dienstGezondheid & Jeugd zhz

Bijlagen Strategisch Informatiebeveiligingsbeleid Dienst Gezondheid & Jeugd

Bijlagen

Strategisch

Informatiebeveiligingsbeleid

versie 1.0

22 oktober 2024

Classsificatie: Intern (Definitief)

GGD ZHZ | LVS | SOJ | Veilig Thuis

Inhoudsopgave

Document historie

Versie	Datum	Veranderingen	Auteur
0.1	12-09-2024	Eerste opzet	Eveliene v.d. Vlies
0.2	3-10-2024	Inhoudelijke en tekstuele aanpassingen n.a.v. review Ben van Zuijlen (Security Coach)	Eveliene v.d. Vlies
0.3	11-10-2024	Inhoudelijke en tekstuele aanpassingen n.a.v. review Ben Hendrikx	Eveliene v.d. Vlies
1.0	22-10-2024	Kleine tekstuele aanpassingen en spelfouten	Eveliene v.d. Vlies

Goedkeuringen

Naam	Rol	Geaccordeerd	Datum document	Versie
Eveline Schurink				

Leeswijzer

Dit document bevat de bijlagen van het Informatiebeveiligingsbeleid van de DG&J en gaat dieper en inhoudelijk in op de onderwerpen in het beleid. Het geeft meer inzicht in de onderwerpen en bevat een compleet overzicht van de maatregelen.

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.
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
   Hier een beschrijving van de verschillende maatregelen en de invulling zoals dit bij de DG&J is gerealiseerd.
G. Vulnerability Disclosure
   Een vulnerability disclosure is het proces waarbij een beveiligingskwetsbaarheid (vulnerability) in software, hardware, of een IT-systeem op een verantwoordelijke manier wordt gemeld aan de eigenaar of ontwikkelaar ervan. Het doel is om de kwetsbaarheid te laten verhelpen voordat deze kan worden misbruikt door kwaadwillenden. Het proces omvat vaak afspraken over hoe en wanneer de informatie over de kwetsbaarheid openbaar mag worden gemaakt, zodat de betreffende partij tijd heeft om een oplossing te ontwikkelen en uit te rollen.

De NEN 7510-1+A1:2020 norm bevat ook implementatierichtlijnen, deze kunnen geraadpleegd worden bij de implementatie, uitvoering en beoordeling van de beveiligingsmaatregelen. Tot slot dient vermeld te worden dat de volgorde van de hoofdstukken en paragrafen in dit document geen maat is van hun belangrijkheid.

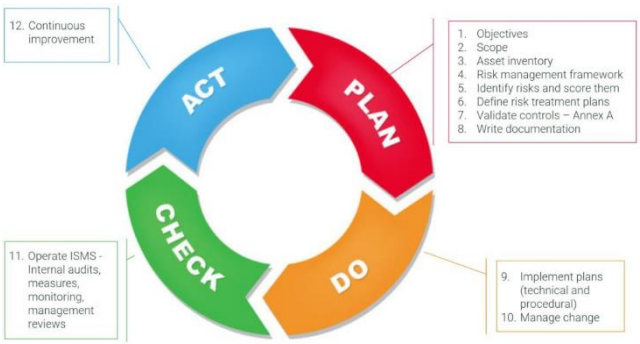
Bijlage A – Schematisch overzicht inrichting ISMS

Informatiebeveiliging is een continu proces. Kort gezegd: eerst moet worden vastgesteld wat nodig is, waarna maatregelen worden getroffen. Deze maatregelen worden vastgelegd in een jaarplan. De maatregelen kunnen veranderen (omdat bedreigingen en risico's veranderen, maar ook wet- en regelgeving is aan verandering onderhevig). Controle kan dan aanleiding geven tot bijsturing van de maatregelen. Daarnaast kan ook het totaalpakket van eisen, maatregelen en controle aan een herijking toe zijn en zal dus periodiek geëvalueerd moeten worden. Het gehele proces van informatiebeveiliging volgt dus een Plan-Do-Check-Act (PDCA)-cyclus (zie afbeelding).

De aanpak van security binnen de DG&J is gebaseerd op de NEN 7510-1+A1:2020.

