Beleidsnotitie:	Informatiebeveiligingsbeleid	
Publicatiedatum:	oktober 2022	
Beoordelingscyclus:	3e kwartaal 2025	
Datum vaststelling directie overleg	5 december 2022	

INHOUDSOPGAVE

1 INLEIDING

1.1 Toelichting

Dit document beschrijft het beleid van SGL met betrekking tot de beveiliging van informatie. De informatievoorziening is van essentieel belang voor de continuïteit van de bedrijfsvoering van SGL.
Zowel op papier als geautomatiseerd zijn wij bij ons dagelijks werk sterk 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.

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 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.

Daarnaast zijn ook aspecten als authenticiteit en controleerbaarheid van belang. Authenticiteit betreft de mate van betrouwbaarheid van de originaliteit en herkomst van een document, een bericht, een gegeven of een ander object en controleerbaarheid heeft betrekking op de mate waarin de gegevens en de weergaven van de gegevens toetsbaar zijn.

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 m.n. cybercrime, hacking, phishing, computervirussen,

computerfraude, etc. De ervaring leert dat bedreigingen op dit terrein steeds vaker voorkomen en ook steeds geraffineerder van aard worden!

1.4 Samenhang tussen informatiebeveiliging en gegevensbescherming

Bescherming van persoonsgegevens richt zich op de zorgvuldige omgang met *persoons-gegevens*. Dit kunnen bijvoorbeeld gegevens van cliënten 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 SGL is de medewerker Informatiebeveiliging en Privacy verantwoordelijk voor de coördinatie van alle activiteiten die betrekking hebben op informatiebeveiliging.
Dit geldt eveneens voor de coördinatie van alle activiteiten die betrekking hebben op de 'Verantwoordingsplicht' naar de AVG .

De Functionaris Gegevensbescherming (hierna te noemen FG) houdt onafhankelijk toezicht op de regels en maatregelen voor bescherming van persoonsgegevens. Deze wettelijke taak staat beschreven in Afdeling 4 (art. 37 t/m art. 39) van de AVG[1].

1.5 Samenhang tussen informatiebeveiliging en risicomanagement

Risicomanagement richt zich op het analyseren en beheersen van instellingsbrede risico's waaraan de SGL 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 informatie-voorziening en de omgang met vertrouwelijke informatie.
Voor de coördinatie van risicomanagement beschikt SGL over een afdeling Beleidsondersteuning en Ontwikkeling.
De medewerker Informatiebeveiliging en Privacy richt zich op informatiebeveiliging en stemt zijn activiteiten af met de strategisch beleidsadviseur van afdeling Beleidsondersteuning en Ontwikkeling.

1.6 Samenhang tussen informatiebeveiliging en kwaliteitszorg

SGL streeft naar een hoge kwaliteit in de uitvoering van cliëntenzorg en de hiervoor benodigde ondersteunende bedrijfsprocessen. SGL als geheel en diverse onderdelen van onze instelling beschikt over kwaliteitscertificaten of –accreditaties. SGL werkt aan continue kwaliteits-verbetering. Ook voor de informatievoorziening en informatiebeveiliging is dit dus van toepassing.
Kwaliteitszorg wordt gecoördineerd door afdeling Beleidsondersteuning en Ontwikkeling van SGL. De medewerker Informatiebeveiliging en Privacy richt zich op informatiebeveiliging en stemt zijn activiteiten af met het afdeling Beleidsondersteuning en Ontwikkeling.

1.7 Doelstelling informatiebeveiligingsbeleid

Het opstellen van dit informatiebeveiligingsbeleid heeft tot doel de doelstellingen en uitgangspunten met betrekking tot informatiebeveiliging binnen SGL vast te stellen. Hiermee vormt het beleid de *leidraad voor alle betrokkenen bij informatiebeveiliging binnen SGL .*

Met het opstellen van het informatiebeveiligingsbeleid wordt invulling gegeven aan onderdelen van de hoofdstukken 4 tot en met 10 van NEN 7510-1 (ISMS) en hoofdstuk 5, Informatiebeveiligingsbeleid, en 6, Organiseren van informatiebeveiliging, van NEN 7510-2.

[1] Zorginstellingen zijn, als overheidsinstelling, *verplicht* een FG aan te stellen!

