Informatiebeveiligingsbeleid Stichting Zomerkind 2018

1 Inleiding

1.1 Toelichting

Dit document beschrijft het beleid van Stichting Zomerkind, hierna ook: de organisatie, met betrekking tot de beveiliging van informatie. De informatievoorziening is van essentieel belang voor de continuïteit van de bedrijfsvoering van Stichting Zomerkind. Zowel op papier als geautomatiseerd zijn wij 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.

1.2 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 blijft 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.

1.3 Samenhang tussen informatiebeveiliging en gegevensbescherming

Bescherming van persoonsgegevens richt zich op de zorgvuldige omgang met persoonsgegevens. Dit kunnen bijvoorbeeld gegevens van (werknemers van) klanten 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 (bijzondere) persoonsgegevens. Binnen de Stichting Zomerkind is de IT beheerder verantwoordelijk voor de coördinatie van alle activiteiten die betrekking hebben op informatiebeveiliging. De Functionaris voor de Gegevensbescherming houdt toezicht op de regels en maatregelen voor de AVG. Deze wettelijke taak staat beschreven in artikel 37 t/m 39 van de AVG.

1.4 Samenhang tussen informatiebeveiliging en risicomanagement

Risicomanagement richt zich op het analyseren en beheersen van organisatie-brede risico's waaraan Stichting Zomerkind staat blootgesteld. 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.

1.5 Samenhang tussen informatiebeveiliging en kwaliteitszorg

De Stichting Zomerkind streeft naar een hoge kwaliteit in de uitvoering van dienstverlening en de hiervoor benodigde ondersteunende bedrijfsprocessen. De organisatie werkt aan continue kwaliteitsverbetering. Ook voor de informatievoorziening en de informatiebeveiliging is dit van toepassing. De activiteiten voor kwaliteitszorg worden gecoördineerd door kwaliteitsmedewerker. De IT-beheerder richt zich op informatiebeveiliging en stemt zijn activiteiten af met de kwaliteitsmedewerker.

1.6 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.

1.7 Doelstelling informatiebeveiliging

Zoals in de voorgaande definitie 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.

1.8 Werkingsgebied

Het informatiebeveiligingsbeleid is van toepassing op het gehele Stichting Zomerkind. Het informatiebeveiligingsbeleid is ook van toepassing op de gegevensuitwisseling van de Stichting Zomerkind met andere organisaties. Het beleid richt zich op alle activiteiten die door of namens de organisatie worden uitgevoerd.

1.9 Verantwoordelijkheid informatiebeveiligingsbeleid

De raad van bestuur is eindverantwoordelijk voor het informatiebeveiligingsbeleid.

1.10 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 Stichting Zomerkind. Het informatiebeleid is openbaar voor alle medewerkers van de organisatie beschikbaar op het intranet.

1.11 Ondersteunende documentatie

Dit informatiebeveiligingsbeleid is binnen de organisatie is verder uitgewerkt in de volgende documenten: Privacystatement, Privacyreglement, Reglement Cameratoezicht, Reglement Datalekken, Verwerkingsovereenkomsten, Register van Verwerkingen, Sociaal mediabeleid, Bewaar- en autorisatiebeleid en een samenvattend Privacybeleidsplan.
Deze documentatie is op het intranet (Google Drive) van de Stichting Zomerkind te vinden onder AVG.

1.12 Inhoud informatiebeveiligingsbeleid

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

2 Uitgangspunten informatiebeveiliging

Bij de toepassing van informatiebeveiliging binnen de Stichting Zomerkind worden de volgende uitgangspunten gehanteerd:

1. De organisatie streeft ernaar aantoonbaar te voldoen aan de voor de organisatie relevante NEN 27001 normen.
2. De organisatie voldoet aan alle, van toepassing zijnde, wet- en regelgeving. In dit verband worden genoemd:
    - Algemene verordening Gegevensbescherming
    - Archiefwet
    - Auteurswet
    -
    - Grondwet (vooral artikel 10 en 13)
    - Telecommunicatiewet
    - Wet Computercriminaliteit (meest recente versie)

- Wet langdurige zorg (Wlz);
- Jeugdwet;
- Wet maatschappelijke ondersteuning 2015 (WMO);
- Wet op de geneeskundige behandelovereenkomst (WGBO).

