangspunten en uitvoering van het informatiebeveiligingsbeleid een kritische succesfactor voor de continuïteit van de Organisatie.

2.6 Doelstelling informatiebeveiliging

Zoals in de voorgaande definitie (2.2) is verwoord, richt informatiebeveiliging zich op de volgende drie aspecten van de informatievoorziening:

- *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.

Informatiebeveiliging heeft tot doel het optreden van bedreigingen die bovenstaande aspecten van de informatievoorziening kunnen schaden, te voorkomen en/of te beperken. Bedreigingen zijn er in vele vormen. Deze kunnen fysiek van aard zijn, zoals brand en wateroverlast of technisch, bijvoorbeeld in de vorm van storingen in programmatuur, apparatuur of de stroomvoorziening. Ook de mens vormt een bedreiging door onopzettelijk fouten en vergissingen te maken die de informatievoorziening verstoren of door opzettelijke kwaadaardige daden, zoals hacking, phishing, computervirussen, computerfraude, etc. De ervaring leert dat bedreigingen op dit terrein steeds vaker voorkomen en ook steeds geraffineerder van aard worden.

2.7 Werkingsgebied

Het informatiebeveiligingsbeleid is van toepassing op heel de Organisatie. Het informatiebeveiligingsbeleid is ook van toepassing op de gegevensuitwisseling van de Organisatie met andere organisaties. Het beleid richt zich op onze eigen medewerkers, tijdelijk personeel, vrijwilligers en op personeel dat door derden wordt ingezet om diensten te verlenen aan onze organisatie.

2.8 Verantwoordelijkheid informatiebeveiligingsbeleid

De directie is eindverantwoordelijk voor het informatie-beveiligingsbeleid en heeft dit beleid op vastgesteld door middel van dit document.

De Security Officer is verantwoordelijk voor het onderhoud van het informatiebeveiligings-beleid.

2.9 Communicatie van het informatiebeveiligingsbeleid

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.

2.10 Ondersteunende documentatie

Dit informatiebeveiligingsbeleid is binnen de organisatie verder uitgewerkt in de volgende documenten welke zijn opgeslagen in Dropbox:

- H3-v1.0 Risicoanalysemethode.docx
- H3-v1.0 bijlage Risicoanalyse productieomgeving Web-applicatie.docx
- H3-v1.0 bijlage Risicoanalyse technisch beheer en change management.docx
- H3-v1.0 bijlage Risicoanalyse omgang bedrijfsmiddelen.docx
- H7-v1.0 Beheer van bedrijfsmiddelen.docx
- H7-v1.0 bijlage Inventarisatie en classificatie van bedrijfsmiddelen.xlsx
- H8 -v1.0 Personeel en informatiebeveiliging.docx
- H8-v1.0 bijlage Richtlijnen aanvaardbaar gebruik bedrijfsmiddelen en informatiebeveiligingsincidenten.docx
- H9-v1.0 Fysieke beveiliging en beveiliging van de omgeving.docx
- H10-v1.0 Beheer van communicatie- en bedieningsprocessen.docx
- H11-v1.0 Toegangsbeveiliging.docx
- H12-v1.0 Verwerving ontwikkeling en onderhoud van informatiesystemen.docx
- H13-v1.0 Beheer van informatiebeveiligingsincidenten.docx
- H14-v1.0 Bedrijfscontinuïteitsbeheer.docx
- H15-v1.0 Naleving.docx

2.11 Inhoud informatiebeveiligingsbeleid

In hoofdstuk 2 zijn de uitgangspunten vastgelegd die worden gehanteerd bij de toepassing van informatiebeveiliging binnen de Organisatie. In hoofdstuk 3 wordt aandacht besteed aan het managementsysteem voor informatiebeveiliging. Hoofdstuk 4 beschrijft de Organisatie van informatiebeveiliging.