1.1 Toelichting PCDA cyclus

De aanpak is gebaseerd op de PDCA cyclus, waarbij de verschillende stappen worden uitgevoerd om de beveiliging op een hoger niveau te krijgen. Dit proces kent een aantal stappen en een aantal herkenbare resultaten.



1. *PLAN*
   In deze fase worden doelstellingen en scope geformuleerd, bepaald welke bedrijfsmiddelen/systemen aanwezig zijn (applicatielijst), welke risico's gekoppeld zijn aan deze systemen (BIV-classificatie), competenties, bewustzijn en communicatie. Beoordelingen van bestaande maatregelen kunnen leiden tot concrete verbetervoorstellen. Onderdeel van de planfase is het maken en evalueren van het beleid, met gewenst niveau, gebaseerd op de ISO standaarden.

2. *DO*
   Geplande verbeteringen worden doorgevoerd in de beveiliging en beheersing van verschillende systemen, risicobeoordeling(en) en risicobehandeling Dit moet leiden tot gedocumenteerde beveiligingsmaatregelen bij de DG&J en haar leveranciers.

3. *CHECK*
   In de verschillende audits, management reviews en met security dashboards worden diverse checks uitgevoerd. Daarnaast worden overzichten bijgehouden met kentallen, zoals aantal datalekken, aantal security incidenten etc.

4. *ACT*
   Resultaten en aanbevelingen uit de check fase worden gebruikt om verbeteringen in te plannen en door te voeren.

Elk halfjaar wordt er gerapporteerd over de resultaten en de status van informatiebeveiliging, met de geplande verbeteringen voor de komende perioden. Door herhaling van de PDCA-cyclus werkt de organisatie doorlopend aan het verbeteren van het ISMS en is daardoor meer 'in control'.

De DG&J maakt gebruik van de applicatie ISOPlanner voor het vormgeven van haar ISMS.

1.2 Verantwoordelijkheden

Onderstaande tabel geeft een overzicht op hoofdlijnen van de verantwoordelijkheden ten aanzien van informatiebeveiliging, gebaseerd op de hoofdstukken uit de NEN 7510-2+A1:2020 norm. Deze verantwoordelijkheden betreft de verantwoordelijkheden binnen de DG&J.

Nr	RACI OVERZICHT **Hoofdstuk**	Directie DG&J	Applicatie-eigenaar	Medewerkers DG&J	Security & Privacy Officer
5	Opstellen informatiebeveiligingsbeleid	A	C	I	R
6	Organiseren van informatiebeveiliging	A	C	I	R
7	Veilig personeel	AR	C	R	R
8	Beheer van bedrijfsmiddelen	A	R	C	C
9	Toegangsbeveiliging (logisch)	A	R	C	C
10	Cryptografie	A	R	I	C
11	Fysieke beveiliging & beveiliging van de omgeving	A	R	R	C
12	Beveiliging bedrijfsvoering	AR	R	R	C
13	Communicatiebeveiliging	A	R	I	C
14	Acquisitie, ontwikkeling en onderhoud van informatiesystemen	A	R	C	C
15	Leveranciersrelaties	AR	R	C	C
16	Beheer van informatiebeveiligingsincidenten	A	R	CR	R
17	Informatiebeveiligingsaspecten van bedrijfscontinuïteitsbeheer	A	R	C	C
18	Naleving	AR	R	C	CR

R=Responsible / A=Accountable / C= Consulted / I= Informed

1.3 Governance

De directie is eindverantwoordelijk voor de uitvoering van het informatiebeveiligingsbeleid. Zij bepaald de prioriteiten en stelt budget beschikbaar om de maatregelen te implementeren, uit te voeren, te verbeteren en de werking te controleren. Het bestuur van de DG&J wordt hierbij op de hoogte gehouden en kunnen gevraagd en ongevraagd advies geven.

De Security Officer is een rol op strategisch en tactisch niveau. De Security Officer ontwikkelt het beleid en bewaakt de uniformiteit ten aanzien van informatiebeveiliging binnen de organisatie en dient gevraagd zowel als ongevraagd directie en bestuur van advies. De Security Officer rapporteert halfjaarlijks over de status, voortgang en planning.

Bijlage B – Uitwerking informatiebeveiligingsprincipes

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 (bijzondere 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.
Proportionaliteit daarin is gewenst, ook om de beschikbare financiële middelen efficiënt te gebruiken ('Fit for purpose').

