Bijlage 7b

Strategisch Informatiebeveiligings- en privacybeleid Gemeenschappelijke regeling Blink

2025 t/m 2028

26 september 2025
Harry van Montfort
Afdeling Financiën en Control

Versiebeheer

Versie	Datum	Door	Wijzigingen
1.0	26-09-2025	H. van Montfort	Eerste versie

Inhoud

Versiebeheer 2

1. Inleiding 4

1.1 Leeswijzer 4

1.2 Informatiebeveiliging 4

1.3 Privacy & Gegevensbescherming (AVG) 4

1.4 Ambitie en visie van Blink op het gebied van informatieveiligheid en privacy 5

2. Strategisch beleid 7

2.1 Doelen 7

2.2 Ontwikkelingen 7

2.2.1 De BIO 7

2.2.2 De AVG 7

2.2.3 De NIS2 7

2.2.4 Het bestuur en de 10 principes voor informatiebeveiliging 8

2.2.5 Dreigingsbeeld Informatiebeveiliging Nederlandse Gemeenten 8

2.2.6 Informatie uit incidenten, afwijkingen, inbreuken op de beveiliging en datalekken 8

2.3 Standaarden informatiebeveiliging 8

2.4 Plaats van het strategisch beleid 9

2.5 Scope informatiebeveiliging en privacy 9

2.6 Uitgangspunten 9

2.6.1 Belangrijkste uitgangspunten 10

2.6.2 IB&P governance 10

2.6.3 Randvoorwaarden 12

3. Organisatie, taken & verantwoordelijkheden 13

3.1 Aansturing: directieteam 13

3.2 Uitvoering: afdelingsmanagers 13

3.3 Controle en verantwoording 14

4. Vaststelling, eigenaarschap, herziening 15

1. Inleiding

Deze beleidsnota beschrijft het strategisch informatiebeveiligings- en privacybeleid (IB&P beleid) voor de jaren 2025 t/m 2028.
Deze nota is richtinggevend en kaderstellend en wordt aangevuld met onderwerp-specifieke beleidsdocumenten voor informatiebeveiliging en privacy op tactisch niveau en werkinstructies op operationeel niveau.

Met dit strategisch Informatiebeveiligingsbeleid zet Gemeenschappelijke regeling Blink (hierna: 'Blink') een volgende stap om de beveiliging van persoonsgegevens en andere informatie binnen de organisatie te continueren en voort te gaan op de stappen die in de voorgaande jaren gezet zijn.

De basis voor dit strategisch beleid vormen ISO 27002 en de daarvan afgeleide Baseline Informatiebeveiliging Overheid (BIO), aangevuld met de 10 principes voor informatiebeveiliging en de Algemene Verordening Gegevensbescherming (AVG).

1.1 Leeswijzer

In hoofdstuk 2 wordt de kern van het strategisch beleid uiteengezet. Dit beleid wordt op tactisch niveau aangevuld met onderwerp-specifieke tactische beleidsregels die aanvullend zijn op dit strategisch beleid. In het jaarlijks uit te brengen Informatiebeveiligings- en privacy plan (vastgesteld door de directie) worden deze tactische en operationele aspecten van informatiebeveiliging en privacy verder uitgewerkt en geconcretiseerd. Dit wordt gedaan op basis van input van de afdelingsmanagers, de CISO, de privacyfunctionarissen (PO en FG), het dreigingsbeeld Nederlandse gemeenten van de IBD en de uitkomsten van risicoanalyses en DPIA's. Daarin staan dan ook de acties en planning vermeld, om de praktijk in overeenstemming te brengen met datgene wat in het beleid is geëist. Hoofdstuk 3 beschrijft vervolgens hoe de taken en verantwoordelijkheden in de organisatie belegd zijn.

