dienstGezondheid & Jeugd zhz

Strategisch Informatiebeveiligingsbeleid Dienst Gezondheid & Jeugd

versie 1.0

Eveliene van der Vlies

22 oktober 2024

Classsificatie: Intern (Definitief)

Revisies

Versie	Datum	Veranderingen	Auteur
0.1	26-08-2024	Eerste opzet	Eveliene v.d. Vlies
0.2	24-09-2024	Tekstuele en inhoudelijke wijzigingen n.a.v. review Ben Hendrikx	Eveliene v.d. Vlies
0.3	3-10-2024	Tekstuele en inhoudelijke wijzigingen n.a.v. review Ben van Zuijlen (Security Coach)	Eveliene v.d. Vlies
0.4	11-10-2024	Tekstuele en inhoudelijke wijzigingen n.a.v. review Ben Hendrikx (Manager Bedrijfsvoering) en Hilde Ophoff-Hardeman (Directiesecretaris)	Eveliene v.d. Vlies
1.0	22-10-2024	Kleine tekstuele aanpassingen en spelfouten	Eveliene v.d. Vlies

Goedkeuringen

Naam	Rol	Geaccordeerd?	Datum	Versie
Eveline Schurink	Directeur Publieke Gezondheid			

Inhoudsopgave

1. Voorwoord 4

2 Management samenvatting 5

3 Inleiding 6

4 Wet- en regelgeving 7

5 Definitie, doelstelling, doelgroep en reikwijdte 8
5.1 Informatieveiligheid en informatiebeveiliging 8
5.2 Doelstelling, randvoorwaarden en uitgangspunten 8
5.3 Doelgroep 9
5.4 Reikwijdte van het beleid 9

6 Beleidsprincipes informatiebeveiliging en privacy 11
6.1 Inleiding 11
6.2 Beleidsprincipes 11

7 Governance IB-beleid 14
7.1 Afstemming met samenhangende risico's 14
7.2 Rollen en hun inpassing in IB-Governance 14
7.2.1 De eerste lijn 14
7.2.2 De tweede lijn 14
7.2.3 De derde lijn 15
7.2.4 Taken, bevoegdheden, verantwoordelijkheden 15
7.3 Bewustwording en training 16
7.4 Controle, oefenen, naleving en sancties 16
7.5 Financiering 17

8 Melding en afhandeling van incidenten en datalekken 18

9 Vaststelling & wijziging 19

1. Voorwoord

De Dienst Gezondheid & Jeugd Zuid-Holland Zuid (DG&J) is verantwoordelijk voor het bewaken, beschermen en bevorderen van de gezondheid van en creëren ontwikkelingskansen voor de inwoners van de regio Zuid-Holland Zuid. De DG&J helpt inwoners mee te doen aan een gezonde en sociaal veilige samenleving.

Het leveren van kwaliteit staat bij het uitvoeren van deze taak voorop. Om deze kwaliteit aan de inwoners van de regio Zuid-Holland Zuid en andere betrokkenen te kunnen bieden is een betrouwbare informatievoorziening essentieel.

De betrouwbaarheid van de informatievoorziening moet zijn gewaarborgd ongeacht de vorm. Uitgebreide aandacht voor de beveiliging van de opslag, verwerking en uitwisseling van informatie is continu vereist. Het beleid met betrekking tot informatiebeveiliging is in het voorliggende document beschreven.

Eveline Schurink
Algemeen Directeur en Directeur Publieke Gezondheid Dienst Gezondheid en Jeugd ZHZ

2 Management samenvatting

Onder informatiebeveiliging wordt verstaan het treffen en onderhouden van een samenhangend pakket aan maatregelen om de kwaliteitsaspecten beschikbaarheid, integriteit en vertrouwelijkheid van de informatievoorziening te garanderen .

De kwaliteitsaspecten:

- **Beschikbaarheid**: de mate waarin gegevens of functionaliteit op de juiste momenten beschikbaar zijn voor gebruikers;
- **Integriteit**: de mate waarin gegevens of functionaliteit juist ingevuld zijn;
- **Vertrouwelijkheid**: de mate waarin de toegang tot (persoons-)gegevens of functionaliteit beperkt is tot degenen die daartoe bevoegd zijn.

Hierbij gaat het ook om de controleerbaarheid van de maatregelen die genomen zijn om deze kwaliteitsaspecten te borgen. In dit document is verwoord op welke manier de DG&J voorziet in adequate informatiebeveiliging en daarmee voldoet aan de relevante wet- en regelgeving, inclusief de privacy wetgeving volgens de AVG.

