Informatiebeveiligingsbeleid BVO NL

Versie 1.0

Eigenaar	: Raad van Bestuur
Vastgesteld Raad van Bestuur	: 3 december 2021
Instemming OR	: 6 januari 2022

Versiebeheer	
Naam document	Informatiebeveiligingsbeleid BVO NL
Verantwoordelijke	Raad van Bestuur
Auteurs	Arnoud de Vos (extern projectleider) en Patrick de Raad (LSO)
Versienummer	1.0
Status	Definitief
Datum eerste versie	08-11-2021
Laatst bijgewerkt	06-01-2022
Trefwoorden	Informatiebeleid, informatiebeveiliging, IB, NEN 7510+A1:2020
Samenvatting	Beleidsuitgangspunten rondom informatiebeveiliging BVO – omschrijving taken, verantwoordelijkheden en bevoegdheden
Classificatie	Intern

Historie	
08-11-2021	Versie 0.1 eerste opzet
18-11-2021	Versie 0.2. Opmerkingen Patrick de Raad, Sandra Blauw en LOK verwerkt.
25-11-2021	Opmerkingen Marina Klein verwerkt
01-12-2021	Opmerkingen eerste bespreking in TT verwerkt
06-01-2022	Instemming OR verwerkt

1. Inhoudsopgave

1. Voorwoord

Bevolkingsonderzoek Nederland (BVO NL) draagt door middel van kwalitatief hoogwaardig bevolkingsonderzoek substantieel bij aan het vroegtijdig behandelen van ziekten, waaronder kanker, met als doel gezondheidswinst te realiseren en sterfte terug te dringen.

Voor deze bevolkingsonderzoeken geldt dat het proces start met het uitnodigen van mensen die binnen de beoogde doelgroep vallen en eindigt met het versturen van een uitslag of een verwijzing. Onlosmakelijk verbonden met dit proces is de registratie en het verwerken van persoonsgegevens. Zo zijn naam en adres een voorwaarde om uitnodigingen te kunnen versturen en is registratie van het BSN noodzakelijk in de communicatie met zorgverleners in de keten.

Naast persoonsgegevens worden ook medische gegevens geregistreerd, verwerkt en verstuurd. Omdat medische gegevens meer nog dan persoonsgegevens behoren tot het privédomein van iedere burger, zijn integriteit en vertrouwelijkheid in de omgang met deze gegevens onlosmakelijk onderdeel van ieder aspect van de bedrijfsvoering. Maar ook de persoonsgegevens van medewerkers van Bevolkingsonderzoek Nederland, alsmede de persoonsgegevens van de ketenpartners dienen goed beschermd te zijn.

Om vertrouwelijkheid, integriteit en beschikbaarheid van informatie te waarborgen, is het nodig om alle componenten waaruit de bedrijfsvoering is opgebouwd middels een risicobenadering periodiek te beoordelen vanuit het domein van informatiebeveiliging. Waar nodig zullen maatregelen getroffen worden om informatie te beschermen tegen ongeautoriseerde inzage en bewerking. Beschermende maatregelen kunnen van technische aard zijn, maar vaker nog zal informatiebeveiliging versterkt kunnen worden door kritisch te kijken naar het eigen handelen.

De Raad van Bestuur committeert zich aan het uitvoeren van dit informatiebeveiligingsbeleid op basis van de NEN 7510:2017 + A1:2020 norm.

Dit informatiebeveiligingsbeleid is van toepassing op alle medewerkers van Bevolkingsonderzoek Nederland, en tevens op onze leveranciers en ketenpartners.

Raad van Bestuur Bevolkingsonderzoek Nederland december 2021

2. Inleiding

Onder informatiebeveiliging binnen Bevolkingsonderzoek Nederland (BVO NL) verstaan we de passende bescherming van vertrouwelijkheid, integriteit en beschikbaarheid van informatie die door of onder verantwoordelijkheid van BVO NL wordt verwerkt. Onder het verwerken van informatie wordt ook het verzamelen, bewaren, raadplegen, gebruiken, verstrekken en vernietigen van informatie verstaan.
Dit beleid biedt richting en ondersteuning voor informatiebeveiliging overeenkomstig bedrijfsmatige eisen en relevante wetten en voorschriften.

Informatiebeveiliging is nodig om een goede werking van werkprocessen van BVO NL en samenwerking met andere organisaties mogelijk te maken in de maatschappelijke context waarin BVO NL zich beweegt.

Om dat te bereiken is dit informatiebeveiligingsbeleid opgesteld en uitgevoerd. Daarbinnen heeft het beleid tot doel om ten aanzien van informatiebeveiliging van BVO NL het volgende vast te leggen:

- Context en belanghebbenden
- Uitgangspunten en kaders
- Organisatie van informatiebeveiliging voor BVO NL
- Inbedding in de organisatie door vastlegging van rollen en verantwoordelijkheden
- Een overzicht van maatregelen en activiteiten

In dit document zijn verwijzingen naar de norm NEN7510:2017 + A1:2020 opgenomen tussen rechte haken.

Dit informatiebeveiligingsbeleid is vastgesteld door de Raad van Bestuur van BVO NL. [5.2, A5.1.1]

2.1 De missie van BVO NL, gebruikte gegevens en veiligheidseisen

De screeningsorganisatie draagt door middel van kwalitatief hoogwaardig bevolkingsonderzoek substantieel bij aan een vroegtijdige behandeling van bovengenoemde kankersoorten met als doel gezondheidswinst te realiseren en sterfte terug te dringen.

De stichting heeft als algemeen nut beogende instelling ten doel het verrichten van bevolkingsonderzoeken gericht op de vroege opsporing van kanker alsmede het verrichten van andere vormen van preventief bevolkingsonderzoek op het gebied van de gezondheid, en voorts al hetgeen met een en ander rechtstreeks of zijdelings verband houdt of daartoe bevorderlijk kan zijn, alles in de ruimste zin van het woord.