1.2 Informatiebeveiliging

Onder informatiebeveiliging wordt verstaan het treffen en onderhouden van een samenhangend pakket van maatregelen om de betrouwbaarheid van de informatievoorziening aantoonbaar te waarborgen. Kernpunten daarbij zijn beschikbaarheid, integriteit (juistheid) en vertrouwelijkheid van (persoons)gegevens en andere informatie.
Het informatiebeveiligingsbeleid geldt voor alle processen van Blink en borgt daarmee de beschikbaarheid, integriteit en vertrouwelijkheid van de informatievoorziening gedurende de hele levenscyclus, ongeacht de toegepaste technologie en ongeacht het karakter van de informatie. Het beperkt zich niet alleen tot de ICT en heeft betrekking op alle belanghebbenden, waaronder bestuur, alle medewerkers, burgers, gasten, bezoekers en externe relaties.

1.3 Privacy & Gegevensbescherming (AVG)

Blink werkt met (persoons)gegevens van inwoners, medewerkers, ondernemers en medewerkers van in Blink participerende gemeenten en van (keten)partners van Blink. Deze gegevens verzamelt Blink voor het goed kunnen uitvoeren van de gedelegeerde gemeentelijke wettelijke taken. Om als organisatie deze taken goed uit te voeren zijn persoonsgegevens noodzakelijk.

Bij de omgang met persoonsgegevens van inwoners en personeel heeft Blink een grote verantwoordelijkheid. Privacy is een essentieel en complex vraagstuk. Dit komt onder andere door

de toenemende digitalisering van de samenleving en dienstverlening van Blink, de gegevensuitwisseling met (keten)partners, de technische mogelijkheden en veranderende wetgeving. Privacy raakt de hele Blink-organisatie en verdient, samen met informatiebeveiliging, continu aandacht. De inwoner moet erop kunnen vertrouwen dat Blink zorgvuldig en veilig met deze persoonsgegevens omgaat.

1.4 Ambitie en visie van Blink op het gebied van informatieveiligheid en privacy

De primaire dienstverlening van Blink richt zich op vier taken:
1) afvalinzameling,
2) grondstoffenmanagement en -verwerking,
3) beheer van de openbare ruimte en
4) beleidsadvisering en -implementatie.
Blink streeft naar duurzaamheid, efficiëntie, effectiviteit en informatieveiligheid bij het uitvoeren van deze taken. Op de lange termijn wil Blink zich ontwikkelen tot een kennisorganisatie.

Om de ambities van Blink waar te maken is een solide inrichting van informatiebeveiliging noodzakelijk. Hierbij is de ambitie om in 2028 niveau 4 te bereiken van het onderstaande volwassenheidsmodel van NBA-LIO/NOREA.

Classificatie conform het volwassenheidsmodel NBA-LIO/NOREA

Zodra niveau 4 bereikt is, heeft Blink informatieveiligheid geborgd binnen haar processen. Zij voldoet aan het eigen informatiebeveiligings- en privacybeleid, wet- en regelgeving én heeft voldoende kennis om proactief op ontwikkelingen te anticiperen. Zij weet haar risico's te verkleinen tot een acceptabel niveau. Noodzakelijke randvoorwaarden om deze groei te bereiken, zijn de beschikbaarheid van kwalitatieve en kwantitatieve resources op de afdelingen en bij onze ICT-partners, en een planmatige, risico gebaseerde aanpak, waarbij de principes van continu verbeteren (PDCA-cyclus) aantoonbaar worden gehanteerd.

Dit strategische informatiebeveiligingsbeleid 2025-2028 is het kader om bedrijfsinformatie te beschermen en draagt bij aan een verdere professionalisering van informatiebeveiliging.
Het strategische informatiebeveiligingsbeleid is primair gericht op het bereiken van een passend niveau van informatiebeveiliging en privacybescherming d.w.z. aansluitend bij de eisen en wensen van de organisatie, belanghebbenden en wet- en regelgeving. Als onderdeel van deze visie stuurt Blink op:

- Het verstevigen van de governance
  De verantwoordelijkheid voor informatieveiligheid is primair in de lijn belegd. Dit betekent een centrale rol voor afdelingsmanagers.
- Risico gebaseerd sturen
  Dit betekent dat het management verantwoordelijk is voor het identificeren van de hoogste risico's, het prioriteren van de risico's en het treffen van maatregelen om deze risico's terug te brengen.
- Integratie in de planning- en control cyclus
  Dit betekent dat informatieveiligheid dient te worden opgenomen in de integrale planning en control cyclus. Implementatie en verantwoording vindt plaats via de planning zoals opgenomen in de bedrijfsvoering kalender. Er vindt een uniforme verantwoording plaats aan interne en externe toezichthouders.