3 Uitgangspunten informatiebeveiliging

Bij de toepassing van informatiebeveiliging binnen de Organisatie worden de volgende uitgangspunten gehanteerd:

1. De Organisatie streeft ernaar aantoonbaar te voldoen aan de norm NEN7510, Informatiebeveiliging in de zorg.
2. De Organisatie voldoet aan alle, van toepassing zijnde, wet- en regelgeving. In dit verband worden genoemd:
- Wet bescherming persoonsgegevens (WBP)
- Besluit BSN in de zorg
3. Informatiebeveiliging is binnen de Organisatie zo ingericht dat de rechten van betrokkenen (patiënten van klanten van de Organisatie, medewerkers, bezoekers, leveranciers) die voortvloeien uit de Wet Bescherming Persoonsgegevens, worden gerespecteerd en kunnen worden geëffectueerd.
4. Beveiliging van informatie is een onderdeel van de integrale managementverantwoordelijkheid. Alle onderdelen van de Organisatie hebben hiertoe verantwoordelijkheden voor informatiebeveiliging toegewezen en vastgelegd.
5. Wanneer de Organisatie samenwerkingsverbanden aangaat met externe partijen, hetzij inhoudelijk, hetzij voor de ontwikkeling of het beheer van de informatievoorziening, wordt nadrukkelijk aandacht besteed aan informatiebeveiliging. Afspraken hierover worden schriftelijk vastgelegd en op de naleving hiervan wordt toegezien.
6. Bedrijfsmiddelen zijn volgens een gestructureerde methode geclassificeerd naar de aspecten beschikbaarheid, integriteit en vertrouwelijkheid.
7. Bij de aanname, tijdens het dienstverband en in geval van ontslag van medewerkers wordt nadrukkelijk aandacht besteed aan de betrouwbaarheid van medewerkers en aan de waarborging van de vertrouwelijkheid van informatie.
8. De Organisatie voert een actief beleid om het beveiligingsbewustzijn van management en medewerkers te stimuleren. Hiertoe voert de Security Officer periodiek bewustwordingscampagnes uit en biedt hij de onderdelen van de Organisatie hiervoor communicatiemiddelen aan.
9. De Organisatie beschikt over gedragsregels voor het gebruik van (algemene) informatievoorzieningen. Op de naleving van deze gedragsregels wordt toegezien.
10. Bij overtreding van de regelgeving voor informatiebeveiliging zal de directie disciplinaire maatregelen treffen.
11. De Organisatie heeft maatregelen getroffen voor de fysieke beveiliging van mensen en middelen, waaronder vertrouwelijke informatie en apparatuur waarop deze informatie is opgeslagen.
12. De Organisatie heeft maatregelen getroffen voor de beveiliging en het beheer van de operationele informatie- en communicatievoorzieningen. Maatregelen tegen allerlei vormen van kwaadaardige programmatuur (computervirussen, spam, spyware, phishing, etc.) vormen hierin een belangrijk onderdeel.
13. De Organisatie heeft maatregelen getroffen waardoor is gewaarborgd dat alleen geautoriseerde medewerkers gebruik kunnen maken van de informatie- en communicatievoorzieningen.
14. Bij de ontwikkeling en aanschaf van informatiesystemen besteden opdrachtgevers, projectleiders, ontwikkelaars en beheerders in alle fasen van het aanschaf- of ontwikkelingsproces nadrukkelijk aandacht aan informatiebeveiliging en dragen zij zorg voor de realisatie van de gestelde beveiligingseisen.

15. De Organisatie heeft adequate maatregelen getroffen, waardoor de beschikbaarheid van de bedrijfsprocessen en de hierbij gebruikte informatie(systemen) is gewaarborgd. Het beheren van een continuïteitsplan, het inrichten van een crisisorganisatie en het oefenen van de getroffen maatregelen vormen hiervan een onderdeel.
16. Als onderdeel van het managementsysteem voor informatiebeveiliging wordt binnen de Organisatie door interne en externe partijen toegezien op de naleving van het informatiebeveiligingsbeleid.
17. De Organisatie beschikt over middelen voor het melden en afhandelen van beveiligingsincidenten. De evaluatie van de afhandeling van beveiligingsincidenten wordt benut voor de verbetering van informatiebeveiliging.

4 Herbeoordeling informatiebeveiligingsbeleid (BH2)

Het informatiebeveiligingsbeleid behoort met geplande tussenpozen, na het optreden van een omvangrijk informatiebeveiligingsincident of zodra zich belangrijke wijzigingen voordoen, te worden beoordeeld om te bewerkstelligen dat het geschikt, toereikend en doeltreffend blijft.