Met het informatiebeveiligingsbeleid (IB-beleid) draagt de DG&J bij aan een betere kwaliteit van de informatievoorziening en zorgt voor een juiste balans tussen functionaliteit, veiligheid en privacy. Informatiebeveiliging werkt door in alle lagen van de organisatie en bij leveranciers.

Vijf beleidsprincipes zijn leidend, namelijk:

1. **Risico-gebaseerd**
   We baseren de maatregelen op de mogelijke veiligheidsrisico's van onze informatie, processen en IT-faciliteiten.
2. **Iedereen**
   Medewerkers voelen zich verantwoordelijk voor een juist en veilig gebruik van middelen en bevoegdheden.
3. **Altijd**
   Informatiebeveiliging zit in het DNA van al onze werkzaamheden.
4. **Security by design**
   Informatiebeveiliging is vanaf de start een integraal onderdeel van ieder project of iedere verandering m.b.t. informatie, processen en IT-faciliteiten.
5. **Security by default**
   Gebruikers hebben alleen toegang tot informatie en IT-faciliteiten die zij nodig hebben voor hun werkzaamheden. Het openstellen van informatie is een bewuste keuze. Met openstellen bedoelen we het toegankelijk maken van informatie, het delen van gegevens en het inzage hebben in gegevens.

Beleid en maatregelen zijn niet voldoende om alle risico's op het terrein van informatiebeveiliging uit te sluiten. De mens zelf creëert de grootste risico's. Bij de DG&J werken we daarom voortdurend aan het vergroten van het beveiligingsbewustzijn van medewerkers om kennis van risico's te verhogen en veilig en verantwoord gedrag aan te moedigen.

Informatiebeveiliging is een continu proces, waarbij we steeds kijken naar mogelijke verbeteringen. Dit gebeurt onder andere door rapportages, controles en bijsturing. Naast de Security en Privacy Officer, kunnen de Functionaris Gegevensbescherming en de externe auditor hier adviezen voor geven.

Het beschreven beleid is nog niet volledig geïmplementeerd, maar dient als de langetermijnvisie waarnaar we streven. Alle openstaande aandachtspunten zijn vastgelegd in ISOPlanner.

3 Inleiding

Om haar taken goed uit te kunnen voeren is de DG&J steeds meer afhankelijk van informatie, nieuwe technologieën en computersystemen. We kunnen niet meer zonder het digitaal verzamelen, vastleggen en delen van informatie met zowel interne als externe partners.

De digitale werkelijkheid is constant in beweging en dat brengt steeds nieuwe en andere risico's met zich mee voor de informatieveiligheid. De risico's vormen een bedreiging voor de kwaliteit en continuïteit van processen en voor het behalen van de strategische doelen. De bedreigingen kunnen de beschikbaarheid, integriteit en vertrouwelijkheid van informatie beïnvloeden. Ook de privacy van patiënten, cliënten, medewerkers en relaties en de reputatie van DG&J kunnen worden geschaad. Informatiebeveiliging is daarom van cruciaal belang.

Informatiebeveiliging vraagt steeds om bijstelling zodat er een passend beveiligingsniveau blijft. Dat komt onder andere door de technologische ontwikkelingen, nieuwe cyber dreigingen, de aangescherpte eisen om te voldoen aan de wet- en regelgeving rondom gegevensbescherming en privacy (AVG).

Het verkleinen en beheersen van de risico's vraagt om inspanningen op organisatorisch, procesmatig en technologisch vlak. Daarnaast moeten bestuurders, medewerkers, en relaties van de DG&J zich ook bewust worden van de risico's en hun handelen daarop afstemmen.

Informatieveiligheid is niet te bereiken door alleen een aantal technische en organisatorische maatregelen vast te stellen. Door de veranderende wereld is het een dynamisch proces. In dit document zijn om die reden vijf hoofdprincipes leidend voor informatiebeveiliging binnen de DG&J. De vast te stellen maatregelen, procedures en richtlijnen kunnen getoetst worden aan de vijf hoofdprincipes die in hoofdstuk 6 zijn beschreven.

Er is een belangrijke relatie tussen informatiebeveiligingsrisico's en risico's op andere gebieden, zoals privacy, veiligheid, fysieke beveiliging en businesscontinuïteit.

De volgende bijlagen zijn opgenomen:

A. Schematisch overzicht van het ISMS
   Informatiebeveiliging is een proces waarin een Plan Do Check Act cyclus centraal staat.
B. Nadere uitwerking van de informatiebeveiligingsprincipes
   Dit vormt de basis voor de implementatie van nieuwe functionaliteit en geeft handvatten om ontwikkelingen en innovaties veilig te realiseren.
C. BIV Classificatie
   Dit geeft de basis voor een risico gebaseerde aanpak van de beveiliging en sluit hiermee aan op de internationale standaarden.
D. Wet- en regelgeving
   Een korte opsomming van relevante wet- en regelgeving voor de DG&J en in het bijzonder de organisatieonderdelen GGD ZHZ, LVS ZHZ, VT ZHZ en SOJ ZHZ.
E. Beleid bescherming persoonsgegevens
   Hier wordt omschreven hoe de DG&J de zorgvuldige en behoorlijke omgang met persoonsgegevens waarborgt.
F. Maatregelenoverzicht vanuit de NEN 7510-1+A1:2020
   Dit wordt bijgehouden in de ISOPlanner.