De stichting tracht haar doel onder meer te verwezenlijken door:

a. Het (doen) exploiteren van een screeningsorganisatie ten behoeve het verrichten van bevolkingsonderzoeken gericht op de vroege opsporing van kanker, het verrichten van andere vormen van preventief bevolkingsonderzoek op het gebied van de gezondheid;
b. het centraal stellen van cliënten alsmede van hun gerechtvaardigde wensen en behoeften bij het verrichten van bevolkingsonderzoek;
c. het zo doelmatig en efficiënt mogelijk organiseren en uitvoeren van de bevolkingsonderzoeken;
d. het samenwerken met andere organisaties of voorzieningen op het terrein van de (preventieve) gezondheidszorg;
e. het voeren van een actief en transparant beleid voor de dialoog met de meest relevante belanghebbenden;
f. het (doen) verrichten en bevorderen van (wetenschappelijk) onderzoek naar de preventie van kanker;

g. kwaliteitsborging in de keten;
h. deskundigheidsbevordering in de keten;
i. informatiemanagement ten behoeve van de landelijke screeningsprogramma's;
j. het faciliteren van wetenschappelijk onderzoek.

Voor al deze activiteiten wordt informatie verwerkt. Het grootste gedeelte van deze informatie bestaat uit cliëntgegevens die geïmporteerd, verwerkt en opgeslagen worden. Het betreft persoonsgegevens die veelal gekoppeld zijn aan medische gegevens. Ook op de opslag en verwerking van persoonsgegevens van medewerkers, leveranciers en ketenpartners is de informatiebeveiliging van toepassing. Vanwege de gevoeligheid van deze informatie, wordt cliëntinformatie alleen ter beschikking gesteld aan derden als onderdeel van onze uitvoeringstaak of als dit wettelijk verplicht is. Hierbij wordt o.a. de procedure gevolgd die is vastgesteld door het RIVM rondom het traject Data & Wetenschap.

2.2 Definitie van informatiebeveiliging

Een samenhangend stelsel van maatregelen dat zich richt op het blijvend realiseren van een noodzakelijk niveau van beschikbaarheid, integriteit en vertrouwelijkheid van informatie.

2.3 Samenhang tussen informatiebeveiliging en privacybescherming

Privacybescherming richt zich op de zorgvuldige omgang met persoonsgegevens, bijvoorbeeld van cliënten of medewerkers. Informatiebeveiliging richt zich op de beveiliging van informatie, waaronder persoonsgegevens. De maatregelen die in het kader van informatiebeveiliging worden getroffen, leveren een bijdrage aan de bescherming van persoonsgegevens. Bij BVO NL is de Landelijke Security Officer (LSO) verantwoordelijk voor de coördinatie van alle activiteiten die betrekking hebben op informatiebeveiliging en privacybescherming. Daarbij kan teruggevallen worden op de Functionaris Gegevensbescherming van BVO NL voor advies over de bescherming van persoonsgegevens.

2.4 Samenhang tussen informatiebeveiliging en risicomanagement

Risicomanagement is het analyseren en beheersen van organisatie brede risico's. Deze doen zich op diverse terreinen voor; hierbij valt te denken aan bijvoorbeeld financiële risico's of de beschikbaarheid en inzet van personeel. Ook in de informatievoorziening en bij de omgang met vertrouwelijke informatie doen zich risico's voor. BVO NL hanteert een integrale methode voor het analyseren en beheersen van risico's. Informatiebeveiliging is hier een onderdeel van.

2.5 Samenhang tussen informatiebeveiliging en kwaliteitszorg

BVO NL streeft naar een hoge kwaliteit in de uitvoering van zorg en de ondersteunende bedrijfsprocessen. Bevolkingsonderzoek Nederland heeft diverse (verplichte) kwaliteitscertificaten en –accreditaties verworven. We werken continu aan kwaliteitsverbetering. Dit geldt ook voor de informatievoorziening en de informatiebeveiliging. De LSO en de Coördinator Kwaliteit coördineren de activiteiten rondom de kwaliteitszorg en informatiebeveiliging.

2.6 Doel en gewenst resultaat van het informatiebeveiligingsbeleid

Het informatiebeveiligingsbeleid is gebaseerd op 3 pijlers:

- **Vertrouwelijkheid**
  Aan de vertrouwelijkheid van gegevens worden hoge eisen gesteld. Als cliëntinformatie, maar ook personeelsinformatie in verkeerde handen valt of openbaar wordt kan dit ernstig nadeel opleveren voor de betrokkenen. Ook kan de goede naam (imago) van BVO NL hierdoor worden aangetast, niet alleen bij cliënten en medewerkers maar ook bij leveranciers en andere stakeholders.
- **Integriteit**
  Aan de juistheid van informatie worden eveneens hoge eisen gesteld. Het is cruciaal dat uitslagen die het resultaat zijn van screening correct zijn vastgelegd. Integriteit wordt

gewaarborgd door informatie zodanig te beschermen dat onbedoelde wijzigingen worden voorkomen.

- **Beschikbaarheid**
  Aan de beschikbaarheid van informatie worden standaard eisen gesteld. De uitvoering van de drie bevolkingsonderzoeken komt niet direct in gevaar als de systemen (applicaties) die de primaire digitale processen faciliteren, maximaal 1 werkdag niet beschikbaar zijn, zoals benoemd in het Business Continuïteit Plan (BCP).

Daarnaast dient BVO NL vanzelfsprekend ook te voldoen aan de geldende wet- en regelgeving. Ook in het kader van de informatiebeveiliging.

Het informatiebeveiligingsdoel moet deze vier onderdelen verenigen en deze moeten te controleren zijn (meetbaar) op tenminste 2 factoren.