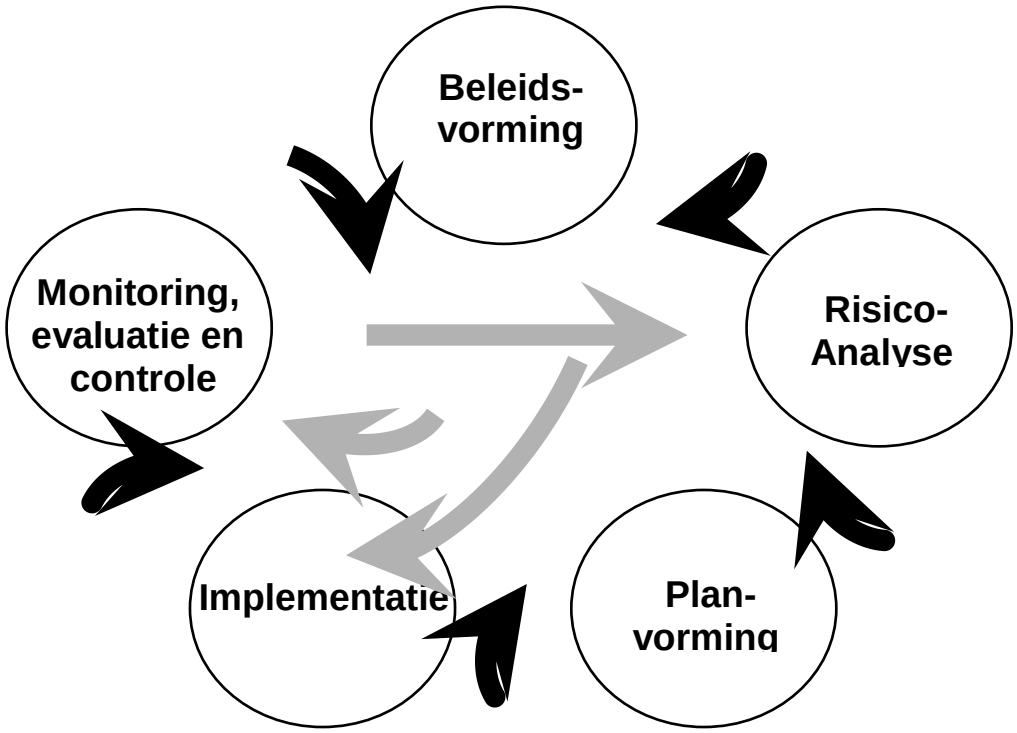
3. Informatiebeveiliging is binnen de organisatie zo ingericht dat de rechten van betrokkenen (cliënten, medewerkers, bezoekers, leveranciers) die voortvloeien uit de Algemene verordening gegevensbescherming worden gerespecteerd en kunnen worden geëffectueerd.
4. Beveiliging van informatie is een onderdeel van de integrale bestuursverantwoordelijkheid. Bij alle activiteiten van de Stichting Zomerkind zijn hiertoe verantwoordelijkheden voor informatiebeveiliging toegewezen en vastgelegd. De in hoofdstuk 4 beschreven organisatie van informatiebeveiliging vormt hierbij de leidraad.
5. Wanneer Stichting Zomerkind 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 door interne of externe auditors.
6. De verantwoordelijke van een activiteit van de Stichting Zomerkind draagt er zorg voor dat de bedrijfsprocessen, informatiesystemen en gegevensverzamelingen volgens een gestructureerde methode zijn geclassificeerd naar de drie aspecten van informatiebeveiliging, te weten beschikbaarheid, integriteit en vertrouwelijkheid.
7. Bij de aanname, tijdens het dienstverband en in geval van ontslag van medewerkers besteedt de leidinggevende nadrukkelijk aandacht aan de betrouwbaarheid van medewerkers en aan de waarborging van de vertrouwelijkheid van informatie.
8. De Stichting Zomerkind voert een actief beleid om het beveiligingsbewustzijn medewerkers en leidinggevende te stimuleren. Hiertoe voert het bestuur, in samenwerking met de teamleider, periodiek bewustwordingscampagnes uit..
9. Bij overtreding van de regelgeving voor informatiebeveiliging en/of relevante wettelijke bepalingen kan de Raad van Bestuur een sanctie opleggen.
10. Stichting Zomerkind heeft maatregelen getroffen voor de fysieke beveiliging van mensen en middelen, waaronder vertrouwelijke informatie en apparatuur waarop deze informatie is opgeslagen.
11. Stichting Zomerkind 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, ransomware, etc.) vormen hiervan een belangrijk onderdeel;
12. Stichting Zomerkind heeft maatregelen getroffen voor Identity & Accessmanagement waardoor is gewaarborgd dat alleen geautoriseerde medewerkers gebruik kunnen maken van de informatie- en communicatievoorzieningen.
13. Bij de ontwikkeling en aanschaf van informatiesystemen besteden opdrachtgevers, projectleiders, ontwikkelaars en beheerders in alle fasen van het aanschaf- of ontwikkelingsproces nadrukkelijk aandacht aan architectuur, informatiebeveiliging en change management en dragen zij zorg voor de realisatie van de gestelde beveiligingseisen.
14. Stichting Zomerkind 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.
15. Als onderdeel van het managementsysteem voor informatiebeveiliging wordt binnen de Stichting Zomerkind door interne en externe partijen toegezien op de naleving van het informatiebeveiligingsbeleid.
16. De Stichting Zomerkind beschikt over middelen voor het melden en afhandelen van beveiligingsincidenten, waaronder datalekken. De evaluatie van de afhandeling van beveiligingsincidenten en datalekken wordt benut voor de verbetering van informatiebeveiliging[1].