Het informatiebeveiligingsbeleid wordt iedere 2 jaar herbeoordeeld.

5 Managementsysteem voor informatiebeveiliging

5.1 Overzicht managementsysteem informatiebeveiliging

Het managementsysteem voor informatiebeveiliging omvat de volgende vijf stappen o.b.v. de Demmingcirkel: *beleidsvorming -> risico-analyse -> planvorming -> implementatie -> monitoring, evaluatie, controle (waarna de cirkel opnieuw begint met het 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

In de volgende paragrafen worden deze vijf stappen toegelicht.

5.2 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.

5.3 Risiconalyse

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.

Voor het uitvoeren van een risicoanalyse wordt de methode gehanteerd die is vastgelegd in het document "Risicoanalysemethode".

Over de uitkomsten van de analyse van de bestaande situatie voor informatiebeveiliging wordt gerapporteerd aan de directie.

5.4 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.

Het informatiebeveiligingsplan wordt vastgesteld door de directie.

5.5 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 medewerkers.

5.6 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.

5.7 Cyclisch proces

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. Een dergelijke beoordeling vindt minimaal éénmaal per drie jaar plaats en wordt geïnitieerd door de Security Officer.

6 Organisatie van de informatiebeveiliging

6.1 Directie (BH3)

De directie behoort informatiebeveiliging binnen de organisatie actief te ondersteunen door duidelijk richting te geven, betrokkenheid te tonen en expliciet verantwoordelijkheden voor informatiebeveiliging toe te kennen en te erkennen.

De directie heeft de volgende taken m.b.t. informatiebeveiliging:

- De directie formuleert informatiebeveiligingsdoelstellingen
- Het is de verantwoordelijkheid van de directie om het informatiebeveiligingsbeleid te formuleren, te beoordelen en goed te keuren
- De directie moet zorgen voor de middelen die nodig zijn voor informatiebeveiliging
- De directie moet plannen en programma's initiëren om het informatiebeveiligings-bewustzijn op een voldoende peil te krijgen en te houden
- De directie moet rollen en verantwoordelijkheden voor de informatiebeveiliging in toekennen
- De directie benoemt een Security Officer
- De directie controleert of het informatiebeveiligingsbeleid en de hieruit voorvloeidende richtlijnen en procedures worden nageleefd in de Organisatie. De Security Officer voorziet de directie van de juiste informatie om haar controlerende taak uit te kunnen oefenen.

6.2 Overleg informatiebeveiliging (BH4)

De portefeuillehouder directie en de Security Officer overleggen regelmatig bilateraal over informatiebeveiliging. In dit overleg wordt aandacht besteed aan (voortgangs)rapportages, voorstellen voor wijzigingen van het informatiebeleid, investeringsvoorstellen voor beveiligingsmaatregelen, etc. Dit overleg wordt ieder kwartaal gehouden en vaker indien hier aanleiding voor is.

6.3 Security Officer (BH5)

De Security Officer is de spin in het web met betrekking tot informatiebeveiliging binnen de Organisatie. 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
- 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 opstellen en coördineren van een verbeterplan m.b.t. informatiebeveiliging
- het coördineren van de implementatie van beveiligingsmaatregelen
- het centraal registreren van ICT-beveiligingsincidenten
- het analyseren en beoordelen van 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 rapporteert aan de directie.

6.4 Generieke rollen voor informatiebeveiliging (BH5)

Voor ieder informatiesysteem en gegevensverzameling worden de volgende rollen en de bijbehorende verantwoordelijkheden toegewezen.

Rol	Verantwoordelijkheden
Functioneel beheerder	Stelt de functionele specificaties op, stuurt het ontwikkel-, test en acceptatieproces aan en is verantwoordelijk voor het in productie nemen van nieuwe releases
Ontwikkelaar / applicatiebeheerder	Ontwikkelt het informatiesysteem, conform de (beveiligings)eisen die door de Security Officer zijn gesteld en doer applicatiebeheer.
Technisch beheerder	Exploitatie van de technische infrastructuur. Ziet toe op een juiste technische werking van de technische infrastructuur
Gebruiker	Toepassing van het informatie-systeem. Naleving van beveiligings-richtlijnen en -procedures

De verschillende betrokkenen maken onderling afspraken over de uitvoering van de (beveiligings)taken en leggen deze desgewenst vast in dienstverlenings-overeenkomsten (SLA's).

