Beweging 3.0

Auteur(s)

Dick van Mourik
Security- & Privacy Officer

Beleid Informatiebeveiliging, Privacybescherming en Cyberveiligheid

Beweging 3.0
Postbus 2633
3800 GD Amersfoort
T +31 (0)6 20 17 00 79
E Dick.vanMourik@beweging3.nl
www.beweging3.nl

Bezoekadres:
Basicweg 24
3821 BR Amersfoort

Colofon

Titel	Beleid Informatiebeveiliging, Privacybescherming en Cyberveiligheid
Versie	4.0
Auteur(s)	Dick van Mourik
Geraadpleegde bronnen	Informatiebeveiligingsbeleid v3.0 NEN 7510-1/2:2017 NEN 7512:2015 NEN 7513:2018 NTA 7516 Algemene verordening gegevensbescherming (AVG)

Versiebeheer

Versie	Referentie	Wijziging(en)
1.0	**DM-IBB19**	**Vastgesteld door RvB dd. 29-10-2019**
2.0	DM-IBB20	Geen wijzigingen
3.0	DM-IBB22	Diverse aanpassingen, zie 1.5 (Wijzigingen) **Vastgesteld door RvB dd. 13-6-2022**
4.0	13-9-2023	Vastgesteld door RvB dd. 4-9-2023 Ter informatie aangeboden aan de RvT op 12-9-2023

Inhoudsopgave

1 Inleiding 4
1.1 Leeswijzer 4
1.2 Doelstelling 4
1.3 Reikwijdte 5
1.4 Evaluatie 5
1.5 Wijzigingen versie 4.0 5
2 Risicomanagement 6
3 Managementsysteem voor informatiebeveiliging en privacy 6
4 Gedragen beleid 7
5 De organisatie van informatiebeveiliging binnen Beweging 3.0 7
5.1 Rollen en verantwoordelijkheden 7
5.2 Externe contacten 8
5.3 Informatiebeveiliging in projectbeheer 9
6 Classificatie van data 10
7 Personeel en informatiebeveiliging 10
7.1 Voorafgaand aan het dienstverband 10
7.2 Tijdens het dienstverband 11
7.2.1 Bewustwording 11
7.2.2 Gedragscode en disciplinaire procedure 11
7.2.3 Thuiswerken 12
7.3 Beëindiging van het dienstverband 12
8 Beheer van bedrijfsmiddelen 12
9 Beveiliging van informatie 13
9.1 Software en systemen 13
9.2 Kwetsbaarhedenbeheer en cyberveiligheid 13
9.3 Fysieke beveiliging 14
9.4 Bedrijfsvoering 14
9.4.1 Gedelegeerde verantwoordelijkheden 14
9.4.2 Beweging 3.0-verantwoordelijkheden 15
9.5 Communicatiebeveiliging 15
9.6 Cryptografie 16
10 Leveranciersmanagement 16
10.1 Acquisitie van informatiesystemen 16
10.2 Leveranciersrelaties 16
11 Beheer van beveiligingsincidenten 17
12 Continuïteit 17
13 Naleving 18
13.1 Wettelijke en contractuele eisen (extern) 18
13.2 Interne regelgeving en audits 19
13.3 Toetsing van het beleid en de doelstelling 19

1 Inleiding

Beweging 3.0 ziet het als haar missie om het leven van bewoners en cliënten en het werk van haar medewerkers zo aangenaam mogelijk te maken: aangenaam leven, aangenaam wonen, aangenaam werken. Een belangrijke voorwaarde voor het waarmaken van deze visie is het vertrouwen dat informatie, waaronder ook (bijzondere en gevoelige) persoonsgegevens, juist verwerkt, beheerst en beschermd wordt. Incidenten op het gebied van de beveiliging van persoonsgegevens kunnen nadelige gevolgen hebben voor de betrokkenen en de organisatie. Ontwikkelingen en dreigingen op het gebied van kunstmatige intelligentie, zorgtechnieken en -innovatie, data- en informatiemanagement en cybercriminaliteit maken het toepassen van een gedegen beleid op het gebied van informatiebeveiliging, privacybescherming en cyberveiligheid urgenter dan ooit.

Dit document beschrijft het beleid ten aanzien van informatiebeveiliging, privacybescherming en cyberveiligheid (verder IPC). Belangrijk uitgangspunt bij het vaststellen van dit beleid en de opgenomen maatregelen is, dat beveiligingsmaatregelen voor zover mogelijk zorgprocessen niet in de weg staan. Vanuit een pragmatisch oogpunt is in dit beleid aandacht voor zowel strategische als tactische aspecten. Dit beleid wordt beheerd door de Security- & Privacy Officer en wordt minimaal eens per drie jaar (of eerder indien ontwikkelingen hierom vragen) herzien.

1.1 Leeswijzer

Dit beleid is onlosmakelijk verbonden met het managementsysteem voor informatiebeveiliging en privacy (P/IMS). Het volgt de hoofdstukindeling van NEN7510-2:2017, de norm voor informatiebeveiliging in de zorg. Om de koppeling tussen dit beleid en de norm inzichtelijk te maken, worden bij aanvang van hoofdstukken en/of paragrafen de corresponderende paragrafen uit de NEN-norm genoemd. Hierbij wordt uitgegaan van de NEN 7510-2:2017, tenzij anders vermeld. Daarnaast wordt per onderwerp een verantwoordelijke benoemd.