3 Managementsysteem voor informatiebeveiliging

3.1 Overzicht managementsysteem informatiebeveiliging

Het managementsysteem voor informatiebeveiliging omvat de volgende vijf stappen.

[1] Voor het melden van datalekken is een specifiek emailadres aangemaakt: privacy@zomerkind.nl.



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.

3.2 Beleidsvorming

Zoals ook aangegeven in paragraaf 1.1, start het managementsysteem voor informatiebeveiliging met het opstellen van het informatiebeveiligingsbeleid. In dit beleid worden de doelstellingen en uitgangspunten voor informatiebeveiliging van de Stichting Zomerkind vastgelegd. De Raad van Bestuur stelt het beleid vast. Hiermee vormt het beleid de leidraad voor de overige stappen van het managementsysteem.

3.3 Risiconalyse

De tweede stap van het managementsysteem voor informatiebeveiliging bestaat uit risicoanalyse. Deze analyse wordt zowel organisatie-breed als per aanleiding uitgevoerd. 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.

3.4 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 vastgelegd. Het verbeterplan wordt in geval van de algemene analyse vastgesteld door de Raad van Bestuur en bij de specifieke analyse aan de opdrachtgever van de risicoanalyse.

3.5 Implementatie

Aan de hand van het verbeterplan wordt de implementatie van de aanvullende beveiligingsmaatregelen ter hand genomen. De genomen maatregelen worden opgenomen in het informatiebeveiligingsplan (IBP).

3.6 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 Stichting Zomerkind. 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.

De organisatie van deze controle en de afspraken voor de bijbehorende rapportage wordt in hoofdstuk 4 nader uitgewerkt.