4 Wet- en regelgeving

De DG&J streeft ernaar om in al haar processen en procedures te voldoen aan de relevante wet- en regelgeving. Dit doet zij op basis van het principe “Pas toe of leg uit”, waardoor de DG&J altijd kan verantwoorden waarom zij wel of niet voldoet.

In bijlage D is een overzicht opgenomen van de relevante wet- en regelgeving.

5 Definitie, doelstelling, doelgroep en reikwijdte

5.1 Informatieveiligheid en informatiebeveiliging

De begrippen informatieveiligheid en informatiebeveiliging worden vaak door elkaar gebruikt, maar ze hebben niet dezelfde betekenis. Informatieveiligheid richt zich op het beschikbaar, integer en vertrouwelijk houden van informatie. Hiervoor moeten informatie en informatiesystemen beschermd worden tegen mogelijke bedreigingen. Dit wordt gedaan door het nemen, onderhouden en controleren van beveiligingsmaatregelen, ook wel informatiebeveiliging genoemd.

5.2 Doelstelling, randvoorwaarden en uitgangspunten

Informatiebeveiliging heeft de volgende doelen:

1. Het waarborgen van de beschikbaarheid van informatie voor de bedrijfsvoering van de DG&J.
2. Het waarborgen dat informatie juist, volledig en actueel is (integriteit) en alleen toegankelijk is voor personen die vanuit hun rol/functie daar toegang tot mogen hebben (beschikbaarheid, integriteit en vertrouwelijkheid).
3. Het voorkomen van beveiligings- en privacy-incidenten en de eventuele gevolgen hiervan verminderen.

Met het informatiebeveiligingsbeleid (IB-beleid) wil de DG&J bijdragen aan een betere kwaliteit van de informatievoorziening en zorgen voor een juiste balans tussen functionaliteit, veiligheid en privacy en uiteraard de daarmee samenhangende kosten.

Het IB-beleid, en de opvolging daarvan, moet de DG&J in staat stellen ‘in control’ en compliant te zijn. Op basis daarvan kan de directie verantwoording afleggen aan het bestuur. De uitvoering van het beleid is ook de basis is om te voldoen aan wettelijke voorschriften, waaronder de privacy wetgeving ‘Algemene Verordening Gegevensbescherming (AVG)’.

Randvoorwaarden
Om deze doelstellingen te kunnen bereiken zijn de volgende randvoorwaarden voor de DG&J van belang:

1. **Beveiligingsorganisatie**
   De verantwoordelijkheden, taken en bevoegdheden van de informatiebeveiligingsfunctie zijn expliciet vastgelegd en worden gedragen door het bestuur, en afgeleid daarvan, door de hele organisatie.
2. **Procesbenadering**
   Informatiebeveiliging is een continu proces. Periodiek worden er risicoanalyses, assessments en audits uitgevoerd. De resultaten hiervan worden opgenomen in rapportages en vastgestelde jaarplannen met duidelijke keuzes in beveiligingsmaatregelen. De uitvoering van deze beveiligingsmaatregelen wordt periodiek gecontroleerd en vastgelegd in de ISOPlanner.

Uitgangspunten
Uit de doelstelling en de randvoorwaarden komen de volgende uitgangspunten voort:

1. **Kader**
   Het beleid biedt een kader om (toekomstige) maatregelen in de informatiebeveiliging te toetsen aan de vastgestelde beveiligingsprincipes (hoofdstuk 6), best practices en normen. Daarnaast biedt het een kader om de taken, bevoegdheden en verantwoordelijkheden in de instelling te beleggen.
2. **Normen**
   Specifiek voor zorginstellingen is de NEN 7510 vastgesteld. NEN 7510 vormt samen met dit beleidsdocument de basis voor een informatiebeveiligingsmanagementsysteem (ISMS, zie bijlage A) van de DG&J. Het ISMS is ingericht op basis van NEN 7510. Formele certificering, volgens de norm NEN 7510, wordt (nog) niet als noodzakelijk gezien voor de DG&J.
4. **Maatregelen**
   De DG&J neemt maatregelen op basis van NEN 7510. De maatregelen voor de DG&J en de wijze van implementatie zijn opgenomen in de bijlagen.