Implicaties

- De risico's worden ingeschat en vastgesteld op basis van een BIV risicoclassificatie (zie bijlage C).
- Een gegevensbeschermingseffectbeoordeling (DPIA – Data Protection Impact Assessment) in het kader van de AVG maakt waar nodig onderdeel uit van de risicoanalyse.
- Er worden maatregelen getroffen om het vastgestelde risico op Beschikbaarheid, Integriteit en Vertrouwelijkheid te brengen naar het geaccepteerde niveau.
- Een informatiesysteem heeft één eigenaar.
- Eigenaren van informatie, informatiesystemen, applicaties en processen zijn verantwoordelijk voor de implementatie en operationele handhaving van maatregelen onder het principe van "Pas toe of leg uit".
- Afwijkingen kunnen worden geaccepteerd binnen de risicobereidheid ('risk-appetite') van de DG&J, uiteindelijk te bepalen door het bestuur.
- Voor afwijkingen moet het risico-acceptatieproces worden gevolgd, met acceptatie door de informatie-, proces- of applicatie-eigenaar.
- De informatie-eigenaar (of eventueel ook de proces- of applicatie-eigenaar) tekent voor acceptatie van de risico's.
- Maatregelen moeten zo worden ingericht dat hun effect controleerbaar is.
- De hoogste risico's worden als eerste gemitigeerd.
- Op basis van de risicoanalyse kan informatiebeveiliging voor gebruiksgemak kiezen.
- Maatregelen moeten (qua kosten) in balans zijn met de vermindering van risico's (proportionaliteitsprincipe).
- Informatie heeft één bron, waardoor eigenaarschap en "single point of truth" goed te duiden is. Hierdoor ontstaat ook een extra ketenverantwoordelijkheid voor de consequenties van wijzigingen bij de bron.
- De DG&J blijft verantwoordelijk voor adequate bescherming van informatie bij gebruik van externe diensten voor informatieverwerking.
- Waar van toepassing bevatten contracten de veiligheidseisen en de levering van externe toetsing (assurance) die laat zien dat maatregelen effectief zijn.

2 Iedereen

Informatiebeveiliging 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 medewerkers 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 in de organisatie.

Implicaties

- Voor alle gebruikers van digitale informatievoorzieningen van de DG&J is een zogenaamde Acceptabel Use Policy (AUP) beschikbaar die is gepubliceerd via de website van de DG&J. Deze AUP is van toepassing op medewerkers en derden.
- Het veilig omgaan met informatie en informatiedragers is een onderdeel van de aanstelling/arbeidsovereenkomst van alle medewerkers (geheimhoudingsverklaring).
- Informatiebeveiliging krijgt aandacht bij indiensttreding van medewerkers en bij periodieke overleggen.
- Informatiebeveiliging krijgt aandacht in reguliere overleggen in afdelingen en projecten.
- Medewerkers en externen spreken elkaar aan op onveilige omgang met informatie en systemen.
- Medewerkers melden (vermoedens van) kwetsbaarheden bij de Security Officer, via TOPdesk DG&J-> tegel 'Melden Beveiligingsincident'.
- Er is een door het bestuur vastgesteld Responsible Disclosure beleid.
- Schending van wetgeving, voorschriften en regels op gebied van informatiebeveiliging kan leiden tot sanctionerende maatregelen, door of namens het bestuur, zoals vastgelegd in het personeelshandboek.

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

- Er wordt een Information Security Management Systeem (ISMS, zie bijlage A) ingericht waarmee door middel van een

PDCA-cyclus alle aspecten van het IB beleid adequaat worden opgevolgd. Bij de DG&J zal dit door middel van de applicatie ISOPlanner gedaan worden.
- Periodiek worden audits en assessments uitgevoerd die het mogelijk maken het beleid en de genomen maatregelen te controleren op effectiviteit (controleerbaarheid).
- Bij instroom van nieuwe medewerkers is er aandacht voor de bewustwording van de risico's en de beveiligingsprocedures van de DG&J rond toegang en gebruik van IT-middelen.
- Periodiek worden accounts met hoge privileges gevalideerd.
- De DG&J organiseert regelmatig cybersecurity-awareness activiteiten voor de diverse doelgroepen: medewerkers en leidinggevenden van de DG&J.
- Bij aanpassingen in rollen, taken, en verantwoordelijkheden van een persoon worden ook de autorisaties daarmee in overeenstemming gebracht en aangepast.
- Er wordt een proces ingericht om het dreigingsbeeld voor de DG&J te bepalen en periodiek bij te stellen. Nieuwe dreigingen leiden waar nodig tot aanpassing van maatregelen. Denk hierbij aan het houden van awareness campagnes, het inrichten van een audit-proces.