3.7 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. Dit wordt in de figuur in paragraaf 3.1 aangegeven door de grijze gestippelde lijnen. Ook is het mogelijk dat nieuwe ontwikkelingen, zoals de introductie van nieuwe bedrijfsprocessen of informatiesystemen aanleiding geven om het informatiebeveiligingsbeleid te heroverwegen. Hiertoe wordt jaarlijks een review van het functioneren van het managementsysteem voor informatiebeveiliging uitgevoerd. Het informatiebeveiligingsbeleid wordt minimaal één maal per drie jaar opnieuw beoordeeld. De managementreview en de beoordeling van het informatiebeveiligingsbeleid worden geïnitieerd door de IT-beheerder.

4 Governance van informatiebeveiliging

4.1 Toelichting

In dit hoofdstuk wordt de governance van informatiebeveiliging binnen de Stichting Zomerkind beschreven. Het is van groot belang dat de verantwoordelijkheden, taken en bevoegdheden met betrekking tot informatiebeveiliging op een eenduidige wijze zijn toegewezen. Deze toewijzing heeft tot doel te voorkomen dat zaken dubbel worden uitgevoerd of dat de uitvoering van beveiligingstaken achterwege blijft. Bovendien levert de toewijzing van taken en verantwoordelijkheden de mogelijkheid om decharge te verlenen voor de uitgevoerde werkzaamheden.

De organisatie van informatiebeveiliging wordt beschreven volgens de volgende invalshoeken:

- het niveau van de beveiligingstaken, waarbij onderscheid wordt gemaakt naar strategische, tactische en operationele informatiebeveiliging
- generieke rollen voor informatiebeveiliging, waarbij de rollen van eigenaar, functioneel beheerder, applicatiebeheerder, technisch beheerder en gebruiker worden onderscheiden
- rollen en functies voor informatiebeveiliging binnen de Stichting Zomerkind.

Tenslotte wordt in dit hoofdstuk ook aandacht besteed aan de overlegvormen die in het kader van informatiebeveiliging van belang zijn en aan de manier waarop controle en rapportage is vormgegeven.

4.2 Strategisch, tactisch en operationeel niveau

In het onderstaande overzicht wordt een indeling van activiteiten met betrekking tot informatiebeveiliging gepresenteerd, waarbij het niveau van de activiteiten als onderscheidend criterium is gehanteerd.

Niveau	Activiteit	Verantwoordelijke	Documentatie	Controle
Strategisch	Beleidsvorming	Raad van Bestuur	Informatiebeveiligingsbeleid Informatie- en security architectuur (ingebed in Enterprise architectuur) Instellingsbrede richtlijnen	Externe auditor Functionaris voor de Gegevens-bescherming
Tactisch	Planning	RvB ism teamleider	Verbeterplan Richtlijnen per eenheid	IT-beheerder Externe auditor
Operationeel	Uitvoering	Medewerkers	Operationele procedures per eenheid	Teamleider Externe auditor

Op strategisch niveau vindt de beleidsvorming met betrekking tot informatiebeveiliging plaats. De Raad van Bestuur is verantwoordelijk voor deze beleidsvorming en wordt hierin ondersteund door de IT-beheerder.

De planning van de activiteiten en uitvoering van activiteiten met betrekking tot informatiebeveiliging vormt het tactische en operationele niveau. Deze activiteit valt onder de verantwoordelijkheid van de teamleider. De teamleider wordt hierin ondersteund door de IT-beheerder. Het verbeterplan is het meet- en stuurinstrument dat bij deze planning wordt ingezet.

Ten behoeve van het structureren van de uitvoering van taken met betrekking tot informatiebeveiliging zijn procedures opgesteld.