Het informatiebeveiligingsdoel van BVO NL is *het voldoen aan de geldende wet- en regelgeving rondom informatiebeveiliging en zorgdragen dat de informatie beschikbaar is, vertrouwelijk blijft en dat de integriteit van de informatie gewaarborgd blijft.*

Het resultaat van deze beveiliging wordt zichtbaar doordat:

- Voldoen aan wet- en regelgeving
  - BVO NL de vergunning van het ministerie van VWS behoudt om bevolkingsonderzoeken te mogen uitvoeren;
  - BVO NL de certificaten behoudt die nodig zijn om te voldoende aan de gelden wet- en regelgeving, waaronder de NEN 7510:2017+A1:2020. Beschikbaarheid van informatie:
  - De systemen van BVO NL een uptime hebben van 99,5% of beter, tijdens kantooruren;
  - De informatie van BVO NL in 99,9% van de tijd beschikbaar is voor ketenpartners, tijdens kantooruren;
- Vertrouwelijkheid
  - Er worden tijdens controles geen actieve gebruikers gevonden die inzage kunnen hebben in cliënt- of medewerkersgegevens, terwijl ze daar vanuit hun functie (of tijdelijk verleende aanvullende rechten) geen toegang toe horen te hebben;
  - BVO NL veroorzaakt, naast de vermiste poststukken, geen grootschalig (meer dan 2% van de cliëntgegevens) datalek;
- Integriteit
  - Er geen ongeoorloofde wijzigingen van de gegevens plaatsvinden, conform de afspraken in de rollen en rechtenmatrix;
  - Er tijdens controles geen actieve gebruikers gevonden worden die onterecht beheerrechten hebben, conform de afspraken in de rollen en rechtenmatrix.

3. Context, belanghebbenden, toepassingsgebied en uitgangspunten

3.1 Context [4.1]

Jaarlijks nemen in Nederland meer dan 3 miljoen mensen van tussen de 30 en 75 jaar oud deel aan door de overheid aangeboden bevolkingsonderzoeken naar kanker. De bevolkingsonderzoeken naar kanker maken deel uit van een groter aanbod van bevolkingsonderzoeken binnen het Nationaal Programma Bevolkingsonderzoek. Het Ministerie van VWS is opdrachtgever van de drie bevolkingsonderzoeken naar kanker. Het Centrum voor Bevolkingsonderzoek van het Rijksinstituut voor Volksgezondheid en Milieu is, in opdracht van VWS, verantwoordelijk voor de regie en subsidieverlening van de bevolkingsonderzoeken. De uitvoering wordt verzorgd door de screeningsorganisatie, in samenwerking met haar ketenpartners, zoals de huisartsen en de ziekenhuizen.

Tot 2006 waren er 20 screeningsorganisaties actief in Nederland en lag de coördinatietaak bij het CvZ. In 2009 en 2010 fuseerden de screeningsorganisaties tot 5 regionale organisaties en kregen de vorm van stichtingen. Daarnaast werd er een landelijke organisatie FSB opgericht voor de gemeenschappelijke ondersteunende diensten voor IT en inkoop voor de vijf screeningsorganisaties. De coördinatietaken werden belegd bij het Centrum voor Bevolkingsonderzoek, als onderdeel van het RIVM.

In 2018 startte een fusietraject om tot één screeningsorganisatie te komen. Op 1 september 2020 vond een bestuurlijke fusie van de vijf screeningsorganisaties en de FSB plaats. Er werd een moederstichting Bevolkingsonderzoek Nederland met hun dochtermaatschappijen de SO's en de FSB opgericht. Op 2 januari 2022 is de juridische fusie tot één screeningsorganisatie Bevolkingsonderzoek Nederland een feit.

BVO NL voert in opdracht van het RIVM/ministerie van VWS de bevolkingsonderzoeken borstkanker (BVO BK), baarmoederhalskanker (BVO BMHK) en darmkanker (BVO DK) uit. De organisatie heeft kantoren in heel Nederland. In totaal zijn er ongeveer 940 medewerkers werkzaam bij BVO NL verspreid over 9 kantoorlocaties, 12 vaste onderzoekscentra en 71 mobiele onderzoekscentra.

Om de drie bevolkingsonderzoeken uit te mogen voeren, heeft BVO NL een WBO-vergunning verkregen van het ministerie van VWS. Hieraan zijn strikte voorwaarden verbonden. Daarnaast is er een beleidskader bevolkingsonderzoek kanker en is er per bevolkingsonderzoek een uitvoeringskader opgesteld waarin de rollen en rechten van elke deelnemende partij zijn vastgelegd. BVO NL voert een reeks van handelingen uit, die start met de uitnodiging van de doelgroep en doorloopt tot en met de aansluiting op een eventueel vervolgtraject in de zorg. Een sluitende keten met een helder beeld van de rollen en taken van de partijen die betrokken zijn bij de uitvoering van het bevolkingsonderzoek. Dit is essentieel voor een optimaal 'aanbod' voor de doelgroep van de bevolkingsonderzoeken. Voor het bevolkingsonderzoek borstkanker is de beschikbaarheid van voldoende MBB'ers de grootste zorg. Daarvoor heeft BVO NL een intern opleidingsprogramma opgestart.

Ten behoeve van alle administratieve handelingen m.b.t. cliënten die tijdens de uitvoering van bevolkingsonderzoeken worden vastgelegd is een overkoepelend software platform ingericht, ScreenIT.

Doordat er zoveel verschillende locaties zijn is goede en heldere communicatie van groot belang. Er is dan ook voor gekozen om speciaal voor informatiebeveiliging een bewustwordingscampagne op te zetten waarin onder andere aandacht is voor de verschillende potentiële beveiligingsincidenten.

3.2 Belanghebbenden [4.2]

De veilige omgang met informatie is van belang voor de volgende belanghebbenden:

- Cliënten:
  - vertrouwelijkheid van hun informatie ter bescherming van hun persoonlijke levenssfeer;
  - integriteit van informatie, zodat cliënten erop kunnen vertrouwen dat er op basis van juiste informatie wordt gehandeld;
  - beschikbaarheid van informatie, zodat cliënten erop kunnen vertrouwen dat hun informatie beschikbaar is.
- Ketenpartners:
  - vertrouwelijkheid van bedrijfsinformatie en persoonsgegevens van medewerkers en ingehuurde medewerkers van ketenpartners. Uitlekken van deze informatie zou kunnen leiden tot (imago)schade voor ketenpartners en verminderd vertrouwen bij hun stakeholders, zoals medewerkers, cliënten/patiënten en leveranciers;
  - integriteit van informatie. Dit is van belang voor ketenpartners om ervoor te zorgen dat informatie van cliënten/patiënten, onderzoeken en beoordelingen correct is;
  - beschikbaarheid van informatie binnen BVO NL. Dit is belangrijk voor ketenpartners, zodat zij voortdurend bediend kunnen worden. Dat is in het bijzonder relevant in gevallen waarin ketenpartners beoordelingen uitvoeren voor BVO NL, of een onderdeel van het proces zijn, zoals bij DK en BMHK.
- Leveranciers:
  - informatiebeveiliging (bij BVO NL). Dit is van belang voor leveranciers, zodat dit aansluit bij hun eigen informatiebeveiligingsbeleid en omdat incidenten (bij BVO NL) ook negatieve gevolgen kunnen hebben voor leveranciers, bijvoorbeeld voor de continuïteit van hun dienstverlening aan BVO NL en daarmee hun bedrijfsvoering en voor hun imago.
- Medewerkers:
  - vertrouwelijkheid van informatie ter bescherming van de persoonlijke levenssfeer van de medewerker, en zodat medewerkers worden gefaciliteerd in de veilige omgang met gegevens van BVO NL, cliënten en (medewerkers van) leveranciers;
  - integriteit van informatie, zodat medewerkers erop kunnen vertrouwen dat ze handelen op basis van juiste informatie en zodat de organisatie over de juiste gegevens beschikt;
  - beschikbaarheid van informatie, zodat medewerkers erop kunnen vertrouwen dat noodzakelijke informatie altijd beschikbaar is.
- Maatschappij, inclusief toezichthouders en wetgevers:
  - vertrouwelijkheid: de zekerheid dat de vertrouwelijkheid van informatie en de privacy van cliënten, medewerkers en anderen adequaat wordt gewaarborgd;
  - integriteit: de zekerheid dat diensten op basis van de juiste informatie worden verleend, administratieve gegevens juist zijn en (financiële) rapportages juiste informatie bevatten;
  - beschikbaarheid: de zekerheid dat noodzakelijke informatie, waaronder gegevens die nodig zijn voor toezicht, beschikbaar is;
  - informatiebeveiliging. Dit is een wezenlijke bouwsteen voor het onder andere voldoen aan de Algemene Verordening Gegevensbescherming (AVG) en de Wabvpz. De uitvoering van dit beleid ondersteunt de aantoonbaarheid van passende beveiliging van persoonsgegevens.

3.3 Toepassingsgebied van dit informatiebeveiligingsbeleid [4.3]

Het toepassingsgebied van de informatiebeveiliging is: “het organiseren en uitvoeren van de bevolkingsonderzoeken borstkanker, baarmoederhalskanker en darmkanker Nederland”.

Dit beleid heeft betrekking op de juridische entiteit Stichting Bevolkingsonderzoek Nederland en de medewerkers, in dit beleid ook wel Bevolkingsonderzoek Nederland of BVO NL genoemd [4.3].

In het Kwaliteit -en Informatiebeveiliging Management Systeem (KMS/ISMS) is een organisatieschema opgenomen. Het beleid is van toepassing op alle medewerkers en al het ingehuurde personeel van Bevolkingsonderzoek Nederland. Daarnaast is dit beleid van toepassing op medewerkers van leveranciers die:

- werken binnen de kantoorgebouwen en-of onderzoekscentra en/of
- een BVO NL-account hebben.

3.4 Uitgangspunten van informatiebeveiliging

Bij de invoering van het Information Security Management System (ISMS) en het opstellen van de verbeterplannen is uitgegaan van de norm NEN 7510:2017 +A1:2020 met bijbehorende doelstellingen en beheersmaatregelen. Met de toepassing van deze standaard wordt optimaal gebruikgemaakt van de ervaring met informatiebeveiliging in andere zorgorganisaties.

3.4.1 Inhoudelijke uitgangspunten

1. BVO NL voldoet aan alle, van toepassing zijnde, wet- en regelgeving. In dit verband worden o.a. genoemd:
   - Archiefwet
   - Auteurswet
   - Algemene Verordening Gegevensbescherming (AVG) en aanpalende wetgeving
   - Grondwet, bijvoorbeeld artikel 10 en 13
   - Telecommunicatiewet
   - Wet basisregistratie personen en aanpalende wetgeving
   - Wet op de beroepen in de individuele gezondheidszorg (Wet BIG)
   - Wet op de Geneeskundige behandelingsovereenkomst, Burgerlijk Wetboek, Boek 7, Titel 7, Afdeling 5 (WGBO).
   - Wet Kwaliteit, klachten en geschillen in de zorg (Wkkgz)
   - Wet Aanvullende bepalingen verwerking persoonsgegevens in de zorg (Wabvpz)
   - Wet op het bevolkingsonderzoek (Wbo)
   - Wet elektronische handtekeningen (Weh)
2. Informatiebeveiliging is een onderdeel van de integrale managementverantwoordelijkheid. Alle organisatieonderdelen van BVO NL hebben hiertoe verantwoordelijkheden toegewezen die zijn vastgelegd.
3. BVO NL bepaalt welke persoonsgegevens worden verwerkt, alsmede de doelen van deze verwerkingen en is daarmee gekwalificeerd als "verwerkingsverantwoordelijke" in de zin van de AVG. Wanneer (onderdelen van) BVO NL samenwerkingsverbanden aangaan met externe partijen, hetzij inhoudelijk, hetzij voor de ontwikkeling of het beheer van de informatievoorziening, wordt nadrukkelijk aandacht besteed aan informatiebeveiliging. Afspraken hierover worden schriftelijk vastgelegd en op de naleving hiervan wordt toegezien. Dit krijgt zijn beslag in verwerkersovereenkomsten en contracten.
4. De bedrijfsprocessen, informatiesystemen en gegevensverzamelingen van alle onderdelen van BVO NL zijn volgens een gestructureerde methode geclassificeerd naar de aspecten ‘beschikbaarheid’, ‘integriteit’ en ‘vertrouwelijkheid’.