Bij vragen of opmerkingen kan contact opgenomen worden met:
Dick van Mourik
Security- & Privacy Officer
Tel.: +31 (0)6 20170079

1.2 Doelstelling

Informatieveiligheid richt zich op de beschikbaarheid, integriteit en vertrouwelijkheid (BIV) van informatie.

Door middel van dit beleid wil Beweging 3.0 richtlijnen vaststellen over hoe binnen de organisatie omgegaan dient te worden met deze BIV-uitgangspunten om zo risico's op het gebied van onder andere privacy, cybercriminaliteit en fraude te beheersen. Deze algemene doelstelling levert, vertaald naar de kernwaarden van betrokken en professioneel handelen, de volgende strategische doelstelling op ten aanzien van informatiebeveiliging:

Informatie wordt adequaat beveiligd en alle medewerkers (intern en extern), vrijwilligers en leveranciers gaan professioneel en bewust om met informatie en respecteren de privacy van anderen. Op deze manier kan Beweging 3.0, ook ten aanzien van de verwerking en beheer van

informatie en persoonsgegevens, een betrouwbare zorgpartner zijn voor haar cliënten en stakeholders.

Met het opstellen van dit beleid wordt tevens invulling gegeven aan NEN 7510-2:2017 en hieruit voortvloeiende normen die betrekking hebben op informatiebeveiliging in de zorg én kan Beweging 3.0 aantonen dat wordt voldaan aan de Algemene verordening gegevensbescherming (AVG).

1.3 Reikwijdte

Waar in dit beleid wordt geschreven over Beweging 3.0 wordt, tenzij expliciet anders aangeven, iedere organisatie bedoeld die onderdeel uit maakt van de organisatie, te weten Beweging 3.0, Indebuurt033, Leef3.nu en Welzin.

Het Beleid Informatiebeveiliging is ook van toepassing op de informatie-uitwisseling en/of –verwerking van bovenstaande afzonderlijke entiteiten met andere organisaties, zoals:

- Organisaties, waar (een gedeelte van de) informatiesystemen geoutsourcet zijn;
- Ketenpartners (gemeenten, zorgkantoren, ziekenhuizen, etc.);
- Organisaties die diensten van Beweging 3.0 afnemen of diensten leveren en in aanraking komen met gegevensverwerkingen.

Tot slot richt het Beleid Informatiebeveiliging zich op eigen medewerkers en vrijwilligers, tijdelijk personeel en personeel dat door derden wordt ingezet om diensten te verlenen aan (onderdelen van) Beweging 3.0, alsmede ook voor uitbestede diensten (o.a. ICT). Voor het gemak en de leesbaarheid van dit document wordt deze groep verder aangeduid met de term ‘medewerker’ of ‘medewerkers’. Het beleid is ook van toepassing op personen, die gebruik maken van huisvesting en/of ICT-voorzieningen van onderdelen van Beweging 3.0.

1.4 Evaluatie

Dit beleid wordt ten minst eens per 3 jaren beoordeeld en, bij wijzigingen, opnieuw vastgesteld door de Raad van Bestuur (verder: RvB). Tussentijdse herziening is mogelijk als hiertoe aanleiding is. Bewaking vindt plaats via de Compliance jaarplanning. De jaarplanning wordt jaarlijks vastgesteld door de RvB.

1.5 Wijzigingen versie 4.0

In de titel van het document is expliciet gemaakt dat het beleid betrekking heeft op Informatiebeveiliging, Privacybescherming én Cyberveiligheid. Ten aanzien van dit laatste onderwerp zijn maatregelen toegevoegd, onder andere in de vorm van de toevoeging van paragraaf 9.2 (Kwetsbaarhedenbeheer en cyberveiligheid) en het nogmaals benoemen van Cyber Incident respons onder hoofdstuk 12 (Continuïteit). Daarnaast zijn onderwerpen en teksten vereenvoudigd en is meer verwezen naar andere documenten waarin specifieke richtlijnen zijn opgenomen.

2 Risicomanagement

Verantwoordelijke	Security- & Privacy Officer | Compliance Officer
NEN 7510 norm	NEN 7510-1:2017

Vanwege het type informatie dat binnen Beweging 3.0 wordt verwerkt, is het noodzakelijk om een beeld te hebben van de risico's en deze procesmatig te beheersen. Risico's, hun ernst en de werking van getroffen beheersmaatregelen dienen periodiek geëvalueerd te worden (PDCA). Opzet, bestaan en werking van beheersmaatregelen worden getoetst door middel van interne audits op het P/IMS. Bevindingen worden geregistreerd in een verbeterregister en besproken in het Beraad Informatieveiligheid (zie 5.1). Hieruit voortvloeiende acties en hun voortgang worden door de Security- & Privacy Officer gemonitord.

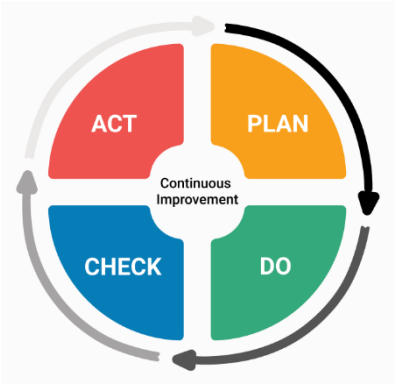
Gerelateerde documenten:

- Beleid Interne Audits
- IPC-PIMS_03_Risicobeoordeling van informatiebeveiliging
- IPC-REG_Verbeterregister
- IPC-RAP_Stavaza Informatie IT cyberveiligheid

3 Managementsysteem voor informatiebeveiliging en privacy

Verantwoordelijke	Security- & Privacy Officer
NEN 7510 norm	NEN 7510-1:2017

Om onder andere risico's, beheersmaatregelen en verbetermaatregelen en daarmee het risicomanagement centraal te beheren, heeft Beweging 3.0 een managementsysteem voor informatiebeveiliging en privacy (P/IMS) ingericht. Vanuit het P/IMS wordt de informatiebeveiliging binnen de organisatie gestuurd en bestuurd. Dit gebeurt voor een deel via de richtlijnen voor risicobeheersing (zie vorig hoofdstuk). Belangrijk hierbij is het volgen van de Plan-Do-Check-Act-cyclus, waarbij continu anticiperen, toetsen en verbeteren het uitgangspunt is.