4.3 Generieke rollen voor informatiebeveiliging

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

Rol	Verantwoordelijkheden
Verantwoordelijke	Beslissingsrecht voor het informatiesysteem, c.q. de gegevensverzameling Bepalen van het doel en de middelen van de verwerking. Bepalen van de beveiligingseisen
Functioneel beheerder/ applicatiebeheerder	Ondersteunen van de verantwoordelijke bij het bepalen van de beveiligingseisen Ondersteunen van de gebruiker, onder andere door voorlichting
Ontwerper/ architect	Stelt kaders voor het ontwerp op Ontwerpt en beheert de architectuur voor het informatiesysteem. Toetst ontwerp aan (enterprise) architectuurkaders. De security architectuur vormt hiervan een onderdeel.
Ontwikkelaar	Ontwikkelt het informatiesysteem, c.q. de gegevensverzameling, conform de (beveiligings)eisen die door de verantwoordelijke zijn gesteld. Denkt actief mee over de realisatie en de beveiliging van het informatiesysteem, c.q. de gegevensverzameling.
Technisch beheerder	Acceptatie van het informatiesysteem voor beheer en exploitatie conform de hieraan gestelde (beveiligings)eisen. Operationele instandhouding van het informatiesysteem en de hiervoor benodigde infrastructuur.
Gebruiker	Toepassing van het informatiesysteem, c.q. de gegevensverzameling Naleving van beveiligingsrichtlijnen en -procedures

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

4.4 Rollen en functies voor informatiebeveiliging

Toelichting
Veel onderdelen binnen onze organisatie zijn bij informatiebeveiliging betrokken. In dit informatiebeveiligingsbeleid worden de verantwoordelijkheden van de volgende functies en rollen beschreven:
- Raad van Bestuur
- Stuurgroep informatiebeveiliging
- Functionaris voor de gegevensverwerking/ Privacyfunctionaris
- Kwaliteitsmedewerker Stichting Zomerkind
- Ouderraad
- Audit/ Interne Controle

Raad van Bestuur
De Raad van Bestuur is eindverantwoordelijk voor alle activiteiten binnen de Stichting Zomerkind en dus ook voor informatiebeveiliging. Binnen de Raad van Bestuur is voor informatiebeveiliging een portefeuillehouder aangewezen. De verantwoordelijkheid voor informatiebeveiliging omvat:
- het vaststellen van de Stichting Zomerkind -brede informatiebeveiligingsbeleid en daaruit voortvloeiende Stichting Zomerkind-brede richtlijnen
- het toezien op de naleving van het informatiebeveiligingsbeleid door de organisatieonderdelen
- het laten evalueren van de toepassing en werking van het informatiebeveiligingsbeleid op basis van rapportages over informatiebeveiliging.

De Raad van bestuur van de Stichting Zomerkind is verantwoordelijk voor het de Stichting Zomerkind-brede beleid met betrekking tot de beheersing van risico's. Hiertoe initieert de Raad van Bestuurs periodiek de uitvoering van een de Stichting Zomerkind-brede risicoanalyse. Risico's met betrekking de informatievoorziening vormen een deelverzameling van de totale risico's van de Stichting Zomerkind. De Raad van Bestuur en de IT-beheerder stemmen hun werkzaamheden periodiek af om tot een effectieve beheersing van risico's te komen.

Stuurgroep informatiebeveiliging
De activiteiten met betrekking tot informatiebeveiliging worden binnen de Stichting Zomerkind bewaakt door de Stuurgroep Informatiebeveiliging. Deze stuurgroep is dus verantwoordelijk voor de ondersteuning en bewaking van de realisatie en evaluatie van het informatiebeveiligingsbeleid en de bijbehorende Stichting Zomerkind-brede richtlijnen.

De samenstelling van de Stuurgroep Informatiebeveiliging is als volgt:
- Portefeuillehouder informatiebeveiliging Raad van Bestuur (voorzitter)
- IT-beheerder (secretaris)
- De teamleider &(incidenteel) de kwaliteitsmedewerker
- De Functionaris gegevensbescherming.