5. Alle informatie en informatiesystemen zijn van kritiek en vitaal belang voor de organisatie. De verantwoordelijkheid voor informatiebeveiliging ligt bij het (lijn-) management, met de Raad van Bestuur als eindverantwoordelijke.
6. In het informatiebeveiligingsbeleid staat het faciliteren van de werkprocessen van de organisatie voorop. Informatiebeveiliging dient hieraan een bijdrage te leveren door het veilig werken met informatie te faciliteren.
7. Toegang tot informatie wordt verleend zodat informatie alleen toegankelijk is voor personen die de informatie nodig hebben om hun taken uit te voeren (principe “need-to-know”). [A9.1.1, A9.1.2, A9.4.1]
8. Toegang tot informatie wordt verleend zodat een keten van activiteiten waarvoor integriteit van de verwerking belangrijk is nooit door één persoon kan worden uitgevoerd (principe functiescheiding). [A6.1.2]
9. Iedere BVO NL medewerker heeft kennis van alle, voor het uitoefenen van zijn functierelevante IB-documentatie die in het handboek is in te zien en handelt hier ook naar.
10. Alle medewerkers (wel of niet in loondienst) van BVO NL die gebruik maken van de informatiesystemen en –diensten, zijn alert op beveiligingsincidenten en kwetsbaarheden in de informatiebeveiliging en rapporteren deze bij constatering direct.
11. Alle contractanten van BVO NL die toegang hebben tot de ruimten, zijn alert op beveiligingsincidenten en kwetsbaarheden in de informatiebeveiliging en rapporteren deze bij constatering direct.
12. Bij de aanname en tijdens het dienstverband van medewerkers en leidinggevenden wordt nadrukkelijk aandacht besteed aan de betrouwbaarheid van medewerkers en aan de waarborging van de vertrouwelijkheid van informatie.

Dit Informatiebeveiligingsbeleid beschrijft het algemene beleid t.a.v. veilig omgaan met informatie. Daarnaast wordt onderliggend beleid vastgesteld per onderwerp, zoals voor de fysieke en HR-aspecten van informatiebeveiliging. Dit onderliggende beleid maakt deel uit van het informatiebeveiligingsbeleid en is opgenomen in het documentbeheer van BVO NL. Deze documentatie wordt nader aangevuld naarmate er meer en/of andere beveiligingsmaatregelen worden geïmplementeerd.

In het algemeen worden beleid, beheersingsmaatregelen en de daaruit voortvloeiende registraties en administraties bijgehouden om de maatregelen en het beleid effectief te kunnen uitvoeren, te kunnen evalueren en de opzet en implementatie daarvan te kunnen aantonen. [7.5.1] In het document “Verklaring van Toepasselijkheid” wordt aangegeven welke maatregelen van toepassing zijn, welke zijn geïmplementeerd en welke van de referentiedoelstellingen niet zijn geïmplementeerd en waarom.

De documentatie wordt beheerd door de afdeling kwaliteit. [7.5.3] Bij de operationele uitvoering van beveiligingsmaatregelen worden aanvullende documenten opgesteld, zoals:

- een jaarlijks communicatieplan, voornamelijk intern, en vooral gericht op bewustwording en training; [7.4]
- een jaarlijkse planning voor controles, interne audits, waarin wordt aangegeven in welke mate de organisatie het ISMS en beheersmaatregelen heeft geïmplementeerd. [9.2]

Formeel goed te keuren documenten zijn via het documentbeheersysteem toegankelijk en worden daar actueel gehouden. [7.5.2]

3.4.2 Organisatie brede en algemene uitgangspunten

1. (De Raad van Bestuur van) BVO NL is verantwoordelijk voor informatiebeveiliging en de bescherming van persoonsgegevens.,
2. De maximaal toegestane uitvalduur van de primaire processen is 1 werkdag,

3. Het maximaal toegestane gegevensverlies van gegevens die van belang zijn voor de primaire processen zal worden bepaald in een risicoanalyse en worden vastgelegd in het continuïteitsplan,
4. Opgeslagen informatie op mobiele apparatuur wordt versleuteld zodat de kans op ongeautoriseerde inzage sterk wordt verkleind [A10.1.1],
5. BVO NL neemt afdoende beveiligingsmaatregelen om beschikbaarheid, vertrouwelijkheid en integriteit van de operationele informatie- en communicatievoorzieningen te waarborgen. Maatregelen tegen allerlei vormen van kwaadaardige programmatuur vormen hiervan een belangrijk onderdeel,
6. De eisen die aan de beveiliging en veiligheid van informatie worden gesteld zijn een afgeleide van de classificatie van deze informatie in combinatie met de eisen die de omgeving van BVO NL en wet- en regelgeving hebben vastgesteld [A8.2.1],
7. Bij ieder proces, project en inkooptraject dat binnen of vanuit BVO NL wordt geïnitieerd wordt in een zo vroeg mogelijk stadium aandacht besteed aan informatiebeveiliging [A6.1.5],
8. BVO NL voert een actief beleid om het beveiligingsbewustzijn van medewerkers en leidinggevenden te stimuleren [A7.2.2] [A12.2.1],
9. BVO NL beschikt over gedragsregels voor het gebruik van (algemene) informatievoorzieningen (gedragscode gebruik ICT-middelen BVO NL). Op de naleving van deze gedragsregels wordt toegezien door de leidinggevenden [A7.1.2],
10. Bij overtreding van de regelgeving voor informatiebeveiliging en/of relevante wettelijke bepalingen kan de bestuurder een sanctie opleggen zoals dat is aangegeven in de cao, de arbeidsovereenkomst en/of de gedragsregels van BVO NL [A7.2.3].

3.4.3 Uitgangspunten m.b.t. toegang en autorisatie

1. Accounts en wachtwoorden zijn strikt persoonlijk [A9.2.3],
2. Beveiliging van informatie is een onderdeel van het werk van iedere medewerker [A7.1.2],
3. Groepsaccounts worden alleen gebruikt als het gebruik van een persoonlijke account leidt tot onwerkbare (ongewenste) situaties,
4. De kantoren zijn toegankelijk voor daartoe geautoriseerde BVO NL-medewerkers. Voor externen zijn aanvullende maatregelen beschreven in het toegangsbeleid [A11.1.2],
5. Inloggen op de KA omgeving is mogelijk met account en wachtwoord vanuit kantoor, maar alleen met een extra authenticatiemiddel (token) vanuit een externe locatie. Inloggen op de systemen die medische gegevens bevatten is alleen mogelijk met een extra authenticatiemiddel. [A9.1.1] [A9.4.2],

3.4.4 Uitgangspunten m.b.t. leveranciers en inkoop

1. Aan leveranciers, met name leveranciers die persoonsgegevens van BVO NL verwerken worden eisen gesteld met betrekking tot informatiebeveiliging. [A15.1.1] [A15.1.2].
2. Bij de ontwikkeling en aanschaf van informatiesystemen en bij de ontwikkeling van procedures wordt aandacht besteed aan informatiebeveiliging [A14.1.1] [A14.2.1],
3. Verwerkers van persoonsgegevens waar BVO NL verantwoordelijk voor is hebben een verwerkersovereenkomst getekend [A15.1.2].