5.3 Doelgroep

Het IB-beleid is bestemd voor iedereen die – intern of extern – te maken heeft met de processen van de DG&J. Het beleid richt zich in eerste instantie op het bestuur, de directie, de Security en Privacy Officer, de leidinggevenden en applicatie eigenaren.

Zij dragen uit dat het beleid van toepassing is op:

- Alle medewerkers zowel met arbeidsovereenkomst als o.b.v. huur
- Ketenpartners
- Ketenleveranciers
- Opdrachtgevers
- Burgers en bezoekers
- Overige externe relaties

Het is belangrijk dat iedereen die – intern of extern – te maken heeft met de processen van de DG&J op de hoogte is van de beveiligingsnormen en -vereisten die van toepassing zijn wanneer zij met gevoelige of vertrouwelijke informatie omgaan. Dit kan bijvoorbeeld door middel van contractuele afspraken, het delen van relevante delen van het beveiligingsbeleid of het instellen van specifieke procedures en controles om de veiligheid te monitoren en te waarborgen bij samenwerking met externe partijen.

5.4 Reikwijdte van het beleid

Bij de DG&J wordt informatieveiligheid breed geïnterpreteerd. Het gaat over alle vormen van formeel vastgelegde informatie (dus niet alleen digitale informatie), die de instelling of haar relaties genereren en beheren.

Daarnaast heeft het beleid betrekking op niet-formeel vastgelegde informatie, zoals uitspraken van medewerkers in discussies, op webpagina's en persoonlijke websites, waarop men de DG&J kan aanspreken. Het IB-beleid heeft betrekking op alle dienstverlening. Het gaat over alle door (namens) de DG&J beheerde apparaten en (uitbesteedde) applicaties waarmee geautoriseerde toegang tot (diensten van) het DG&J-netwerk kan worden verkregen en/of waarmee data wordt verwerkt. Dit betreft dus alle applicaties waarvan de DG&J gebruik maakt.

Onder apparaten en applicaties vallen:

- Alle fysiek op het netwerk aangesloten apparaten zoals servers, werkstations, laptops, gebouwbeheerssystemen.
- Alle draadloos op het netwerk aangesloten mobiele apparaten, zoals notebooks, tablets, smartphones, smartwatches.
- IoT-devices, zoals bewakingscamera's en sensoren.
- Alle op deze apparaten beschikbare (web/cloud)services en applicaties ('apps').

De DG&J faciliteert in beperkte mate het gebruik van privéapparaten (BYOD). Het gebruik van BYOD voor toegang tot applicaties of informatie van de instelling valt onder dit IB-beleid. Het beleid is locatie-onafhankelijk: het geldt ook als men op een andere locatie dan op het kantoor van de DG&J, met informatie of informatievoorzieningen van de DG&J werkt (zoals bijvoorbeeld thuis, in de trein of bij een client bijvoorbeeld)

6 Beleidsprincipes informatiebeveiliging en privacy

6.1 Inleiding

De DG&J is een organisatie met als motto: "Open waar mogelijk, gesloten waar nodig". Adequate beveiliging van informatie is steeds een randvoorwaarde en het openstellen van informatie moet een bewuste keuze zijn. De DG&J heeft vijf beleidsprincipes voor informatiebeveiliging vastgesteld. Deze helpen om te bepalen welke beveiligingsmaatregelen er nodig zijn.

Een beleidsprincipe bestaat uit:

1. Een titel (vaak verklarend).
2. Een korte uitleg (de achtergrond).
3. De implicaties die uit het beleidsprincipe volgen als basis voor de te nemen maatregelen.

Een korte introductie van de vijf beleidsprincipes volgt in paragraaf 6.2. Een gedetailleerde uitwerking van deze principes is opgenomen in bijlage B.

De uiteindelijk door de DG&J vastgestelde maatregelen zijn niet altijd 1-op-1 toepasbaar in alle situaties. Soms zijn er bijvoorbeeld processen die afwijken of bestaan er technische of organisatorische beperkingen. In die gevallen moeten er vervangende maatregelen worden genomen waarmee het achterliggende principe tot zijn recht komt en de risico's voldoende worden afgedekt, volgens het uitgangspunt "Pas toe of leg uit".

Om tot een goede afweging te komen of vervangende maatregelen inderdaad tot een acceptabel restrisico leiden, moeten ze aan het IB-beleid van de DG&J worden getoetst. Met de beleidsprincipes en hun implicaties voor informatiebeveiliging en privacy uit dit hoofdstuk kan die toetsing plaatsvinden, ook al zijn vervangende maatregelen niet uitputtend in het beleid of in baselines vastgelegd.