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 en privacy van (persoons-)gegevens en de continuïteit van de processen. Dit voorkomt (vaak dure) herstelwerkzaamheden achteraf.

Implicaties

- Voor elk nieuw project/software-inkoop/innovatie worden de security-eisen (non-functional requirements) vanaf de start meegenomen.
- Voor de livegang wordt de toepassing van de security-eisen getoetst en/of getest.
- Bij elk IT-systeem of inrichting wordt ter bevordering van informatiebeveiliging het principe van 'minste rechten' gehanteerd. Dat betekent dat ernaar wordt gestreefd om niet meer rechten te verlenen dan nodig zijn voor adequate functie- en bedrijfsuitoefening.
- Toegang tot systemen is gebaseerd op autorisatieschema's.
- Scheiding van verantwoordelijkheden wordt toegepast in processen en procedures.
- In het ontwerp wordt meegenomen dat het gebruik van informatie en IT-voorzieningen herleidbaar is tot een verantwoordelijke gebruiker.
- Er wordt een richtlijn "security in projecten" vastgesteld,

gebaseerd op de maatregelen die voortkomen uit de risicoclassificatie en maatregelen die mogelijk voortvloeien uit de gegevensbeschermingseffectbeoordeling (DPIA) in het kader van de AVG.
- Bij procesontwerp worden maatregelen meegenomen die de continuïteit van het proces afdoende kunnen waarborgen.

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 (persoons-)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

- De beveiligingsbaseline van de standaardconfiguratie moet worden vastgelegd. (bv. het standaard beschermen van alle externe communicatie met SSL technologie)
- Het principe bij initiële inrichting van een informatiesysteem of een infrastructuur is “gesloten, tenzij”.
- Afwijking van de initiële inrichting volgt het principe “Pas toe of leg uit.”
- Security wordt geborgd in een changemanagementproces.
- Toegang tot informatie is rol-gebaseerd, waardoor gebruikers alleen toegang hebben tot informatie en IT-faciliteiten die zij nodig hebben voor hun werkzaamheden (vastgelegd in een autorisatieschema)

Bijlage C – BIV classificatie

Classificatie geeft een inschatting van de gevoeligheid en het belang van informatie om tot een juiste mate van beveiliging te komen. Niet alle informatie is even vertrouwelijk of hoeft bij een incident even snel weer beschikbaar te zijn. Het is niet erg efficiënt of gebruiksvriendelijk om niet-vertrouwelijke informatie op dezelfde manier te beschermen als vertrouwelijke informatie.

De DG&J volgt een risico gestuurde aanpak. Het bestuur stelt eens per jaar vast wat de risicobereidheid van de organisatie is als resultaat van de jaarlijkse risicoanalyse sessies.

De classificatie van processen en systemen is bij de DG&J opgenomen in de applicatielijst. De applicatie eigenaren zijn verantwoordelijk voor het vaststellen van de BIV classificatie, waarbij zij geadviseerd en ondersteund kunnen worden door de Security Officer. De BIV classificatie bepaalt welke maatregelen van toepassing zijn en in welke mate deze geïmplementeerd moeten worden. Met een aanvullende risicoanalyse of DPIA kan de mogelijke schade worden geëvalueerd die een dreiging kan toebrengen en kunnen aanvullende maatregelen worden gedefinieerd.

Een aantal maatregelen zijn generiek en daarom niet afhankelijk van individuele BIV en privacy classificatie scores. De DG&J heeft een redelijk aantal applicaties en diensten uitbesteed en hierbij moet duidelijk zijn welke maatregelen de leverancier implementeert en welke maatregelen onder verantwoordelijkheid gebeuren van de DG&J.

Hoofdstuk 15: Leveranciersrelaties in de NEN 7510 gaat vooral over het duidelijk maken van deze verantwoordelijkheden.