Het P/IMS bevat onder andere informatie over risico's, getroffen beheersmaatregelen en bijbehorende controls, een verbeterregister en een jaarplanning ten behoeve van informatiebeveiliging. Het beheer van het P/IMS is de verantwoordelijkheid van de SPO en vormt onder andere de basis voor interne (voortgangs)rapportages aan de RvB en de Auditcommissie van de Raad van Toezicht (verder: RvT).

Gerelateerde documenten:

- IPC-PIMS_06 PIMS Handboek
- Diverse documenten, zoals o.a. Toepassingsgebied, Context van de organisatie, Verklaring van Toepasselijkheid. Zie verder SharePoint.

4 Gedragen beleid

Verantwoordelijke	Raad van Bestuur | Security- & Privacy Officer		
NEN 7510 norm	5.1.1	5.1.2	7.2.1

De RvB van Beweging 3.0 is eindverantwoordelijk voor het Beleid IPC en neemt een actieve rol bij de uitvoering. De verantwoordelijkheid voor het samenstellen, implementeren en uitvoeren van het beleid en de hieruit voortvloeiende processen wordt door de RvB gedelegeerd naar de SPO. De SPO rapporteert aan de RvB en de Auditcommissie van de RvT. De RvB zal door middel van een directiebeoordeling de kwaliteit van het P/IMS en de werking van de PDCA-cyclus toetsen. Hierin worden alle aspecten van het P/IMS meegenomen.

Het Beleid Informatiebeveiliging wordt ten minste eens per drie jaar herzien, waarbij toetsing plaatsvindt ten aanzien van het voldoen aan relevante wet- en regelgeving, de eisen die worden gesteld aan de organisatie als gevolg van de uitgevoerde werkzaamheden en eventuele veranderingen in de omgeving (wensen van klanten). In dit beleid worden deze vereisten vertaald naar beleidsregels die, na goedkeuring door de RvB, via publicatie op intranet kenbaar worden gemaakt bij de gehele organisatie.

5 De organisatie van informatiebeveiliging binnen Beweging 3.0

5.1 Rollen en verantwoordelijkheden

Verantwoordelijke	Security- & Privacy Officer	
NEN 7510 norm	6.1.1	6.1.2

Hoewel de volledige organisatie te maken heeft met informatiebeveiliging, hebben sommige rollen en functies hierin specifieke verantwoordelijkheden of bevoegdheden. Dit betreft:

- Raad van Bestuur
- Security- & Privacy Officer
- Functionaris Gegevensbescherming
- Management
- Beraad Informatieveiligheid

Raad van Bestuur
De Raad van Bestuur (RvB) is eindverantwoordelijk voor het vaststellen en uitvoeren van dit beleid. De uitvoering van het beleid is belegd in de organisatie. Toezicht hierop is door de RvB gedelegeerd aan de Security- & Privacy Officer. De RvB verantwoordt zich aan de Raad van Toezicht (RvT).

Security- & Privacy Officer
De Security- & Privacy Officer vormt het eerste aanspreekpunt, beantwoordt vragen en adviseert de RvB, het management en de medewerkers over informatiebeveiliging, privacy en cyberveiligheid. Taken en verantwoordelijkheden staan beschreven in het document *Verantwoordelijkheden privacy en informatiebeveiliging*, te vinden in het Document Management Systeem (DMS).

De Security maakt deel uit van de compliance functie en valt hiërarchisch onder de Manager Finance & Control. De Security- & Privacy Officer rapporteert direct aan de portefeuillehouder binnen de RvB en de Auditcommissie van de RvT.

Functionaris Gegevensbescherming
Naast de Security- & Privacy Officer, die belast is met het houden van toezicht op het naleven van de interne beleidsregels met betrekking tot informatiebeveiliging en advisering over privacyvraagstukken in de eerste lijn, beschikt Beweging 3.0 over een (externe) Functionaris Gegevensbescherming (FG). Deze houdt toezicht op de naleving van de privacywetgeving. Waar de functies van deze functionarissen elkaar qua taken overlappen, zijn afspraken gemaakt over de concrete invulling hiervan. Deze afspraken zijn vastgelegd in een beleidsdocument.

Management
Het management is *op operationeel niveau* verantwoordelijk voor het implementeren van de benodigde maatregelen voortvloeiend uit de risicoanalyse, het toezien op de naleving van dit Beleid Informatiebeveiliging door de (eigen) organisatieonderdelen en het evalueren en verbeteren van de toepassing en werking van het beleid op basis van rapportages over informatiebeveiliging. Daarnaast wordt van het management verwacht:

- een beschikbaar budget voor de uitvoering van maatregelen ten einde risico's van informatiebeveiliging tot een acceptabel niveau te mitigeren;
- een positieve en actieve houding ten aanzien van informatiebeveiliging;
- fungeren als voorbeeldfunctie;
- toezicht houden op de naleving van Informatiebeveiligingsmaatregelen;
- medewerking verlenen aan verbeteracties;
- informatiebeveiliging behandelen in werkoverleg, beoordelingen etc.