6.2 Beleidsprincipes

De vijf hierna vermelde beleidsprincipes helpen bij de implementatie van het IB-beleid. Op basis van deze vijf beleidsprincipes kunnen maatregelen worden geformuleerd die relevant zijn voor de bescherming van processen van de DG&J. De beleidsprincipes vormen de basis voor de communicatie rondom het IB-beleid van de DG&J.

Ook zijn de beleidsprincipes bedoeld om als basis te gebruiken voor de toetsing van uitzonderingen of keuzes bij onvoorziene omstandigheden.
De vijf door de DG&J vastgestelde beleidsprincipes zijn:

1. Risico-gebaseerd
2. Iedereen
3. Altijd
4. Security by design
5. Security by default

1	**Risico-gebaseerd** Informatiebeveiliging is risico-gebaseerd.
Kern	We baseren de maatregelen op de mogelijke veiligheidsrisico's van onze informatie, processen en IT-faciliteiten.
Achtergrond	Voor een goede risicoafweging bij het beschermen van informatie en het treffen van de juiste maatregelen, is het van belang om de waarde van (persoons-) informatie vast te stellen. Als de waarde van informatie bekend is, kan ook de juiste mate van beveiliging worden bepaald, één die past bij de risico's.
Implicaties	Denk aan het inrichten van een risicomanagementproces (BIV-classificatie), het vastleggen van verantwoordelijkheden, het borgen van risico's in contracten. Zie bijlage B voor een overzicht van alle implicaties.

2	**Iedereen** Informatiebeveiliging en privacy is een verantwoordelijkheid van iedereen.
Kern	Iedereen is en voelt zich verantwoordelijk voor een juist en veilig gebruik van middelen en bevoegdheden.
Achtergrond	Iedereen is zich bewust van de waarde van informatie en handelt daarnaar. Deze waarde wordt bepaald door de mogelijke schade als gevolg van verlies van beschikbaarheid, integriteit of vertrouwelijkheid. Van zowel medewerkers als derden wordt verwacht dat ze bewust omgaan met (persoons-)informatie in welke vorm dan ook en dat ze actief bijdragen aan de veiligheid van de geautomatiseerde systemen en de daarin opgeslagen informatie. Het succes van beveiliging staat of valt met goede communicatie. Goede communicatie wordt daarom actief bevorderd, op en tussen alle niveaus binnen de DG&J.
Implicaties	Denk hierbij aan het vastleggen van afspraken in arbeidsvoorwaarden, omgangsvormen, gedragscodes en huisregels, etc. Zie bijlage B voor een overzicht van alle implicaties.

3	**Altijd** Informatiebeveiliging is een continu proces.
Kern	Informatiebeveiliging zit in het DNA van al onze werkzaamheden.
Achtergrond	De omgeving verandert continu; cyberdreigingen nemen toe en af; processen veranderen, medewerkers veranderen etc. Eenmalig de maatregelen bepalen en implementeren is onvoldoende om een veilig klimaat te behouden. Informatiebeveiliging heeft alleen zin als dit een continu proces is van het nemen van maatregelen, bewustzijn en controles.
Implicaties	Denk hierbij aan het houden van awareness campagnes, het inrichten van een audit-proces. Zie bijlage B voor een overzicht van alle implicaties.

4	**Security by design** Integrale aanpak informatiebeveiliging.
Kern	Informatiebeveiliging is vanaf de start een integraal onderdeel van ieder project of iedere verandering m.b.t. informatie, processen en IT-faciliteiten.
Achtergrond	Security by design betekent dat al tijdens de start van een project, het ontwerp van een nieuwe applicatie of ICT-omgeving en bij technische of

	functionele veranderingen rekening wordt gehouden met de beveiliging van (persoons-)gegevens en de continuïteit van de processen. Dit voorkomt (vaak dure) herstelwerkzaamheden achteraf.
Implicaties	Denk hierbij aan het vaststellen en toetsen van beveiligingseisen in projecten en het inregelen van autorisatieschema's. Zie bijlage B voor een overzicht van alle implicaties.

5	**Security by default** Standaard beperkte toegang en veilige instellingen.
Kern	Gebruikers hebben alleen toegang tot informatie en IT-faciliteiten die zij nodig hebben voor hun werkzaamheden. Het openstellen van informatie is een bewuste keuze.
Achtergrond	Security by default betekent dat in elke configuratie die wordt geïmplementeerd de aanwezige security opties standaard aan staan. Dit voorkomt ongewenste en ongecontroleerde toegang tot (persoons-) gegevens. Openstellen van informatie is daarmee altijd een bewuste keuze na een zorgvuldige afweging.
Implicaties	Denk hierbij aan het definiëren van standaard rollen en het standaard beperken van autorisaties en het standaard beschermen van alle externe communicatie met SSL-technologie. Zie bijlage B voor een overzicht van alle implicaties.