2. Strategisch beleid

2.1 Doelen

De strategische doelen van het informatiebeveiligings- en privacybeleid (IB&P-beleid) zijn:

- Het managen van de informatiebeveiliging.
- Adequate bescherming van bedrijfsmiddelen en persoonsgegevens.
- Het toepassen van dataminimalisatie.
- Het minimaliseren van risico's van menselijk gedrag.
- Het voorkomen van ongeautoriseerde toegang.
- Het garanderen van correcte en veilige informatievoorzieningen.
- Het beheersen van de toegang tot informatiesystemen.
- Het waarborgen van veilige informatiesystemen.
- Het adequaat reageren op incidenten.
- Het beschermen van (kritieke) bedrijfsprocessen.
- Het beschermen en correct verwerken van persoonsgegevens van burgers en medewerkers.
- Voldoen aan de wettelijke verplichtingen voortvloeiend uit de AVG en dit op ieder moment met bewijs kunnen aantonen.
- Het waarborgen van de naleving van dit beleid.

2.2 Ontwikkelingen

De ontwikkelingen die van belang zijn voor het IB&P beleid zijn de volgende:

2.2.1 De BIO

De BIO (Baseline Informatiebeveiliging Overheid) is het normenkader voor de gehele overheid. De werkwijze van deze BIO is gericht op risicomanagement. Dat wil zeggen dat de afdelingsmanagers nu meer dan vroeger moeten werken volgens de aanpak van BIO en de ISO27001 norm en daarbij is risicomanagement van belang. Dit houdt voor het management in, dat men op voorhand keuzes maakt en continu afwegingen maakt of informatie in bestaande en nieuwe processen adequaat beveiligd is in termen van beschikbaarheid, integriteit en vertrouwelijkheid.

2.2.2 De AVG

Nieuwe technologische ontwikkelingen, innovatieve voorzieningen, globalisering en een steeds digitaler wordende overheid maakt het zorgvuldig omgaan met persoonsgegevens steeds complexer en noodzakelijker. Blink is zich hiervan bewust en wil daarom met dit beleid aangeven hoe zij in algemene zin invulling geeft aan nationale en Europese wet- en regelgeving op het gebied van privacy, waaronder de Algemene Verordening Gegevensbescherming (hierna te noemen: AVG).

2.2.3 De NIS2

Sinds 17 oktober 2024 is in de Europese Unie de NIS2 richtlijn van kracht. Dit is een Europese wet die tot doel heeft om de digitale- en economische weerbaarheid te vergroten. De NIS2 richtlijn wordt in de lidstaten van de Europese unie vertaald in nationale wetgeving. In Nederland is die vertaling in de Cyberbeveiligingswet (Cbw) nog niet gereed; volgens de laatste verwachtingen (bron: NCTV) zal deze in kwartaal 2 van 2026 in werking treden. De Cbw/NIS2 wordt van toepassing op Blink en dit betekent dat er aantoonbaar voldaan moet worden aan de verplichtingen van de NIS2, zoals Zorgplicht, Meldplicht en Toezicht. De BIO wordt onderdeel van de zorgplicht van NIS2

voor de overheid. Het voldoen aan de BIO en andere bestaande kaders voor informatiebeveiliging bij de overheid, zijn dus een belangrijk beginpunt.

2.2.4 Het bestuur en de 10 principes voor informatiebeveiliging

De 10 principes voor informatiebeveiliging zijn een bestuurlijke aanvulling op het normenkader BIO en gaan over de waarden die de bestuurder (in casu het Dagelijks Bestuur van Blink) zichzelf oplegt. De principes zijn als volgt:

1. Bestuurders bevorderen een veilige cultuur.
2. Informatiebeveiliging is van iedereen.
3. Informatiebeveiliging is risicomanagement.
4. Risicomanagement is onderdeel van de besluitvorming.
5. Informatiebeveiliging behoeft ook aandacht in (keten)samenwerking.
6. Informatiebeveiliging is een proces.
7. Informatiebeveiliging kost geld.
8. Onzekerheid dient te worden ingecalculeerd.
9. Verbetering komt voort uit leren en ervaring.
10. Het bestuur controleert en evalueert.