1.8 Werkingsgebied

Het informatiebeveiligingsbeleid is van toepassing op geheel SGL.
Het informatiebeveiligingsbeleid is ook van toepassing op de gegevensuitwisseling van SGL met andere organisaties conform NEN7512, 'Vertrouwensbasis voor gegevensuitwisseling'.
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.

1.9 Belanghebbenden

Belanghebbenden:
- Wet- en regelgevers;
- Externe toezichthouders: IGJ[2], AP[3], NZa;
- Cliënten/verwanten/wettelijke vertegenwoordigers;
- Medewerkers;
- Vrijwilligers;
- Ketenpartners (andere VVT-instellingen, ziekenhuizen, huisartsen etc.);
- Zorgverwijzers (b.v. VVT, ziekenhuizen, huisartsen);
- Zorgkantoren en gemeenten;
- Interne toezichthouder: Raad van Toezicht;
- Centrale Cliënten Raad; lokale cliëntenraden;
- Leveranciers;
- Banken/accountants.

1.10 Verantwoordelijkheid voor informatiebeveiligingsbeleid

De Raad van Bestuur is eindverantwoordelijk voor het informatiebeveiligingsbeleid en heeft dit beleid op [datum] vastgesteld.

De medewerker Informatiebeveiliging en Privacy is verantwoordelijk voor het onderhoud van het informatiebeveiligingsbeleid.

1.11 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 SGL. De medewerker Informatiebeveiliging en Privacy is verantwoordelijk voor de communicatie van het beleid en wordt hierin ondersteund door de afdeling Communicatie. Het bevorderen van het beveiligingsbewustzijn bij management en medewerkers vormt een belangrijk aandachtspunt bij deze communicatie.

1.12 Ondersteunende documentatie

Dit informatiebeveiligingsbeleid is binnen de SGL verder uitgewerkt in de volgende documenten:
- Integrale Risico Analyse (IRA2021);
- Implementatieplan 2022 (IMP2022);
- ISMS Beleid SGL;

[2] Inspectie Gezondheid en Jeugd
[3] Autoriteit Persoonsgegevens

2 UITGANGSPUNTEN INFORMATIEBEVEILIGING

Bij de toepassing van informatiebeveiliging binnen SGL worden de volgende algemene uitgangspunten gehanteerd:

1. SGL streeft ernaar aantoonbaar te voldoen aan de norm NEN 7510, Informatiebeveiliging in de zorg, en aan hieruit volgende normen, zoals de NEN7512: *Vertrouwensbasis voor gegevensuitwisseling*, en NEN 7513: *Logging*.
2. Certificering voor NEN7510-1:2017 is vooralsnog voor SGL niet aan de orde.
3. SGL voldoet aan alle, van toepassing zijnde, wet- en regelgeving. In dit verband worden genoemd:
    a. Algemene verordening gegevensbescherming (AVG);
    b. Archiefwet;
    c. Auteurswet;
    d. Grondwet (vooral artikel 10 en 13);
    e. Telecommunicatiewet;
    f. Wet beroepen in de individuele gezondheidszorg (Wet BIG);
    g. Wet cliëntenrechten bij elektronische verwerking van gegevens in de zorg;
    h. Wet Computercriminaliteit;
    i. Wet geneeskundige behandelingsovereenkomst (WGBO);
    j. De Wabvpz (Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg);
    k. Wet kwaliteit, klachten en geschillen zorg (Wkkgz);
    l. Wet toelating zorginstellingen.
    m. Wet Zorg en Dwang (WZD)
    n. Wet Langdurige Zorg (WLZ)
    o. Wet Maatschappelijke Ondersteuning (WMO)
    p. Wet Meldplicht Datalekken (WMD)
4. Informatiebeveiliging is binnen SGL zo ingericht dat de rechten van betrokkenen (cliënten, medewerkers, vrijwilligers, bezoekers, leveranciers) die voortvloeien uit de AVG worden gerespecteerd en kunnen worden geëffectueerd.
5. Beveiliging van informatie is een onderdeel van de integrale management-verantwoordelijkheid. Alle onderdelen van SGL hebben hiertoe verantwoordelijkheden voor informatiebeveiliging toegewezen en vastgelegd. De in hoofdstuk 3 beschreven organisatie van informatiebeveiliging vormt hierbij de leidraad.
6. Wanneer (onderdelen van) SGL samenwerkingsverbanden aangaan met externe partijen, hetzij inhoudelijk, hetzij voor de ontwikkeling of het beheer van de informatie-voorziening, wordt nadrukkelijk aandacht besteed aan informatiebeveiliging. Afspraken hierover worden schriftelijk vastgelegd en op de naleving hiervan wordt toegezien door interne en/of externe instanties [Medewerker Informatiebeveiliging en Privacy, auditteam en/of externe toezichthouders en auditors].
7. Bij het ontwerp en de realisatie van beveiligingsmaatregelen zoekt SGL actief samenwerking met en aansluiting bij externe betrokkenen.
8. De leiding van ieder organisatieonderdeel van SGL 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.
9. 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.
10. SGL voert een actief beleid om het beveiligingsbewustzijn van management en medewerkers te stimuleren. Hiertoe voert de medewerker Informatiebeveiliging en Privacy, in samenwerking met de afdeling Communicatie, periodiek bewustwordingscampagnes uit en biedt hij de onderdelen van SGL hiervoor communicatiemiddelen aan.
11. SGL beschikt over gedragsregels voor het gebruik van (algemene) informatievoorzieningen en voor social media. Het lijnmanagement ziet toe op de naleving van deze gedragsregels.