4. Rollen en verantwoordelijkheden

De Raad van Bestuur van BVO NL is eindverantwoordelijk voor informatiebeveiliging als onderdeel van de bestuurlijke verantwoordelijkheid (governance). De RvB geeft invulling aan die verantwoordelijkheid door het vaststellen van beleid en doelstellingen, de integratie daarvan in de processen van de organisatie, toewijzing van rollen en verantwoordelijkheden, het ter beschikking stellen van middelen, het bekendmaken van het beleid en het belang daarvan, het aansturen en ondersteunen van medewerkers bij en het toezien op uitvoering van het beleid, evaluatie en bijstelling van het beleid en het managementsysteem en de jaarlijkse directiebeoordeling. [5.1, 9.3] Daarbij wordt de RvB ondersteund door de organisatie, namelijk door: [5.3, A6.1.1a]

- Alle medewerkers die elk verantwoordelijk zijn voor het uitvoeren van het informatiebeveiligingsbeleid als onderdeel van hun professionele verantwoordelijkheid. Om hen daarbij te ondersteunen zijn gedragsregels uitgewerkt waarin medewerkers bewust worden gemaakt van hun rol/bijdrage en geïnformeerd over hoe zij deze kunnen uitvoeren/leveren, zowel bij indiensttreding als op basis van regelmatige bewustwordings- en leerinterventies. Daarvoor wordt jaarlijks een programma opgesteld; [7.3]
- management / leidinggevenden die toezien op de naleving van het beleid;
- de LSO, die het opstellen, de uitvoering, evaluatie en bijstelling van het beleid en de jaarlijkse verbetercycli m.b.t. informatiebeveiliging coördineert. Deze rapporteert bijvoorbeeld over beveiligingsincidenten aan de RvB en het MT en zorgt ervoor dat informatiebeveiliging is opgenomen in plannen voor bedrijfscontinuïteit/calamiteitenplannen en het communicatieplan voor bewustwording en training op het gebied van informatiebeveiliging;
- de Functionaris Gegevensbescherming (FG), die toezicht houdt, kaders aangeeft, informeert en adviseert vanuit zijn/haar wettelijke taak over de bescherming van persoonsgegevens;
- afdeling kwaliteit die:
    - opzet en bestaan van het KMS/ISMS bewaakt;
    - interne audits coördineert;
    - externe (certificerings)audits coördineert;
    - medewerkers ondersteunt bij het uitvoeren en continue verbeteren van de processen.
- afdeling informatiebeveiliging die:
    - medewerkers ondersteunt bij het uitvoeren en continue verbeteren van de IB processen
    - afdeling kwaliteit ondersteund bij de opzet en bestaan van het KMS/ISMS
- andere medewerkers die verantwoordelijk zijn voor specifieke onderdelen van het beleid, zoals het uitvoeren van specifieke beveiligingsmaatregelen en de bewaking daarvan. Deze specifieke taken en verantwoordelijkheden worden benoemd in de beschrijving van de beheersmaatregelen.

4.1 Contacten met andere organisaties [A6.1.3]

De afdeling informatiebeveiliging onderhoudt contacten met andere organisaties over informatiebeveiliging en informeert zich frequent over risico's en ontwikkelingen op dit gebied, bijvoorbeeld via al dan niet gespecialiseerde internetfora en websites. [A6.1.4, A12.6.1].

Contacten met de Autoriteit Persoonsgegevens worden door de FG onderhouden.

Contacten met andere toezichthouders, instanties en belangengroepen worden in voorkomende gevallen door de RvB, het MT of aangewezen functionarissen/afdelingen onderhouden.

Contactpersonen bij calamiteiten worden in het bedrijfscontinuïteitsplan beschreven.

4.2 Generieke rollen, toegespitst op informatiebeveiliging

4.2.1 De Raad van Bestuur

De RvB van BVO NL wijst een lid aan die eindverantwoordelijk is voor informatiebeveiliging. Deze verantwoordelijkheid omvat:

- het vaststellen van het informatiebeveiligingsbeleid en daaruit voortvloeiende richtlijnen;
- het toezien op de naleving van het informatiebeveiligingsbeleid en het evalueren van de toepassing en werking van het Information Security Management System.

4.2.2 Management / Leidinggevenden

Het management is verantwoordelijk voor de inrichting en uitvoering van de bedrijfsprocessen. De verantwoordelijkheid voor de bedrijfsprocessen omvat ook de beveiliging van de informatie en de ICT-infrastructuur. Het lijnmanagement wordt hierbij ondersteund door de afdeling informatiebeveiliging.

De verantwoordelijkheid van het lijnmanagement omvat onder andere de volgende taken:

- positieve en actieve houding ten aanzien van informatiebeveiliging;
- fungeren als voorbeeldfunctie;
- toezicht houden op de naleving van informatiebeveiligingsmaatregelen;
- medewerking verlenen aan verbeteracties;
- (mede) autoriseren van medewerkers;
- informatiebeveiliging behandelen in werkoverleg, beoordelingen, et cetera;
- keuze informatiesystemen binnen het verantwoordelijkheidsgebied.

4.2.3 Proceseigenaar

De proceseigenaar is verantwoordelijk voor het definiëren van de bedrijfsprocessen die door het systeem worden ondersteund. De proceseigenaar zal de details voor het beoogde gebruik van de systemen vaststellen. Dit vereist dat de proceseigenaar de gebruikersvereisten voor het systeem vaststelt en goedkeurt. Het is essentieel voor het succes van de systeemvalidatie dat de informatie die wordt verstrekt voor het vaststellen van de gebruikersvereisten nauwkeurig wordt gecommuniceerd door personen die het meest bekend zijn met de gegevensverwerking die door het systeem moet worden geautomatiseerd.