Beraad Informatieveiligheid
Eens per kwartaal komt het Beraad Informatieveiligheid bijeen om onderwerpen met betrekking tot informatiebeveiliging, privacy en cyberveiligheid te bespreken en te beoordelen.

Gerelateerde documenten:

- Verantwoordelijkheden privacy en informatiebeveiliging

5.2 Externe contacten

Verantwoordelijke	Diverse, zie tabel	
NEN 7510 norm	6.1.3	6.1.4

In diverse gevallen is het noodzakelijk contact op te nemen met externe organisaties (bijv. politie, regelgevende organen, toezichthouders). In onderstaand schema ligt vast wie in welke situatie contact opneemt met relevante organisaties. Op intranet is onder 'calamiteiten' een volledig overzicht te vinden van contactgegevens.

Type Incident	Verantwoordelijke	Instantie	Opmerkingen
Ongeval	BHV	Alarmdienst 112 Inspectie SZW	Een ongevallen registratie ligt bij BHV. Bij ongeval wordt 112 gebeld.

			Afhankelijk van het ongeval kan dit ertoe leiden dat de Inspectie SWZ wordt benaderd.
Brand	Receptie	Brandweer	Bij brand dient te allen tijde de brandweer te worden benaderd. Dit zal hoofdzakelijk via gebouwbeheer en de eigen receptie lopen.
Diefstal, inbraak	Backoffice FM	Politie	Bij ontvreemding van bedrijfs- en/of persoonseigendommen van personeel, bewoners of bezoekers van Beweging 3.0 wordt de politie ingeschakeld.
Incidenten Zorg	BK, manager en RvB	Inspectie Gezondheidszorg en Jeugd (IGJ) Nederlandse Zorgautoriteit (NZa)	Bij meldingen/klachten over de kwaliteit van zorg
Informatiebeveiligings- en privacy gerelateerde incidenten	Security- & Privacy Officer	Autoriteit Persoonsgegevens, AFM, Politie	Afhankelijk van het type incident, kan contact worden opgenomen met meerdere overheidsinstanties.

Beweging 3.0 heeft er op dit moment voor gekozen om zich ten aanzien van informatiebeveiliging niet aan te sluiten bij speciale belangengroepen. Wel is de Security- & Privacy Officer geabonneerd op nieuwsbrieven en fora en volgt deze actief LinkedIngroepen op het gebied van informatiebeveiliging, privacy en bewustwording om nieuwe ontwikkelingen te volgen. Voor de implementatie van en toezicht op de naleving van de Algemene verordening gegevensbescherming (o.a. de FG-rol) wordt gebruik gemaakt van de expertise van AVG Juristen. Via deze organisatie kan ook gebruik gemaakt worden van een kennisbank en juridische toetsing.

5.3 Informatiebeveiliging in projectbeheer

Verantwoordelijke	Programma Manager
NEN 7510 norm	6.1.5

Om te borgen dat bij ieder project aandacht wordt besteed aan informatiebeveiliging en privacyaspecten, wordt de compliance functie actief betrokken bij (nieuwe) projecten. Indien noodzakelijk betrekt de Security- & Privacy Officer de FG bij het project. Indien nodig wordt een Data Protection Impact Assessment (DPIA) uitgevoerd. Eventuele bevindingen of verbetermaatregelen worden vastgelegd in de verbetermatrix in het P/IMS.

6 Classificatie van data

Verantwoordelijke	Security- & Privacy Officer
NEN 7510 norm	8.2

Beweging 3.0 verwerkt gevoelige en vertrouwelijke gegevens. Verschillende typen informatie dienen op verschillende wijzen te worden beschermd. Hiervoor heeft Beweging 3.0 het volgende data-classificatieschema opgesteld, welke tevens de bron is voor de inrichting van het DMS:

Classificatie	Type	Beschrijving
0	Publiek	Informatie toegankelijk voor iedereen. Deze bevat geen vertrouwelijke informatie en mag gedeeld worden buiten de organisatie.
I	Intern	Informatie toegankelijk voor iedereen binnen de organisatie. Deze bevat organisatie specifieke informatie en mag niet gedeeld worden met personen buiten de organisatie die niet door middel van een (opdracht)overeenkomst aan Beweging 3.0 verbonden zijn, tenzij hiervoor expliciet toestemming is gegeven door de informatie-eigenaar.
II	Vertrouwelijk	Informatie toegankelijk voor een selecte groep medewerkers. Deze bevat zeer gevoelige informatie en mag niet gedeeld worden buiten deze groep, tenzij hiervoor expliciet toestemming is gegeven door de eigenaar.

Persoonsgegevens vallen binnen de groep “Vertrouwelijk” en worden alleen verwerkt in daarvoor bestemde beveiligde applicaties, zoals het Elektronisch Cliëntendossier.

Bij de samenstelling van de tabel is bewust gekozen voor een zo beperkt mogelijk aantal opties en een zo algemeen mogelijke beschrijving.

7 Personeel en informatiebeveiliging

Zoals in paragraaf 5.1 aangegeven raakt informatiebeveiliging iedereen. Niet alleen een aantal specifieke functies. Een aantal beheersmaatregelen heeft betrekking op (gedrag en instructie van) personeel. Deze worden in dit hoofdstuk behandeld.