De IT-beheerder
De IT-beheerder is de spin in het web met betrekking tot informatiebeveiliging binnen de Stichting Zomerkind. Op hoofdlijnen omvat deze beschrijving de volgende verantwoordelijkheden:
- beleidsvorming, het beheren van de Stichting Zomerkind-brede informatiebeveiligingsbeleid en hieruit voortvloeiende Stichting Zomerkind-brede richtlijnen en procedures
- monitoring, controle en registratie, het bewaken van het niveau van informatiebeveiliging binnen de Stichting Zomerkind
- signaleren van tekortkomingen in de naleving van het informatiebeveiligingsbeleid en het geven van aanwijzingen voor aanvullende maatregelen aan het lijnmanagement
- communicatie en voorlichting, het coördineren van de implementatie van het gewenste niveau van informatiebeveiliging en het stimuleren van het beveiligingsbewustzijn bij management, medewerkers en andere betrokkenen
- evaluatie en advies, het adviseren van de Raad van Bestuur en andere leidinggevenden over informatiebeveiliging en het rapporteren over de status van informatiebeveiliging binnen Stichting Zomerkind.

De IT-beheerder rapporteert functioneel direct aan de portefeuillehouder binnen de Raad van Bestuur.

Lijnmanagement
De teamleider is verantwoordelijk voor de inrichting en uitvoering van de primaire en secundaire bedrijfsprocessen. De verantwoordelijkheid voor de bedrijfsprocessen omvat ook de beveiliging van de informatie en de ICT-infrastructuur waarvan het organisatieonderdeel eventueel zelf eigenaar is. Het lijnmanagement wordt hierbij ondersteund door de IT-beheerder.

De verantwoordelijkheid van het lijnmanagement omvat onder andere de volgende taken:
- zich ervan vergewissen dat de uitvoering van de bedrijfsprocessen geschiedt conform de wet- en regelgeving en het vigerende informatiebeveiligingsbeleid
- uitstralen van een positieve en actieve houding ten aanzien van informatiebeveiliging
- fungeren als voorbeeld met betrekking tot het gewenste gedrag
- toezicht houden op de naleving van informatiebeveiligingsmaatregelen
- medewerking verlenen aan verbeteracties
- autoriseren van medewerkers voor bevoegdheden tot informatie(systemen)
- informatiebeveiliging behandelen in werkoverleg, beoordelingen, etc.
- afhandelen van vertrouwelijke Informatiebeveiligingsincidenten
- verantwoording afleggen over de naleving van het informatiebeveiligingsbeleid in periodieke rapportages.

Functionaris voor de gegevensbescherming
De Functionaris voor de gegevensbescherming is verantwoordelijk voor het toezicht op de naleving van de Algemene verordening gegevensbescherming binnen de Stichting Zomerkind. Deze functionaris doet hiertoe aanbevelingen voor een betere bescherming van verwerkingen van persoonsgegevens. De IT-beheerder en de Functionaris voor de gegevensbescherming stemmen hun activiteiten af om een goede taakverdeling met betrekking tot informatiebeveiliging en bescherming van persoonsgegevens binnen de Stichting Zomerkind te waarborgen.

Portefeuillehouder Personeelszaken
De portefeuillehouder Personeelszaken (RvB) is verantwoordelijk voor het beheer van het personeelsbeleid van de Stichting Zomerkind. De uitvoering hiervan vindt gedeeltelijk centraal en gedeeltelijk decentraal plaats. Er is een relatie tussen personeelsbeleid en informatiebeveiliging, onder andere daar waar het de selectie en het ontslag van personeel betreft. Dit dient op een zorgvuldige manier te geschieden met de waarborging van een goede informatiebeveiliging. Hiertoe bewaakt de portefeuillehouder Personeelszaken, samen met de [CISO / ISO], de samenhang tussen personeelsbeleid en informatiebeveiliging.