De proceseigenaar stelt vast welke functionaris toegang heeft tot het informatiesysteem. Dit geldt tevens voor de rol(len) die gekoppeld zijn aan het betreffende account. Deze toegang (autorisatie) wordt gedocumenteerd in een autorisatiematrix. In deze matrix staan alle functionarissen die toegang hebben tot het betreffende informatiesysteem met de bijbehorende rollen en rechten. Eenmaal per jaar stelt de proceseigenaar deze matrix vast. Van deze matrix mag alleen worden afgeweken na schriftelijke toestemming van de proceseigenaar.

4.2.4 Systeemeigenaar

De systeemeigenaar zorgt ervoor dat het systeem gedurende zijn gehele levenscyclus de gegevensverwerking ondersteunt conform de wensen en eisen van de proceseigenaar. De systeemeigenaar is de persoon die verantwoordelijk is voor de beschikbaarheid, beveiliging, naleving, onderhoud, back-up en ondersteuning van het geautomatiseerde systeem. Voorafgaand aan de implementatie van het systeem moet er een plan zijn voor het onderhoud en de ondersteuning van de productieomgeving van het systeem. Dit omvat de operationele procedures voor ondersteunend personeel. De systeemeigenaar is in eerste instantie verantwoordelijk voor het toezicht op de validatie van het computersysteem en is uiteindelijk gedurende de hele levensduur van het systeem verantwoordelijk voor het in een gevalideerde status houden van het systeem.

In het geval van kleinschalige lokale systemen kan de eigendomsrol ook worden toegewezen aan de proceseigenaar. In het geval van complexe systemen of systemen die door meerdere gebruikersgroepen of vestigingen worden gebruikt kan de eigendomsrol worden toegewezen aan een aangewezen ICT persoon die dichter bij de bron van het systeem staat en in een betere positie verkeert om de prestaties van het systeem te beheersen. In deze gevallen worden deze rollen, systeemeigenaar en proceseigenaar, door afzonderlijke onafhankelijke personen vervuld.

4.2.5 De applicatiebeheerder

De applicatiebeheerder is verantwoordelijk voor het toekennen van de juiste autorisaties en documentatie hiervan. Hij/zij doet dat op basis van de door de systeemeigenaar vastgestelde autorisatiematrix. De applicatiebeheerder is tevens verantwoordelijk voor de juiste administratie van de autorisatiematrix. De applicatiebeheerder ziet erop toe dat de applicatie de ingevoerde informatie zo verwerkt dat de output voldoet aan gemaakte afspraken.

4.2.6 De systeembeheerder

De systeembeheerder is verantwoordelijk voor de instandhouding van geautomatiseerde informatievoorziening en maakt daarover waar nodig ook afspraken met de leveranciers die onderdelen daarvan verzorgen. De systeembeheerder is tevens verantwoordelijk voor het accountbeheer op netwerkniveau (referentiedocument: overzicht personeelsbestand P&O), een juiste documentatie en implementatie van de toegang tot de mappenstructuur en het beschikbaar stellen van applicaties op basis van de ICT-middelenmatrix.

4.2.7 De medewerker Servicedesk

De medewerker Servicedesk is verantwoordelijk voor een juiste en tijdige opvolging van geregistreerde IB-incidenten.

4.2.8 De coördinator kwaliteit

De coördinator kwaliteit is medeverantwoordelijk voor het uitvoeren van risicoanalyses en het documenteren van door het MT benoemde systeem-, proces-, en informatieverantwoordelijken. Ook het integreren van informatiebeveiliging in het KMS/ISMS met het beheer van het daarbij behorende verbeterregister, behoort tot het takenpakket.

4.2.9 Manager O&O

De manager O&O is verantwoordelijk voor de ontwikkeling, het beheer en uitvoering van het personeelsbeleid van BVO NL. De verantwoordelijkheid omvat de volgende taken:

- beheer van taakomschrijvingen waarin ook aandacht voor informatiebeveiliging;
- beheer en uitvoering van het personeelsbeleid, inclusief sanctiebeleid;
- aanname, mutatie, ontslag van personeel.

De manager O&O wordt daarbij ondersteund door de manager HRM.

4.2.10 Manager Financiën en IT

De manager F&I is verantwoordelijk voor de ontwikkeling, het beheer en uitvoering van het ICT beleid van BVO NL. De verantwoordelijkheid omvat de volgende taken:

- leidinggeven aan de afdeling ICT en het verder ontwikkelen van de competenties van de medewerkers;
- het opdrachtgeverschap van de verschillende ICT projecten en verbetertrajecten.

De manager F&I wordt daarbij ondersteund door de manager IT

4.2.11 Gebruiker
Is verantwoordelijk voor de uitvoering van het informatiebeveiligingsbeleid dat is uitgewerkt in een aantal documenten (zie bijlage), zoals gedragscodes, beleidsstukken, richtlijnen en werkinstructies. Al deze stukken zijn te raadplegen in het handboek kwaliteit.

4.3 Specifieke rollen

4.3.1 Landelijke Security Officer
De Landelijke Security Officer (LSO) coördineert alle activiteiten met betrekking tot informatiebeveiliging binnen het Bevolkingsonderzoek Nederland. De LSO werkt nauw samen met de Functionaris Gegevensbescherming en de afdelingen kwaliteit, informatiebeveiliging en IT en rapporteert aan de RvB.

Deze rol omvat de volgende werkzaamheden:

- Beleidsvoorbereiding en het beheren van het informatiebeveiligingsbeleid en hieruit voortvloeiende richtlijnen en procedures,
- Het coördineren van de implementatie van het gewenste niveau van informatiebeveiliging en privacybescherming en het stimuleren van het beveiligings- en privacy bewustzijn bij medewerkers en leidinggevenden,
- Het op peil brengen en houden van het informatieveiligheidsbeleid en privacybescherming conform vastgestelde norm;
- Het adviseren over ontwikkelingen, risico's en kansen met betrekking tot beveiligings- en privacyvraagstukken;
- Fungeren als aanspreekpunt op het gebied van informatiebeveiliging en privacybescherming.

4.3.2
4.3.3 Security Board
4.3.4 Bestaat uit de LSO, FG en de portefeuillehouder ICT van de RvB.