7 Governance IB-beleid

7.1 Afstemming met samenhangende risico's

Bij governance moet aandacht zijn voor alle soorten risico's en hun onderlinge samenhang. Om die reden besteedt de DG&J aandacht aan afstemming van informatiebeveiliging, business-continuïteit en privacybescherming.

Waar mogelijk en nodig vertaalt deze afstemming zich ook naar het tactische en operationele niveau. De governance rondom informatiebeveiliging wordt daarom in gezamenlijkheid opgepakt. Dit hoofdstuk gaat in op de governance van de informatieveiligheid en informatiebeveiliging (hierna IB-Governance genoemd) als onderdeel van de governance van de DG&J.

7.2 Rollen en hun inpassing in IB-Governance

Deze paragraaf beschrijft hoe de IB-Governance is georganiseerd, wie waarvoor verantwoordelijk is en aan wie wordt gerapporteerd. In de diverse rollen is onderscheid gemaakt in richtinggevend (strategisch), sturend (tactisch) en uitvoerend (operationeel).

De IB-Governance bij DG&J is ingericht volgens het zogenaamde Three Lines of Defence Model (ook wel '3LoD'). Dit model wordt algemeen toegepast als model om Governance, Risk en Compliance (GRC) te borgen in een operationele organisatie. Het beschrijft niet alleen de rollen binnen de organisatiestructuur, maar ook hun onderlinge samenwerking.

7.2.1 De eerste lijn

Het 3LoD-model heeft als uitgangspunt dat het lijnmanagement (de business) verantwoordelijk is voor haar eigen processen. De directeur zorgt samen met het Directieteam ervoor dat beveiligingsmaatregelen worden geïmplementeerd, dat awareness-programma's worden uitgevoerd, dat personeel wordt opgeleid, etc. Dit is rol van de eerste lijn. Bij de DG&J zijn een aantal activiteiten uitbesteed en de maatregelen gelden ook voor de leveranciers, zij moeten minimaal een vergelijkbaar niveau realiseren. Er kan afgeweken worden als een risico-analyse is gemaakt en mocht het niveau lager zijn dan vereist, dan kan er onderbouwd afgeweken worden o.b.v. uitkomst van de risico-analyse. Dit alles wordt vastgelegd in de ISOPlanner.

7.2.2 De tweede lijn

Er moet een functie zijn die de eerste lijn ondersteunt, adviseert, coördineert en die bewaakt of het management zijn verantwoordelijkheden ook daadwerkelijk neemt. Dit is de tweede lijn. Ook bepaalde beleidsvoorbereidende taken, het organiseren van de PDCA-cyclus, van integrale risicoanalyses en self-assessments en het opstellen van jaarplannen en rapportages zijn taken van de tweede lijn.

De tweede lijn voor informatiebeveiliging wordt bij de DG&J ingevuld door een Security Officer. De Security Officer is verantwoordelijk voor het opstellen van het informatiebeveiligingsbeleid en het ISMS-proces. Daarnaast vertaalt hij dit waar nodig naar tactische (en operationele) plannen. Dit doet hij samen met management en systeem- en proceseigenaren.

De Privacy Officer in de tweede lijn behandelt de verschillende privacy vraagstukken binnen de organisatie.

De Security Officer is verantwoordelijk voor het bredere risico management proces, waarvan informatiebeveiliging een onderdeel is.

7.2.3 De derde lijn

Het is wenselijk dat er binnen de organisatie een functie bestaat die controleert of het samenspel tussen de eerste en tweede lijn soepel functioneert en daarover een objectief, onafhankelijk oordeel velt met mogelijkheden tot verbetering. Daarbij kijkt men ook of er geen overlapping is en of er blinde vlekken bestaan. Deze functie is de derde lijn.

De binnen de AVG verplichte Functionaris Gegevensbescherming (FG), de (ingehuurde) auditor en externe accountant behoren bij DG&J tot de derde lijn. Zij opereren volledig los van alle andere organisatieonderdelen. Zij kunnen adviseren en rapporteren aan de directeur, maar ook onafhankelijk aan het Bestuur.

7.2.4 Taken, bevoegdheden, verantwoordelijkheden

De diverse taken, bevoegdheden en verantwoordelijkheden zijn onderverdeeld in strategisch, tactisch en operationeel niveau.

Het operationele niveau (eerste lijn) is verantwoordelijk voor de implementatie van de informatiebeveiligingsmaatregelen en de afhandeling van incidenten. Dat gebeurt in overleg met de functioneel beheerders, IT functionarissen en veelal in samenwerking met de leveranciers.