Wij verwachten van leveranciers dat zij minimaal hetzelfde niveau van bescherming van (persoons-)gegevens bieden als de DG&J zelf en haar opdrachtgevers.

1.4 De BIV-classificatie BESCHIKBAARHEID

BESCHIKBAARHEID		
Laag (score: 1)	Beschikbaarheid is niet belangrijk. Algeheel verlies of niet beschikbaar zijn van deze informatie gedurende meerdere dagen brengt geen merkbare (meetbare) schade toe aan de belangen van de organisatie, haar medewerkers of haar cliënten/patiënten.	Beschikbaarheid > 95% RTO (Recovery Time Objective) = 48-168 uur, afhankelijk van de categorie informatie
Midden (score: 2)	Beschikbaarheid is belangrijk. Algeheel verlies of niet beschikbaar zijn van deze informatie gedurende een of twee dagen brengt merkbare schade toe aan de belangen van de organisatie, haar medewerkers of haar cliënten/patiënten.	Beschikbaarheid > 97% RTO= 24-48 uur, afhankelijk van de categorie informatie
Hoog(score: 3)	Beschikbaarheid is noodzakelijk. Algeheel verlies of niet beschikbaar zijn van deze informatie gedurende een werkdag brengt merkbare schade toe aan de belangen van de organisatie, haar medewerkers of cliënten/patiënten.	Beschikbaarheid > 99% RTO= 1-24 uur, afhankelijk van de categorie informatie

1.5 De BIV-classificatie INTEGRITEIT

INTEGRITEIT		
Laag (score: 1)	Integriteit is onbelangrijk. Blijvende juistheid van informatie (vanaf de bron tot het laatste gebruik) is gewenst, maar hoeft niet gegarandeerd te zijn. Indien informatie niet correct is, leidt dit tot beperkte schade.	Bedrijfsproces tolereert fouten
Midden (score: 2)	Integriteit is beschermd. Blijvende juistheid van informatie moet gewaarborgd zijn. Sommige toleranties zijn toelaatbaar. Juistheid van informatie is belangrijk, maar niet kritisch. Het is niet noodzakelijk dat correctheid onbetwistbaar aangetoond kan worden. Indien informatie niet correct is kunnen de organisatie of cliënten/patiënten substantiële schade lijden.	Een beperkt aantal fouten is toegestaan
Hoog (score: 3)	Integriteit is noodzakelijk. Informatie moet gegarandeerd correct zijn. Informatie waarbij het noodzakelijk is dat de correctheid niet betwist kan worden, zoals onomkeerbare financiële transacties. Hieronder vallen ook de registraties van de uitslagen van medische behandelingen en onderzoeken bij de juiste cliënten. Indien informatie niet correct is, kunnen de organisatie of haar cliënten/patiënten ernstige schade lijden.	Bedrijfsproces eist foutloze informatie

1.6 De BIV-classificatie VERTROUWELIJKHEID

VERTROUWELIJKHEID		
Laag (score: 1)	Informatie is voor intern gebruik. Openbaar worden van gegevens leidt tot weinig of geen schade voor de organisatie of betrokkene.	Gegevens zijn alleen in te zien en te bewerken door personen binnen de organisatie.
Midden (score: 2)	Informatie is vertrouwelijk. De organisatie of betrokkene kan substantiële schade lijden indien informatie toegankelijk is voor ongeautoriseerde personen. Informatie mag alleen toegankelijk zijn voor personen die hier vanuit hun functie toegang toe moeten hebben (need-to-know basis). Hieronder vallen onder andere persoonsgegevens.	Gegevens alleen toegankelijk voor direct betrokkenen binnen de organisatie op basis van functie of rol.
Hoog (score: 3)	Informatie is geheim. De organisatie of betrokkene kan ernstige schade lijden indien informatie toegankelijk is voor ongeautoriseerde personen. Informatie mag uitsluitend toegankelijk zijn voor een zeer geselecteerde groep personen. Hieronder vallen onder andere bijzondere (medische) persoonsgegevens.	Toegang is beperkt tot expliciet aangewezen personen binnen de organisatie. Beheerders hebben, waar mogelijk, geen toegang tot de gegevens. Beheerders maken alleen gebruik van persoonlijk herleidbare accounts. Een DPIA is verplicht bij een hoog privacy risico voor de betrokkenen.