4.3.5 Informatiebeveiliging Management Forum (IBMF)
Bestaat uit de LSO en FG en (meerdere) managementvertegenwoordigers uit zowel Financiën & IT, Organisatie & Ontwikkeling en Uitvoering BVO.

4.3.6 Regionale Security Officer
De Regionale Security Officer (RSO) voert regionale activiteiten uit met betrekking tot informatiebeveiliging binnen Bevolkingsonderzoek Nederland, zoals:

- ondersteunen bij implementatie van informatiebeveiligingsbeleid
- controle op naleving informatiebeveiligingsbeleid
- fungeren als lokaal aanspreekpunt voor informatiebeveiliging

De RSO rapporteert aan de LSO.

4.4 Overlegvormen

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

- Overleg Security Board
- Overleg IBMF
- Overleg afdeling informatiebeveiliging

De Security Board bestaat uit de portefeuillehouder Raad van Bestuur, de FG en de LSO. In dit overleg wordt maandelijks aandacht besteed aan rapportages, voorstellen voor de Raad van Bestuur, voorstellen voor wijzigingen van het informatiebeleid, investeringsvoorstellen voor beveiligingsmaatregelen, etc. De realisatie en naleving van het informatiebeveiligings- en

privacybeleid en de bijbehorende richtlijnen en naleving worden minimaal eenmaal per kwartaal besproken.

Het IBMF bespreekt de implementatie van informatiebeveiliging. Het overleg vindt minimaal zesmaal per jaar plaats.

In het overleg van de afdeling kwaliteit wordt het beheer en de uitvoering en verbetering van het KMS/ISMS besproken. De LSO en/of medewerkers van de afdeling informatiebeveiliging worden daar waar nodig betrokken.

In het overleg van de afdeling informatiebeveiliging wordt de uitvoering van het informatiebeveiligingsbeleid en de daarvoor benodigde activiteiten als ook de uitvoering en verbetering van het KMS/ISMS besproken, Daar waar nodig worden medewerker van de afdeling kwaliteit betrokken.

De LSO heeft afstemming met de in paragraaf 4.2 en 4.3 genoemde betrokkenen ten behoeve van de kwaliteit van de informatiebeveiliging.

5. Aanpak van informatiebeveiliging [4.4]

BVO NL wil passende informatiebeveiliging bereiken door het toepassen van een Managementsysteem voor Informatiebeveiliging (ISMS) met jaarlijkse verbetercycli, zoals deze ook worden toegepast in het kwaliteitsmanagement, bekend als de Plan-Do-Check-Act-cyclus. Het KMS/ISMS is hiervoor de basis.

Het Informatiebeveiligingsbeleid wordt driejaarlijks geëvalueerd en opnieuw vastgesteld en tussentijds wanneer de actuele situatie daarom vraagt.

6. Monitoring en borging

6.1 Voorwaarde voor een succesvolle informatiebeveiliging

Alle medewerkers van BVO NL worden geacht de gemaakte IB-afspraken na te leven. Deze afspraken, vastgelegd in beleid, procedures en werkinstructies worden na vaststelling bekend gemaakt via intranet. Alle medewerkers worden geacht het handboek regelmatig te raadplegen en de inhoud van nieuwe of aangepaste relevante IB-documentatie te kennen.

6.2 Monitoring

1. Het naleven van het IB-beleid, procedures en werkinstructies wordt gemonitord. De wijze waarop gemonitord wordt staat beschreven in 'Gedragscode gebruik ICT-middelen BVO NL',
2. Het vastgestelde niveau van informatiebeveiliging wordt middels periodiek gegenereerde managementrapportages bewaakt,
3. Wekelijkse rapportages die automatisch vanuit een auditingtool worden gestuurd geven inzicht in eventuele afwijkingen op de gedocumenteerde inrichting op netwerkniveau,
4. Periodieke checks op basis van de door de systeemeigenaren vastgestelde autorisaties (matrixen) brengen eventuele discrepanties in de toegekende autorisaties aan het licht,
5. Periodieke checks op basis van de gedocumenteerde autorisaties die toegang geven tot de mappenstructuur en checks op de Active Directory accountdatabase,
6. Interne en externe audits tonen aan of, en zo ja, welke hiaten er met betrekking tot informatiebeveiliging bestaan.

6.3 Borging

Het vastgestelde niveau van informatiebeveiliging wordt geborgd door:

1. Het gebruik van een verbeterregister.

- Geconstateerde afwijkingen die door monitoring aan het licht zijn gekomen, worden geregistreerd in het afwijkingenregister. Middels een risicoweging wordt bepaald of de geconstateerde afwijkingen dusdanige risico's voor de organisatie opleveren dat deze behandeld dienen te worden [A16.1.5] [A16.1.6],

2. Directiebeoordeling.

- De bestuurder beoordeelt jaarlijks de effectiviteit van het KMS/ISMS. Eventuele tekortkomingen worden vertaald naar verbetermaatregelen [A5.1.2].

7. Publicatie en wijzigingen

Dit document staat voor alle medewerkers ter inzage op het intranet en wordt op aanvraag ter beschikking gesteld aan stakeholders, zoals cliënten. Dit document wordt periodiek geactualiseerd. De geactualiseerde versie wordt door de bestuurder of diens gedelegeerde op het intranet gepubliceerd en de medewerkers worden daarop geattendeerd. [A5.1.1]

8. Bijlage: IB- en privacy documenten

Naam document	Vastgesteld door RvB d.d.
Automatiseringsplan	
Bedrijfscontinuïteitsplan	
Data-integriteit binnen BVO NL	
Encryptie en maatregelen	
Fysiek toegangsbeleid BVO NL	
Gedragscode gebruik ICT-middelen BVO NL	
ICT middelenbeleid BVO NL	
ICT middelenmatrix BVO NL	
Informatiecategorieën	
Meldinginbreuk in verband met persoonsgegevens	
Softwareselectie en -acceptatie	
Toegangsbeveiliging informatiesystemen	
Verklaring van toepasselijkheid NEN7510:2017+A1:2020	
Verlenen externe toegang aan beheerpartijen	
Wachtwoordbeleid BVO NL	

Dit overzicht wordt in een later stadium verder aangevuld zodra bepaald is welke documenten gebruikt worden binnen BVO NL.