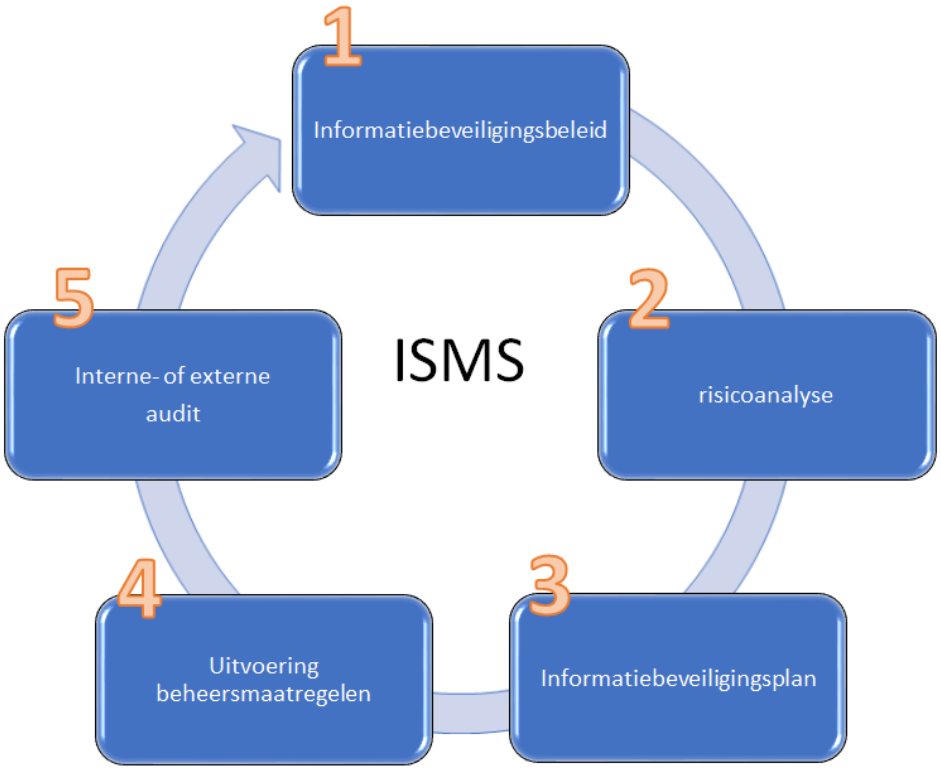
12. Bij overtreding van de regelgeving voor informatiebeveiliging en/of relevante wettelijke bepalingen kan de Raad van Bestuur een sanctie opleggen conform wat hierover met betrekking tot op non-actiefstelling, disciplinaire straffen, en beëindiging van het dienstverband is vastgelegd in de CAO.
13. Alle onderdelen van SGL hebben maatregelen getroffen voor de fysieke beveiliging van mensen en middelen, waaronder vertrouwelijke informatie en apparatuur waarop deze informatie is opgeslagen.
14. Alle onderdelen van SGL hebben 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.
15. SGL richt lokale en regionale systemen voor externe gegevensuitwisseling in als 'Goed Beheerde Zorgsystemen' om hiermee te kunnen aansluiten op de landelijke basisinfrastructuur voor gegevensuitwisseling in de zorg.
16. Alle onderdelen van SGL hebben maatregelen getroffen voor Identity & Accessmanagement[4] waardoor is gewaarborgd dat alleen *geautoriseerde* medewerkers gebruik kunnen maken van de informatie- en communicatievoorzieningen. Voor de omgang met cliëntgegevens vormt het privacyreglement hiervoor de leidraad.
17. 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.
18. Alle onderdelen van SGL hebben adequate maatregelen getroffen waardoor de beschikbaarheid van de bedrijfsprocessen en de hierbij gebruikte informatie(systemen) is gewaarborgd.
19. Als onderdeel van het managementsysteem voor informatiebeveiliging wordt binnen SGL door interne en externe partijen toegezien op de naleving van het informatiebeveiligings-beleid.
20. Alle onderdelen van SGL beschikken 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.