7.1 Voorafgaand aan het dienstverband

Verantwoordelijke	Manager HRMD		
NEN 7510 norm	7.1.1	7.1.2	13.2.4

Voordat een medewerker in dienst treedt bij Beweging 3.0 wordt deze gescreend. Voor alle medewerkers worden, voor zover mogelijk en realistisch, controles uitgevoerd ten aanzien van de volledigheid van het CV, de juistheid van aanwezige kwalificaties, de identiteit, referenties en de afwezigheid van dringende redenen om de sollicitant niet aan te nemen.

Indien van toepassing voor de functie kunnen aanvullende eisen gesteld worden aan het screeningsproces, zoals de BIG-registratie.

Voorafgaande aan het uitvoeren van de werkzaamheden dient de nieuwe medewerker de arbeidsovereenkomst getekend te hebben. Hierin wordt verwezen naar diverse onderwerpen en documenten aangaande informatiebeveiliging.

Voor ingehuurd personeel, zoals externe contractanten en ZZP'ers, en vrijwilligers geldt, dat zij voordat de werkzaamheden voor Beweging 3.0 aanvangen, een geheimhoudingsverklaring dienen te tekenen. Deze verklaring wordt centraal, in het personeelsinformatiesysteem, opgeslagen.

Gerelateerde documenten:

- Arbeidsovereenkomst
- Gedragscode
- Geheimhoudingsverklaring
- Wegwijzers nieuwe medewerker

7.2 Tijdens het dienstverband

7.2.1 Bewustwording

Verantwoordelijke	Security- & Privacy Officer
NEN 7510 norm	7.2.2

Medewerkers van Beweging 3.0 worden periodiek, maar ten minste eens per jaar, op de hoogte gebracht van het organisatiebeleid ten aanzien van informatiebeveiliging en privacy. De wijze waarop dit gebeurt, staat beschreven in het Bewustwordingsprogramma. Dit programma wordt ten minste eens per drie jaren door de Security- & Privacy Officer herzien op basis van wensen en behoeften van de organisatie en vervolgens vastgesteld door de RvB.

Gerelateerde documenten:

- Programma Bewustwording

7.2.2 Gedragscode en disciplinaire procedure

Verantwoordelijke	Manager HRMD			
NEN 7510 norm	7.2.3	11.2.6	11.2.8	11.2.9

Relevante beleidsregels op het gebied van informatiebeveiliging die zijn gericht op het gedrag van de medewerkers zijn vastgelegd in de *Gedragscode*. Medewerkers van Beweging 3.0 worden verondersteld deze te kennen. Bij overtreding van de Gedragscode en/of andere beleidsregels van de organisatie, kan een disciplinair procedure (zoals opgenomen in de Gedragscode) worden gestart.

Gerelateerde documenten:

- Gedragscode

7.2.3 Thuiswerken

Verantwoordelijke	Manager HRMD | Manager ICT
NEN 7510 norm	6.2.2

Ten behoeve van het werken op andere locaties dan de locaties van Beweging 3.0 is een beleid opgesteld. Dit beleid staat beschreven in het document *Plaatsonafhankelijk E werken (thuiswerken)*. Bepalingen uit de Gedragscode zijn hierin ook van belang.

Technische beveiliging van informatie wordt afgedwongen binnen de digitale werkomgeving van Beweging 3.0, waarvoor richtlijnen zijn opgenomen in het opgestelde *Beleid Logische Toegangsbeveiliging*, het *Beleid Wachtwoorden*, het *Beleid Beheer Bedrijfsmiddelen* en diverse inrichtingsdocumenten gericht op IT security.

Gerelateerde documenten:

- Beleid Plaatsonafhankelijk E werken (thuiswerken)
- Beleid Logische Toegangsbeveiliging
- Beleid Wachtwoorden
- Beleid Beheer Bedrijfsmiddelen
- Diverse documenten t.b.v. de inrichting van de digitale werkplek en infrastructuur

7.3 Beëindiging van het dienstverband

Verantwoordelijke	Manager HRMD
NEN 7510 norm	7.3.1

Geheimhouding en het zorgvuldig omgaan met informatie en gegevens die betrekking hebben op Beweging 3.0, haar cliënten, medewerkers, en contactpersonen, geldt ook na beëindiging van het dienstverband. Dit is opgenomen in de arbeidsovereenkomst.

Hoewel vrijwilligers geen arbeidsovereenkomst ontvangen, dienen ook zij te tekenen voor geheimhouding. In betreffende verklaring is opgenomen dat geheimhouding ook na beëindiging van de (vrijwillige) werkzaamheden blijft gelden.

8 Beheer van bedrijfsmiddelen

Verantwoordelijke	Manager ICT | Manager H&F | Security- & Privacy Officer							
NEN 7510 norm	6.2.1	8.1.1	8.1.2	8.1.3	8.1.4	8.2.1	8.2.2	8.2.3
	8.3.1	8.3.2	8.3.3	11.2.1	11.2.2	11.2.3	11.2.4	
	11.2.5	11.2.6	11.2.7	11.2.8	11.2.9	12.5.1	12.6.2	

Beweging 3.0 heeft richtlijnen en verantwoordelijkheden ten aanzien van het beheer van bedrijfsmiddelen vastgelegd in het Beleid Beheer Bedrijfsmiddelen. Dit beleid is gebaseerd op het gelijknamige hoofdstuk uit de NEN-norm, aangevuld met een aantal gerelateerde onderwerpen.