Kwaliteitscoördinator Stichting Zomerkind
Er zijn relaties tussen kwaliteitszorg en informatiebeveiliging. Beide onderwerpen richten zich namelijk op bepaalde aspecten van de bedrijfsvoering. Kwaliteitszorg richt zich op een continue verbetering van de bedrijfsprocessen teneinde de gewenste kwaliteit te kunnen leveren. Gewenste kwaliteit wordt bepaald door het management, de medewerkers, maar vooral ook door de klanten van de organisatie en de maatschappelijke omgeving waar de organisatie zich in begeeft. Informatiebeveiliging richt zich op de beschikbaarheid, integriteit en de vertrouwelijkheid van de informatievoorziening. Hiermee kan informatiebeveiliging een bijdrage leveren aan de kwaliteit van de bedrijfsvoering. De Kwaliteitscoördinator en de IT-beheerder stemmen hun activiteiten regelmatig af teneinde beide aandachtsgebieden optimaal tot hun recht te laten komen en dubbel werk te voorkomen.

Cliëntenraad (CR)
De CR is de spreekbuis van de cliënten. Via de CR kunnen de medewerkers invloed uitoefenen op het beleid binnen de Stichting Zomerkind. Hiertoe heeft de CR diverse rechten, waaronder adviesrecht en voordrachtsrecht. Enerzijds wordt de CR geïnformeerd over de hoofdlijnen van beleid en de daaruit voortvloeiende richtlijnen en maatregelen met betrekking tot informatiebeveiliging. Daarnaast worden specifieke richtlijnen met betrekking tot informatiebeveiliging die een directe relatie hebben met het persoonlijke gedrag van het personeel ter beoordeling aan de CR voorgelegd.

Audit/ Interne controle
De stuurgroep informatiebeveiliging stemt zijn prioriteiten af met de auditor (bijvoorbeeld externe accountant).

In paragraaf 4.6 wordt de structuur met betrekking tot controle en rapportage over informatiebeveiliging nader uitgewerkt.

4.5 Overlegvormen voor informatiebeveiliging

Voor overleg, coördinatie en afstemming op het gebied van informatiebeveiliging worden de volgende overlegvormen onderscheiden:

- Bilateraal overleg portefeuillehouder Raad van Bestuur, IT-beheerder en teamleider;
- Overleg Stuurgroep Informatiebeveiliging;

De portefeuillehouder informatiebeveiliging (RvB), de teamleider en de IT-beheerder overleggen regelmatig over informatiebeveiliging. In dit overleg wordt aandacht besteed aan (voortgangs)-rapportages, voorstellen voor de Raad van Bestuur, voorstellen voor wijzigingen van het informatiebeleid, investeringsvoorstellen voor beveiligingsmaatregelen, etc. Dit overleg wordt minimaal twee maal per jaar gehouden.

De Stuurgroep Informatiebeveiliging bespreekt de realisatie en naleving van het informatiebeveiligingsbeleid en de bijbehorende Stichting Zomerkind-brede richtlijnen één maal per jaar.

4.6 Monitoring, controle en rapportage over informatiebeveiliging

Monitoring betreft het continu bewaken van het niveau van informatiebeveiliging binnen de Stichting Zomerkind. 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 de teamleider. De teamleider richt deze controle in naar eigen inzicht. Hierover vindt geen formele rapportage plaats.

Voortgangscontrole en -rapportage vinden periodiek plaats op verzoek van de portefeuillehouder informatiebeveiliging of de stuurgroep informatiebeveiliging.

Daarnaast hebben de Functionaris voor de gegevensbescherming en de IT-beheerder het recht en de mogelijkheid om gevraagd en ongevraagd interne audits uit te (laten) voeren met betrekking tot de naleving van wet/ en regelgeving voor privacybescherming en informatiebeveiliging.

Aldus vastgesteld in de vergadering van de Raad van Bestuur van de Stichting Zomerkind d.d. 11 december 2018 en goedgekeurd door de Raad van Toezicht van de Stichting Zomerkind in haar vergadering van 17 december 2018.

Mr. M.J. Toet
Voorzitter Raad van Bestuur Stichting Zomerkind.