[4] het checken van authenticatie (ben je wie je zegt dat je bent?) en autorisatie (wat mag je wel en niet!) voordat er toegang wordt verleend tot systemen en informatie

3 MANAGEMENTSYSTEEM VOOR INFORMATIE-BEVEILIGING

3.1 Overzicht

Het managementsysteem voor informatiebeveiliging, Het 'Information Security Management System (hierna te noemen ISMS) omvat (globaal) de volgende vijf stappen.



De samenhang tussen deze vijf stappen en de Deming-cirkel (PDCA) is als volgt:

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

Bij de uitvoering van het managementsysteem voor informatiebeveiliging wordt zoveel mogelijk aangesloten bij andere managementsystemen binnen SGL .

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 (voorliggend document). In dit beleid worden de doelstellingen en uitgangspunten voor informatiebeveiliging van SGL vastgelegd. De Raad van Bestuur stelt het beleid vast. Hiermee vormt het beleid de leidraad voor de overige stappen van het managementsysteem.

3.3 Risicoanalyse

Deze analyse wordt zowel SGL-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.

Over de uitkomsten van de analyse van de bestaande situatie voor informatiebeveiliging wordt op centraal niveau gerapporteerd aan RvB/management. Bij de specifieke analyse wordt gerapporteerd aan de opdrachtgever van de risicoanalyse.

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 RvB/management 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. Dit betekent onder andere het opstellen van richtlijnen en procedures voor informatiebeveiliging, het invoeren van beveiligingshulpmiddelen en het voorlichten en opleiden van management en medewerkers.

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 informatie-beveiliging binnen SGL. 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 informatie-beveiligingsbeleid 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.

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 medewerker Informatiebeveiliging en Privacy.

4 INPASSING ISMS IN DE BEDRIJFSVOERING

Een belangrijk uitgangspunt voor het ISMS is, dat het zoveel als mogelijk wordt ingepast in de bestaande bedrijfsvoering van SGL.
Daarbij dient rekening gehouden te worden met:

- Eisen voor de bedrijfsvoering en wettelijke en contractuele eisen en verplichtingen met betrekking tot informatiebeveiliging;
- Eisen voor de bedrijfsvoering en wettelijke en contractuele eisen en verplichtingen met betrekking tot privacy;
- Afstemming op het strategische kader van de organisatie voor risicomanagement waarin het ISMS wordt vastgesteld en bijgehouden;
- Criteria aan de hand waarvan risico's worden beoordeeld;
- Goedkeuring door de directie.

In dit hoofdstuk wordt de organisatie rondom het ISMS beschreven.

De directiebeoordeling die aan het einde van ieder jaar wordt uitgevoerd (zie 4.1.5), kán aanleiding geven tot aanpassing van het ISMS-beleid, alsook het informatiebeveiligings- en privacybeleid.

4.1 Invulling ISMS organisatie

4.1.1 Adviesgroep Informatiebeveiliging & Privacy

Binnen SGL is, conform NEN7510-1:2020, een informatiebeveiligings-managementforum (IBMF) actief.