Bijlage D – Wet- en regelgeving

Deze bijlage geeft een overzicht van de belangrijkste aan informatieveiligheid gerelateerde wet- en regelgeving met specifieke aandachtspunten voor de DG&J.

1. **Algemene Verordening Gegevensbescherming (AVG)**
   De DG&J voldoet aan de eisen in de AVG voor het beschermen van gegevens en heeft de rechten van cliënten/patiënten en andere betrokkenen vastgelegd in de privacy verklaring.
   In het applicatieoverzicht wordt geregistreerd of er (bijzondere) persoonsgegevens worden verwerkt. Naleving van het informatiebeveiligingsbeleid inclusief de daarin vermelde technische en organisatorische maatregelen zorgen samen voor het voldoen aan de AVG richtlijnen.
2. **Wettelijke Bewaartermijnen/Archiefwet**
   De DG&J houdt zich aan de wettelijke voorschriften ten aanzien van bewaartermijnen, zoals die zijn vastgelegd in specifieke wetgeving (zoals de Belastingwet en in het arbeidsrecht) en in de Archiefwet en het Archiefbesluit. De DG&J hanteert daarbij de selectielijst van de VNG. Dit selectiedocument gaat over alle informatie zoals die bijvoorbeeld is vastgelegd in (gedigitaliseerde) documenten, informatiesystemen, websites en e-mail. Dit is onderdeel van de jaarlijkse externe accountantsrapportages.
3. **Wet Computercriminaliteit III**
   De Wet Computercriminaliteit richt zich op de strafrechtelijke probleemgebieden in relatie tot het computergebruik. De wet bestaat uit artikelen die op diverse plekken zijn toegevoegd aan het Wetboek van Strafrecht. De extra artikelen houden zich bezig met:
   - Vernieling en onbruikbaar maken.
   - Aftappen van gegevens.
   - Denial of service, verstikkingsaanval.
   - Computervredebreuk.
   - Diensten afnemen zonder betalen.
   - Malware, kwaadaardige software.

   Naleving van dit Informatiebeveiligingsbeleid, met name van de beveiligingsmaatregelen en het te verwachten gedrag zorgen ervoor dat de DG&J een adequaat basisniveau van beveiliging heeft tegen deze dreigingen. Indien er aanvallen op de DG&J plaatsvinden die de beveiliging significant doorbreken en die vallen onder de Wet Computercriminaliteit, zal het bestuur van de DG&J aangifte doen.

- Baseline Informatieveiligheid Overheid (BIO)
- Informatiebeveiliging in de zorg (NEN 7510-1+A1:2020)
- De Network and Information Security directive, of NIS2-richtlijn
- Algemene Verordening Gegevensbescherming (AVG)
- Basisregistratie Personen (BRP)
- Landelijk Register Zorgaanbieders (LRZA)
- Besluit elektronische gegevensverwerking door zorgaanbieders
- Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg
- Wet op de geneeskundige behandelovereenkomst (WGBO)
- Wet op de beroepen in de individuele gezondheidszorg (Wet BIG)
- Wet kwaliteit, klachten en geschillen zorg (Wkkgz)
- Wet cliëntenrechten zorg (Wcz)
- Ambtenarenwet
- Wet Open Overheid (WOO)
- Jeugdwet (JW)

- Meldplicht datalekken
- Nieuwe Wet maatschappelijke ondersteuning (nieuwe Wmo)
- Wet Publieke Gezondheid (WPG)

Het informatiebeveiligingsbeleid bij de DG&J is gebaseerd op het NEN 7510-1+A1:2020 normenkader.

Bijlage E – Beleid bescherming persoonsgegevens

Zie Qlink: http://dgjzhz.qlink.biz/qlinkBook.aspx?idd=4&idp=28&id=4010&retpor=4_28

Bijlage F – Maatregelen overzicht vanuit NEN 7510-1+A1:2020

Zie ISOPlanner.

Bijlage G – Vulnerability Disclosure

Zie website DG&J:
Dienst Gezondheid & Jeugd - Coordinated Vulnerability Disclosure (dienstgezondheidjeugd.nl)

dienstGezondheid & Jeugd zhz

Karel Lotsyweg 40
Postbus 166, 3300 AD Dordrecht

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