Om de samenhang in de organisatie van de informatiebeveiligingsfunctie goed tot uitdrukking te laten komen en de initiatieven en activiteiten op het gebied van informatiebeveiliging op elkaar af te stemmen wordt bij de DG&J gestructureerd overleg gevoerd over het onderwerp informatiebeveiliging en met de belangrijkste leveranciers.

Strategisch niveau	**Tactisch niveau**	**Operationeel niveau**
Op strategisch niveau wordt richtinggevend gesproken over governance, risk en compliance, alsmede over doelen, scope en ambitie op het gebied van informatiebeveiliging, in samenhang met privacy. Dit gebeurt in het Bestuur, geadviseerd door de directie. De Security en Privacy Officer adviseren de Directie. Hierbij wordt afgestemd met de IT-strategie en de risicobereidheid van de DG&J.	Op tactisch niveau wordt de strategie vertaald naar plannen, maatregelen, te hanteren normen, evaluatiemethoden, e.d. Deze plannen en instrumenten zijn sturend voor de uitvoering. Dit tactisch overleg wordt gevoerd in het ontwikkelingsoverleg met de Security Officer en hoofd Stafafdeling Bedrijfsvoering. Waar nodig in overleg met overige betrokken functionarissen zoals de proces- of systeemeigenaren en leveranciers.	Op operationeel niveau worden de zaken besproken die de dagelijkse bedrijfsvoering aangaan in de zin van uitvoering en implementatie. Dit zal veelal gebeuren in het beheeroverleg.

Alle drie overlegtypes worden zoveel mogelijk ingepast in bestaande overlegvormen met hetzelfde karakter.

Zo bespreekt men op strategisch niveau niet alleen informatiebeveiliging en privacy, maar ook andere risico's waarmee de DG&J te maken kan krijgen, zoals financieel, personeel en commercieel. Dat betekent bij de DG&J dat informatiebeveiliging op de agenda staat van de directie en het bestuur.

Voorbeelden van te bespreken IB onderwerpen op het strategisch niveau:

- Bepalen IB strategie (beleid)
- Organisatie voor IB inrichten
- IB planning en control vaststellen
- Accorderen risico beoordelingen
- Audit resultaten en voortgang actiepunten
- Business continuity management
- Communicatie naar management en organisatie
- Rapportages

Op tactisch niveau zal het ook gaan over keuze van IT-functionaliteit en -services op de agenda van het MT en het ontwikkelingsoverleg.
Voorbeelden van te bespreken IB onderwerpen op het tactisch niveau:

- Planning & Control IB (IB halfjaar rapportages).
- Voorbereiden normen en wijze van toetsen.
- Evalueren beleid en maatregelen, ook van externe partijen bij contracten.
- Leveranciers beoordelingen
- Begeleiding interne assessments en externe audits (classificaties, risicoanalyses en audits, inclusief DPIA's).
- Communicatie naar proces- en systeemeigenaren, leveranciers en IT-ondersteuning.

Op operationeel niveau worden de zaken besproken die de dagelijkse bedrijfsvoering aangaan in de zin van uitvoering en implementatie.
Voorbeelden van te bespreken IB onderwerpen op het operationeel niveau:

- Implementeren IB-maatregelen.
- Registreren en evalueren incidenten, inclusief privacy incidenten en datalekken
- Communicatie naar eindgebruikers
- SLA's (securityparagraaf)

7.3 Bewustwording en training

Beleid en maatregelen zijn niet voldoende om risico's op het terrein van informatiebeveiliging uit te sluiten. De mens zelf creëert ook risico's. Bij de DG&J werken we daarom voortdurend aan het vergroting van het beveiligingsbewustzijn van medewerkers om kennis van risico's te verhogen en veilig en verantwoord gedrag aan te moedigen. Onderdeel van het beleid zijn regelmatig terugkerende bewustwordingscampagnes voor alle medewerkers.

Verhoging van het beveiligingsbewustzijn is een verantwoordelijkheid van zowel de leidinggevenden als de Security Officer.

7.4 Controle, oefenen, naleving en sancties

Bij de DG&J is het Hoofd Stafafdeling Bedrijfsvoering verantwoordelijk voor de (planning van de) audits. De Security Officer controleert op de uitvoering van de informatiebeveiligings jaarplannen.

De interne controles vinden periodiek plaats en worden naast de reguliere formele audits aangevuld met diverse incidentele activiteiten, zoals het nemen van steekproeven, het uitvoeren van penetratietesten en het controleren van de feitelijke werking van de vastgestelde beveiligingsmaatregelen. Daarnaast worden vaardigheden en procedures periodiek getest via bijvoorbeeld oefeningen.