Voor de volledigheid is in hetzelfde beleid aandacht besteed aan richtlijnen voor de beveiliging van apparatuur. De beveiliging van software, wat ook een bedrijfsmiddel is, wordt beschreven in een separaat beleid. Zie ook hoofdstuk 9, paragraaf 1.

Gerelateerde documenten:

- Beleid Beheer Bedrijfsmiddelen
- Beleid Persona en Middelen matrix

9 Beveiliging van informatie

Informatie wordt op verschillende wijzen beveiligd, zowel softwarematig, als fysiek door (technische) beveiliging van apparatuur en de plaatsen waar deze apparatuur wordt gebruikt. De beveiliging van apparatuur wordt buiten beschouwing gelaten, dit wordt beschreven in hoofdstuk 8.

9.1 Software en systemen

Verantwoordelijke	Manager ICT | Security- & Privacy Officer					
NEN 7510 norm	9.1.1	9.1.2	9.2.1	9.2.2	9.2.3	9.2.4
	9.2.5	9.2.6	9.3.1	9.4.1	9.4.2	9.4.3

Richtlijnen en procedures ten aanzien van de toegang tot applicaties en systemen liggen vast in het *Beleid Logische Toegangsbeveiliging*. Beleid en procedures hebben niet alleen betrekking op het verstrekken, wijzigen en intrekken van toegang, maar bevatten ook richtlijnen ten aanzien van periodieke controles op het gebied van autorisatieprocessen en bijbehorende autorisatiematrixen. Regels met betrekking tot het gebruiken en beheren van wachtwoorden zijn opgenomen in *Beleid Wachtwoorden*.

Waar technische beveiligingsmaatregelen, waaronder wachtwoordeisen, onder de verantwoordelijkheid van softwareleveranciers vallen, wordt beoordeling en toetsing van deze maatregelen verder beschreven in hoofdstuk 10 ‘Leveranciersbeheer’.

Gerelateerde documenten:

- Beleid Logische Toegangsbeveiliging
- Beleid Wachtwoorden
- Diverse documenten t.b.v. de inrichting van de digitale werkplek en infrastructuur

9.2 Kwetsbaarhedenbeheer en cyberveiligheid

Verantwoordelijke	Manager ICT | Security- & Privacy Officer
NEN 7510 norm	18.2.3

Ten behoeve van het beoordelen van de staat van beveiliging en de naleving van technische maatregelen voert Beweging 3.0 periodiek gerichte kwetsbaarhedenscans uit en laat zij eens per jaar de website en digitale werkomgeving door middel van een penetratietest onderzoeken. Eventuele afwijkingen en bevindingen worden besproken in het Beraad Informatiebeveiliging en opgenomen in het verbeterregister. Van daaruit wordt opvolging gemonitord.

Daarnaast is Beweging 3.0 aangesloten bij Z-CERT een csirt (computer security incident response team) voor de zorg. Z-CERT informeert aangesloten zorginstellingen over kwetsbaarheden die invloed kunnen hebben op zorg gerelateerde toepassingen.

Ten behoeve van cyberveiligheid is tevens een *Cyber Incident Respons* plan opgesteld, welke is vastgesteld door de RvB. Dit plan wordt eens per drie jaar herzien, tenzij ontwikkelingen eerder tot wijzigingen leiden. Het Cyber Incident Respons plan wordt jaarlijks geoefend.

Gerelateerde documenten:

- Cyber Incident Response plan

9.3 Fysieke beveiliging

Verantwoordelijke	Manager H&F | Coördinator Veiligheid | Security- & Privacy Officer					
NEN 7510 norm	11.1.1	11.1.2	11.1.3	11.1.4	11.1.5	11.1.6

Informatiebeveiliging heeft niet alleen betrekking op de inrichting van beveiliging van software en andere bedrijfsmiddelen. Ook de wijze waarop locaties worden beveiligd zijn van belang. Dit staat beschreven in het *Beleid Fysieke Toegangsbeveiliging*, welke wordt beheerd door Huisvesting & Facilitair.

Gerelateerde documenten:

- Beleid Fysieke Toegangsbeveiliging

9.4 Bedrijfsvoering

9.4.1 Gedelegeerde verantwoordelijkheden

Verantwoordelijke	Manager ICT | Compliance Officer | Security- & Privacy Officer				
NEN 7510 norm	12.1.3	12.1.4	12.2.1	12.3.1	12.4.1
	12.4.2	12.4.3	12.4.4	12.6.1	

Diverse onderwerpen ten aanzien van beveiliging van de bedrijfsvoering zijn onderdeel van diensten die zijn ingekocht bij leveranciers. Hiermee is sprake van een gedelegeerde (en daarmee gedeelde) verantwoordelijkheid, waarbij Beweging 3.0 met name een controlerende functie heeft.

Het gaat hierbij onder andere om ICT-diensten, capaciteitsbeheer, de scheiding van omgevingen, beheersmaatregelen tegen malware, de back-up van informatie, logging en het beheer van kwetsbaarheden. Afspraken met betrekking tot deze onderwerpen worden vastgelegd in Service Level Agreements (SLA's, zie ook hoofdstuk 10). Via rapportages (schriftelijk en mondeling) vindt monitoring plaats.

9.4.2 Beweging 3.0-verantwoordelijkheden

Verantwoordelijke	Compliance Officer | Security- & Privacy Officer		
NEN 7510 norm	12.1.1	12.1.2	12.7.1

Bedieningsprocedures zijn, waar nodig, beschreven in diverse beleidsdocumenten en procedures en worden ter beschikking gesteld aan medewerkers via intranet of op basis van het need-to-know en need-to-use principe. Voor een deel zijn deze belegd in de *Gedragscode* en het beleid *Plaatsonafhankelijk E werken*. Waar het gaat om bedieningsprocedures met betrekking tot het maken van back-ups en het onderhouden van apparatuur, staat een en ander beschreven in dit document en het Beleid Beheer Bedrijfsmiddelen.