De volgende overwegingen gelden voor het IBMF:

- Uitgangspunt is dat de functie van het IBMF deel uitmaakt van de informatiegovernance structuur van SGL.
- Dit IBMF zal binnen SGL worden aangeduid met 'Adviesgroep Informatiebeveiliging & Privacy', hierna te noemen 'AIP';
- Uit praktische overwegingen heeft de AIP naast informatiebeveiliging óók privacy-bescherming als aandachtsveld; beiden zijn immers sterk aan elkaar verbonden;
- De AIP dient zo slagvaardig mogelijk te zijn en dus beperkt van omvang. Daarom is ervoor gekozen leden alléén vergaderingen te laten bijwonen indien een vertegenwoordiging van de discipline noodzakelijk wordt geacht;
- Binnen de AIP dient een zo volledig mogelijk bereik te zijn vertegenwoordigd van informatieveiligheid en -governance;
- De AIP vergadert in principe maandelijks over de voortgang van het ISMS en de risico's op het vlak van informatiebeveiliging en privacy.

4.1.2 Taken en rollen

- De RvB stelt formeel als hoofdverantwoordelijke het informatiebeveiligingsbeleid vast. De uitvoering van het beleid dient gecontroleerd te worden, zowel de RvB als de staf kunnen opdracht geven dit te (laten) controleren. Het management adviseert de RvB formeel over het vast te stellen beleid.
- De AIP heeft een permanente functie als commissie voor informatiebeveiliging en privacy. Strategische en tactische beslissingen over vormgeving van beleid worden binnen deze groep genomen en alleen indien nodig voorgelegd aan de RvB ter accordering.
- De medewerker Informatiebeveiliging en Privacy heeft binnen de AIP een voorzittersrol.

- De medewerker Informatiebeveiliging en Privacy geeft namens het RvB/management op dagelijkse basis invulling aan de sturende rol door besluitvorming voor te bereiden en toe te zien op de uitvoering ervan.
- De medewerker Informatiebeveiliging en Privacy bevordert en adviseert, gevraagd én ongevraagd, over informatiebeveiliging & privacy en rapporteert eens per jaar concernbreed aan het RvB/management overleg over de stand van zaken.
- De FG ziet toe op handhaving van de AVG. Informatiebeveiliging is daarbij een middel.
- Uitvoerende taken zijn zoveel mogelijk belegd bij lijnmanagers.

Doelgroep	**Relevantie voor IB en Privacybeleid**
Raad van Bestuur	Integrale verantwoordelijkheid en kaderstelling.
Management	Planvorming en implementatie binnen de kaders.
Alle (zorg)medewerkers/ vrijwilligers	Gedrag en naleving.
Lijnmanagement, teamleiders en coördinatoren	Sturen en monitoren op naleving van het beleid.
Adviesgroep informatie-beveiliging & privacy AIP	Algemene en dagelijkse coördinatie van informatiebeveiliging & privacybescherming; gevraagd of ongevraagd adviseren over de implementatie van het informatiebeveiligings- en privacybeleid.
Medewerker Informatie-beveiliging en Privacy	Voorzitter van AIP, sturende en adviserende rol over informatieveiligheid
Medewerker Informatie-beveiliging en Privacy	Sturende, adviserende en operationele rol voor Verantwoordingsplicht AVG
Functionaris Gegevens-bescherming	Onafhankelijke controle op handhaving AVG/toetsing van het privacybeleid/ afgevaardigde van de Autoriteit Persoonsgegevens.
Afdeling Beleidsondersteuning en Ontwikkeling	Onafhankelijke toetsing van het beleid, intern én extern.
Cliënten, verwanten, dienst-verleners, leveranciers en zorgpartners	Geïnformeerd over- en compliance aan het beleid.

Onderstaand is een RACI-tabel ingevuld voor de uit te voeren taken.
R = Responsible: diegene die verantwoordelijk is voor de uitvoering ;
A = Accountable: eindverantwoordelijk en bevoegd om goedkeuring te geven aan het resultaat;
C = Consulting: verlenen advies en geven van richting;
I = Informed: geïnformeerd over resultaat: éénrichting.