6.5 Goedkeuringsproces voor middelen voor de informatievoorziening (BH6)

De directie stelt voldoende middelen ter beschikking om de planning van de informatiebeveiliging te kunnen uitvoeren. De geringe omvang van de Organisatie maakt dat er geen formele goedkeuringsprocedures benodigd zijn.

6.6 Geheimhoudingsovereenkomst (BH7)

Eisen voor vertrouwelijkheid die een weerslag vormen van de behoefte van de organisatie aan beveiliging van informatie behoren in een geheimhoudingsovereenkomst te worden vastgesteld. Bij personeelsleden met een dienstbetrekking is geheimhouding onderdeel van de arbeidsovereenkomst. Bij overige personeelsleden en leveranciers wordt dit vastgelegd als onderdeel van de dienstverleningsovereenkomst of in een separate overeenkomst.

6.7 Contact met overheidsinstanties (BH8)

- De Organisatie heeft geprobeerd om contact te leggen met het Nationaal Cyber Security Centrum. Dit is afgewezen, de Organisatie werd verwezen naar commerciële dienstverleners.

- In het document "NEN7510, Werken met" van het NEN-instituut wordt aangegeven dat de Autoriteit persoonsgegevens geen contactpersonen aan individuele partijen toewijst.
- De politie onderhoudt ook geen contacten met individuele bedrijven als dit niet strikt noodzakelijk is.

6.8 Contact met speciale belangengroepen (BH9)

Informatiebeveiliging is een belangrijk kennisdomein voor de Organisatie. Kennis wordt ingewonnen via:

- de Security Officer van de managed hosting provider
- jaarlijkse "Threat reports" uitgegeven door onder andere Verizon
- blogs, zoals www.threatpost.com van beveilingsbedrijf Kaspersky
- nieuwsbrieven van beveiligingsbedrijf FOX-IT en het SANS instituut
- het Nationaal Cyber Security Centrum

6.9 Onafhankelijke beoordeling van informatiebeveiliging (BH10)

De informatiebeveiliging wordt periodiek door een externe auditor, die is aangesloten bij Norea, beoordeeld. Dit gebeurt 1 maal in de 3 jaar.

6.10 Samenwerking met externe partijen (BH11, 12, 13)

De samenwerking met externe partijen kan gevolgen hebben voor de informatiebeveiliging van de Organisatie. Voor de samenwerking met externe partijen ten behoeve van ontwikkeling en hosting van de Web-applicatie dient een risicoanalyse uitgevoerd te worden conform de risicoanalysemethode van de Organisatie. Er zal geen aparte risicoanalyse uitgevoerd worden maar deze zal worden meegenomen in de risicoanalyse van de bedrijfsmiddelen van de Organisatie. Noodzakelijke beheersmaatregelen ter bescherming van bedrijfsmiddelen dienen geïmplementeerd te worden. In de overeenkomst en begeleidende documentatie (zoals SLA's, geheimhoudingsovereenkomsten) met extere partijen dient aandacht te worden besteed aan informatiebeveiliging en worden procedures nader uitgewerkt

6.11 Monitoring, controle en rapportage over informatiebeveiliging

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, c.q. zo snel mogelijk te herstellen.

Met betrekking tot informatiebeveiliging worden de volgende controlevormen onderscheiden:

- operationele controle op de naleving van het informatiebeveiligingsbeleid en de hieruit voortvloeiende richtlijnen en maatregelen
- controle op de voortgang van de implementatie en borging van het informatiebeveiligingsbeleid en de hieruit voortvloeiende richtlijnen en maatregelen
- onafhankelijke controle.

Operationele controle op de naleving van beleid en richtlijnen wordt verricht door Security Officer. De Security Officer rapporteert iedere maand de aan de directie.

Voortgangscontrole en -rapportage m.b.t. de voortgang van de implementatie van informatiebeveiliging binnen de Organisatie. De Security Officer rapporteert iedere maand de voortgang aan de directie.

Onafhankelijke controle met betrekking tot informatiebeveiliging wordt uitgevoerd door een onafhankelijke auditor.