Veranderingen in de organisatie, bedrijfsprocessen, informatie verwerkende faciliteiten en systemen die van invloed zijn op de informatiebeveiliging worden beheerst door de aansluiting met projectbeheer en de instelling van regie- en stuurgroepen. Wijzigingen ten aanzien van (ingekochte) software verlopen via een hiervoor ontwikkeld beleid en wijzigingsprocedure. Beweging 3.0 ontwikkelt zelf geen software. Eisen ten aanzien van de beveiliging en het beheer van software zijn opgenomen in documentatie ten aanzien van Leveranciersmanagement.

Beweging 3.0 heeft diverse risico's, beheersmaatregelen en controles benoemd, welke zijn vastgelegd in het P/IMS. Ten aanzien van de beheersmaatregelen en controles vindt periodieke toetsing plaats op opzet, bestaan en werking conform het Beleid Interne Audit.

Gerelateerde documenten:

- Gedragscode
- Plaats onafhankelijk E werken
- Beleid Beheer Bedrijfsmiddelen
- Beleid Interne Audit

9.5 Communicatiebeveiliging

Verantwoordelijke	Manager ICT | Inkoop						
NEN 7510 norm	13.1.1	13.1.2	13.1.3	13.2.1	13.2.2	13.2.3	14.1.2
	NEN 7512:2015				NTA 7516:2019		

Beheersmaatregelen ten behoeve van het borgen van de veiligheid van informatie in netwerken en de bescherming tegen onbevoegde toegang zijn uitbesteed aan KPN voor wat betreft algemeen netwerkbeheer, Simac (cloud werkomgeving en serverbeheer) en diverse softwareleveranciers voor wat betreft SaaS-oplossingen. Afspraken zijn vastgelegd in Service Level Agreements. Binnen Beweging 3.0 wordt voor opslag en verwerking van informatie geen gebruik gemaakt van openbare netwerken.

De uitwisseling van informatie vindt, waar mogelijk, softwarematig plaats door middel van koppelingen tussen applicaties, waarbij gegevens beveiligd en versleuteld worden verzonden. Voor het delen van informatie met andere partijen via e-mail of andere media worden medewerkers van Beweging 3.0 gehouden aan de richtlijnen ten aanzien van 'Veilig mailen' die zijn vastgelegd in de Gedragscode en de Werkinstructie veilig mailen.

In overeenkomsten en verwerkersovereenkomsten worden leveranciers gehouden aan afspraken ten aanzien van het veilig uitwisselen van persoonsgegevens. Ten aanzien van verwerkersovereenkomsten is een proces opgesteld waarvan de Inkoper van Beweging 3.0 eigenaar is. Waar het elektronisch verzenden van persoonsgegevens naar andere partijen noodzakelijk is en niet via een beveiligde koppeling mogelijk is, maakt Beweging 3.0 gebruik van ZorgMail, een toepassing die beveiligd en versleuteld mailen mogelijk maakt en de intentie heeft afgegeven zich te committeren aan de regels die middels NTA 7516:2019 worden gesteld aan veilig e-mailen en chatapplicaties.

Intern e-mailverkeer is beveiligd. Daarnaast geldt de afspraak dat vertrouwelijke en kritische informatie niet wordt gedeeld via chatapplicaties, tenzij deze onderdeel uit maken van de beveiligde applicaties die reeds in gebruik zijn.

Gerelateerde documenten:

- Gedragscode
- Werkinstructie veilig mailen

9.6 Cryptografie

Verantwoordelijke	Manager ICT		
NEN 7510 norm	10.1.1	10.1.2	18.1.5

Beweging 3.0 past cryptografische maatregelen toe om informatie op devices en de uitwisseling van gegevens te versleutelen. Bij nieuwe projecten is het bepalen van informatiebeveiligingseisen vast onderdeel, waaronder ook het uitvoeren van een DPIA. Op basis van het project en de verwerking van informatie wordt bepaald in hoeverre cryptografie dient plaats te vinden.

10 Leveranciersmanagement

10.1 Acquisitie van informatiesystemen

Verantwoordelijke	Inkoop | Security- & Privacy Officer					
NEN 7510 norm	14.1.1	14.1.2	14.1.3	14.2.2	14.2.3	14.2.4
	14.2.5	14.2.7	14.2.8	14.2.9	14.3.1	

Beweging 3.0 ontwikkelt zelf geen software. Wanneer een softwarebehoefte bestaat voor de verwerking van informatie (waaronder ook persoonsgegevens) en hiervoor nog geen oplossing beschikbaar is, dan worden de mogelijkheden onderzocht via een project. Hierbij is aandacht voor maatregelen ten behoeve van de beheersing van risico's op het gebied van informatiebeveiliging, privacy en cyberveiligheid. Op deze onderwerpen wordt een beoordeling uitgevoerd door de SPO.

Wanneer er sprake is van de verwerking van persoonsgegevens in de zin van de AVG, dan zal indien nodig een DPIA uitgevoerd worden. Dit is verankerd in projectbeheer (zie 5.3).