Rol > taak	**RvB**	**MT**	**Perso-neel**	**Lijn-mngmnt**	**AIP**	**SO**	**PO**	**FG**	**Beleids-ondersteuning**
Update beleid	A	C	I	C	R	R	R	C	I
Uitvoering beheersmaatregelen	A	R	I	R	C	C	C	C	I
Risicoanalyse	A	C	--	R	R	R	R	C	C
Directieverklaring	A	R	--	C	C	C	C	I	I
Auditering beleid	A	R	--	C	C	C	C	C	R
Besluitvorming risico's	A	R	--	C	C	C	C	C	I
Compliancy aan beleid	A	I	I	I	I	I	I	I	I

Rol > taak	RvB	MT	Perso-neel	Lijn-mngmnt	AIP	SO	PO	FG	Beleids-ondersteuning
Bevorderen bewustzijn	A	R	I	R	R	R	R	R	C

4.1.3 Auditering

Eenmaal per jaar wordt binnen SGL in het kader van de PDCA cyclus de effectiviteit van de gerealiseerde beheersmaatregelen gecontroleerd middels een audit op het gebied van informatiebeveiliging. Deze kan intern of extern worden uitgevoerd.
Deze audit maakt onderdeel uit van de interne kwaliteitscyclus.

4.1.4 Rapportage en frequentie

De PDCA-cyclus vereist regelmatige rapportage over de status en voortgang van de informatieveiligheid & privacy binnen SGL.

- Jaarlijks wordt de informatieveiligheid & privacy op onderdelen geauditeerd op initiatief van het RvB. Dit kan de vorm van een interne òf externe controle aannemen. Aanvullend dient een *directieverklaring* te worden opgesteld.
- Eenmaal per jaar wordt over de status van informatieveiligheid binnen SGL gerapporteerd aan het RvB/MT-overleg door FG.
- Eenmaal per 3 jaar wordt een risicoanalyse op het gebied van informatiebeveiliging en privacy uitgevoerd door een externe partij.
- Eenmaal per jaar wordt het informatiebeveiligingsplan herzien op initiatief van de AIP en voorgelegd aan het RvB/management.
- Eenmaal per drie (3) jaar wordt het informatiebeveiligingsbeleid herzien op initiatief van de AIP en vastgesteld door RvB.
- De voortgang van projecten op het gebied van informatiebeveiliging is vast onderdeel van de rapportage binnen het MT, minimaal éénmaal per jaar.

4.1.5 Directieverklaring

Het RvB/management van SGL beoordeelt met dezelfde frequentie als het (interne) kwaliteitsmanagementsysteem het ISMS om de geschiktheid, adequaatheid en doeltreffendheid te waarborgen.
De volgende aandachtspunten worden daarbij in overweging genomen:
Status en acties als gevolg van voorgaande directiebeoordelingen;

- Externe en interne onderwerpen, relevant voor het ISMS;
- Status van prestaties:
  - Auditresultaten;
  - Mate van voldoen aan doelstellingen;
- Resultaten van monitoren en meten.
- Feedback van belanghebbenden;
- Resultaten van risicobeoordeling;
- Kansen voor continue verbetering.

De directiebeoordeling zal schriftelijk worden vastgelegd en omvat:

- Besluitvorming t.a.v. noodzaak voor wijzigingen in het ISMS;
- Besluitvorming t.a.v. mogelijkheden voor continue verbetering.

BIJLAGE: AFKORTINGEN

AVG Algemene Verordening Gegevensbescherming: Nederlandse versie van de Europese privacywet, de GDPR.

AP Autoriteit Persoonsgegevens: toezichthouder op de AVG.

AIP Adviesgroep Informatiebeveiligng en Privacy: De 'SGL-versie' van de verplichte IBMF uit de NEN7510:2017.

FG Functionaris Gegevensbescherming: feitelijk de officiële functionaris binnen een organisatie die toezicht dient te houden op naleving van de AVG.

IBMF Informatiebeveiligingsmanagementforum; een forum voor aansturing vanuit het management voor beveiligingsvraagstukken (verplichting vanuit NEN7510).

ISMS Information Security Management System; een managementcyclus conform de principes van PDCA voor informatiebeveiliging.

NEN7510:2020 Laatste versie van de Nederlandse norm voor informatiebeveiliging in de zorg. Inmiddels verplicht voor zorginstellingen.

PDCA Plan-Do-Check-Act. Managementcyclus conform Deming.

UAVG Uitvoeringswet AVG. Nederlandse interpretatie van de Europese GDPR en aanvullend op de AVG.