De bevindingen van de interne en externe controles en mogelijke externe eisen met betrekking tot beveiliging, zijn input voor de nieuwe jaarplannen van de DG&J. Deze kunnen ook tot wijziging van het IB-beleid leiden.

Controle op de naleving vindt plaats door toezicht te houden op hoe in de dagelijkse praktijk met informatiebeveiliging wordt omgegaan. Hierbij is het van belang dat leidinggevenden de medewerkers aanspreken op tekortkomingen. Voor het toezicht op de naleving van de AVG is de 'Functionaris Gegevensbescherming' (FG) verantwoordelijk.

Als uit de controles blijkt dat de naleving ernstig tekortschiet, dan kan de DG&J de betrokken verantwoordelijke medewerkers een sanctie opleggen. De sanctie wordt opgelegd binnen de kaders van het personeelshandboek, arbeidsovereenkomsten en de wettelijke mogelijkheden.

7.5 Financiering

De financiering van informatiebeveiliging wordt bij de DG&J centraal geregeld.

Algemene zaken, zoals het opstellen van een informatiebeveiligingsplan, uitvoeren van beveiligingsmaatregelen of een externe audit, vallen binnen de begrotingen. Bewustwordingscampagnes en trainingen voor specifieke toepassingen of doelgroepen worden ook uit deze middelen betaald.

De beveiliging van uitbesteedde informatiesystemen en processen, inclusief de kosten daarvan, zijn integraal onderdeel van verantwoord beheer van het betreffende informatiesysteem of proces. Beveiligingskosten van werkplekken maken onderdeel uit van de werkplekkosten.

8 Melding en afhandeling van incidenten en datalekken

Een incident is een gebeurtenis die de bedrijfsvoering negatief kan beïnvloeden. Incidentbeheer en -registratie gaat over het detecteren, vastleggen en afhandelen van incidenten.

Belangrijk hierbij is dat medewerkers herkennen wanneer er sprake is van een incident, datalek of inbreuk op de informatiebeveiliging en dit ook melden. Iedere medewerker is verantwoordelijk voor het signaleren en melden van incidenten en inbreuken op de informatiebeveiliging, inclusief datalekken.

Security incidenten kan men bij de DG&J melden via TOPdesk DG&J, tegel ‘Melden Beveiligingsincident’.

Van incidenten kan worden geleerd. Incidentregistratie en periodieke rapportage over opgetreden incidenten horen dan ook thuis in een volwassen informatiebeveiligingsomgeving. De incidenten worden afgehandeld volgens het door de DG&J vastgestelde security incident managementproces, waar de afhandeling van datalekken een onderdeel van is.

Er is een vastgesteld beleid voor Vulnerability Disclosure (zie bijlage G). Daarmee geeft de DG&J mogelijke melders van kwetsbaarheden in de informatiesystemen een garantie dat de DG&J, onder voorwaarden, geen juridische stappen tegen hen onderneemt.

9 Vaststelling & wijziging

Het bestuur stelt het IB-beleid vast dat de Security Officer voorstelt, na goedkeuring in de directie. Het IB-beleid volgt de kaders van het beleid van de DG&J. Het wordt 1x per jaar geëvalueerd en zo nodig bijgesteld. Minimaal 1 keer per 4 jaar, of na belangrijke ontwikkelingen op cyberveiligheidsgebied, wordt het beleid herzien en opnieuw door het bestuur vastgesteld.

Kleinere wijzigingen in dit beleid worden verwerkt door de Security Officer en goedgekeurd in het directie overleg van de DG&J.

Op grond van de samenwerking met onze IT-leverancier, de Service Gemeente Dordrecht, is een regionaal Strategisch Informatiebeveiligingsbeleid tot stand gekomen waarin ook de DG&J wordt genoemd. Dit regionale beleid is gebaseerd op de BIO (Baseline Informatiebeveiliging Overheid).

Wij hebben er echter bewust voor gekozen om een eigen Strategisch Informatiebeveiligingsbeleid te formuleren op basis van de NEN 7510.
Dit beleid is specifiek afgestemd op de unieke eigenschappen van onze organisatie en de bijzondere persoonsgegevens die wij verwerken. Hierdoor sluit het beleid beter aan op onze interne visie en strategische doelstellingen dan het bredere regionale beleid.

Daarnaast hebben wij als DG&J, naast SGD, diverse andere leveranciers en moeten we voldoen aan andere wet- en regelgeving dan gemeenten. Wij dragen zelf de verantwoordelijkheid voor onze informatiebeveiliging en onderbouwen dit met een eigen Strategisch Informatiebeveiligingsbeleid.

dienstGezondheid & Jeugd zhz

Karel Lotsyweg 40
Postbus 166, 3300 AD Dordrecht

078 770 8500
info@dgjzhz.nl
www.dienstgezondheidjeugd.nl