10.2 Leveranciersrelaties

Verantwoordelijke	Inkoop | Security- & Privacy Officer		
NEN 7510 norm	15.1.1	15.1.2	15.1.3
	15.2.1	15.2.2	

Beweging 3.0 maakt afspraken met leveranciers over de eisen die gesteld worden aan de beveiliging van informatie. Afspraken worden vastgelegd in de overeenkomst of in een separate verwerkersovereenkomst. Daarnaast worden specifieke afspraken vastgelegd in een Service Level Agreement (SLA).

Monitoring van de afspraken vindt plaats door middel van Service Level Rapportages (SLR) en periodieke overleggen met leveranciers, waarin SLA en SLR besproken worden. Dit vormt tevens de basis voor de jaarlijkse leveranciersbeoordeling.

11 Beheer van beveiligingsincidenten

Verantwoordelijke	Security- & Privacy Officer			
NEN 7510 norm	16.1.1	16.1.2	16.1.3	16.1.4
	16.1.5	16.1.6	16.1.7	

Om beveiligingsincidenten op een eenduidige manier te beheren heeft Beweging 3.0 het document Beleid en Procedure Beveiligingsincidenten vastgesteld door de RvB. Hierin staan de verschillende rollen, verantwoordelijkheden en procedures beschreven. Over de opgetreden beveiligingsincidenten wordt eens per half jaar door de Security- & Privacy Officer gerapporteerd aan de RvB.

Gerelateerde documenten:

- Beleid en Procedure Beveiligingsincidenten

12 Continuïteit

Verantwoordelijke	Manager ICT | Cluster manager | Security Officer			
NEN 7510 norm	17.1.1	17.1.2	17.1.3	17.2.1

De continuïteit van zorg- en informatie verwerkende processen zijn geborgd in calamiteitsplannen die per locatie zijn opgesteld en zijn gepubliceerd op intranet. Het maken van back-ups wordt verzorgd door diverse leveranciers, met wie afspraken zijn gemaakt met betrekking tot frequentie, recovery en bewaartermijnen. Doel van de afspraken is, om in geval van storing of andere calamiteit het gegevensverlies zo veel als mogelijk te beperken en de beschikbaarheid van informatie te behouden.

Ten behoeve van continuïteit is, zoals aangegeven in 9.2 (Kwetsbaarhedenbeheer en cyberveiligheid) is een *Cyber Incident Respons* plan opgesteld.

Gerelateerde documenten:

- Cyber Incident Response plan

13 Naleving

13.1 Wettelijke en contractuele eisen (extern)

Verantwoordelijke	Security Officer & FG & Manager ICT			
NEN 7510 norm	18.1.1	18.1.2	18.1.3	18.1.4

Beweging 3.0 houdt een registratie bij van relevante wet- en regelgeving. Op basis van functie of rol is een verdeling gemaakt ten aanzien van het bijhouden van eventuele wijzigen. Hiermee blijft informatie up-to-date en kan kennis eenvoudig worden overgedragen. Jaarlijks wordt onderzocht of het overzicht compleet is en of aan genoemde wetgeving wordt voldaan.

Toezicht op naleving van de AVG en de daaruit voortvloeiende UAVG is de verantwoordelijkheid van de FG. Voor overige wetgeving die relevant is voor informatiebeveiliging, privacy en cyberveiligheid zal op naleving worden toegezien door de Security- & Privacy Officer. E.e.a. wordt geborgd vanuit het P/IMS en de richtlijnen voor interne audits (zie ook 13.2). Naleving van contractuele eisen wordt geborgd met de uitvoering van interne audits en het uitvoeren van leveranciersbeoordelingen.

Bij opslag van informatie, waaronder persoonsgegevens en registraties, worden wettelijke bewaartermijnen in acht genomen conform het daarvoor bestemde beleid. Implementatie en handhaving van dit beleid is de verantwoordelijkheid van de Security- & Privacy Officer en de eigenaren die per onderwerp zijn benoemd.

Gerelateerde documenten:

- Bewaarbeleid
- Diverse wetgeving
- Diverse normen

13.2 Interne regelgeving en audits

Verantwoordelijke	Security- & Privacy Officer		
NEN 7510 norm	18.2.1	18.2.2	18.2.3

Interne regelgeving, zoals beleid en onder andere gedragscode, waarbij beheersmaatregelen zijn vastgesteld die voorzien zijn van concrete controls, worden door middel van interne audits getoetst op naleving. De te auditen beheersmaatregelen zijn vastgelegd in het ISMS en worden geselecteerd op basis van risico inschatting waarbij technische beheersmaatregelen zoals benoemd in de Verklaring van Toepasselijkheid minimaal 1x elke 3 jaar intern worden getest. Bevindingen van interne audits worden vertaald naar verbeteracties, die in het ISMS worden vastgelegd en door de Security Officer worden gemonitord.

Naast interne audits, die conform plan worden uitgevoerd, zullen beleid en interne regelgeving extern worden getoetst door middel van security assessments, pentesten en audits door onafhankelijke partijen.

Gerelateerde documenten:

- Beleid Interne Audit

13.3 Toetsing van het beleid en de doelstelling

De uitkomsten van interne- en externe toetsing bepalen in belangrijke mate de mate van beveiliging van informatie. Waar het gaat om het bewust handelen en het hebben van respect voor privacy dienen nog concrete instrumenten ontwikkeld worden. Deze worden opgenomen in het Programma Bewustwording.

Over de stand van zaken ten aanzien van dit beleid en de beschreven doelstelling worden door Security- & Privacy Officer en FG periodiek gerapporteerd aan de RvB.

Gerelateerde documenten:

- Programma Bewustwording