De principes gaan vooral over de rol van het bestuur bij het borgen van informatiebeveiliging in de Blink-organisatie. Deze principes ondersteunen de bestuurder bij het uitvoeren van goed risicomanagement. Als er iets verkeerd gaat met betrekking tot het beveiligen van de informatie binnen de bedrijfsprocessen van Blink, dan kan dit directe gevolgen hebben voor inwoners, medewerkers, ondernemers, in Blink participerende gemeenten en partners van Blink. Daarmee is het onderwerp informatiebeveiliging nadrukkelijk een onderdeel op de agenda van het Dagelijks Bestuur.

2.2.5 Dreigingsbeeld Informatiebeveiliging Nederlandse Gemeenten

Het Dreigingsbeeld Informatiebeveiliging Nederlandse Gemeenten geeft een actueel zicht op incidenten en factoren uit het verleden, aangevuld met een verwachting voor het heden en de nabije toekomst. Dit dreigingsbeeld is daarmee het ideale document om focus aan te brengen in het actualiseren van beleid en plannen voor informatiebeveiliging van Blink. Het helpt ons om inzicht te krijgen in digitale dreigingen en de impact daarvan op de organisatie. Daarnaast is het een waardevol instrument voor de CISO en de Functionaris Gegevensbescherming om management, directie en bestuur effectief te adviseren over digitale risico's. Het dreigingsbeeld wordt door Blink gebruikt bij de implementatie van ons beleid om efficiënt, effectief, zorgvuldig en vooral ook veilig te kunnen werken.

2.2.6 Informatie uit incidenten, afwijkingen, inbreuken op de beveiliging en datalekken

Blink kent naast het hierboven genoemde dreigingsbeeld een eigen systeem waarin incidenten worden vastgelegd. Dit systeem geeft ook waardevolle informatie om van te leren en dus zijn incidenten uit het verleden ook nadrukkelijk input bij het actualiseren van het beleid. Dit geldt ook voor afwijkingen die bijvoorbeeld bij audits, testen en management reviews worden vastgesteld.

2.3 Standaarden informatiebeveiliging

De basis voor de inrichting van het beveiligingsbeleid is ISO 27001. De maatregelen worden op basis van best practices bij (lokale) overheden en ISO 27002 genomen.
Voor de ondersteuning van gemeenten bij het formuleren en realiseren van hun informatiebeveiligingsbeleid heeft de interbestuurlijke werkgroep Normatiek in 2018 de Baseline

Informatiebeveiliging Overheid (BIO) uitgebracht, afgeleid van beide NEN-normen. Deze BIO bestaat uit een baseline met verschillende niveaus van beveiligen. Het niveau van beveiliging dat voor Blink van toepassing is zal worden vastgesteld aan de hand van een verplichte Baseline Beveiligingstoets (BBN-toets).
Blink heeft, als gemeenschappelijke regeling, de inhoud en structuur van het IBP-beleid ook afgestemd op die van de BIO. Ook het Informatiebeveiligings- en privacyplan zal deze structuur volgen.
Binnen Blink wordt naast ICT ook Operationele Technologie (OT) ingezet. Met OT worden systemen bedoeld voor de besturing van apparaten door middel van Proces Automatisering (PA). Het IBP-beleid van Blink is ook van toepassing op PA en op beleidsafdelingen die zich met PA bezighouden. Ten aanzien van PA gebruikt Blink naast onderhavig beleid ook de Cybersecurity Implementatie Richtlijn (CSIR).

2.4 Plaats van het strategisch beleid

Het strategisch beleid wordt gebruikt om de basis te leggen voor de tactische beleidsplannen en daarmee richting te geven voor de verdere invulling van informatiebeveiliging en privacy op tactisch en operationeel niveau.
Deze beleidsnota beschrijft op strategisch niveau het informatiebeveiligings- en privacybeleid. Dit beleid zal worden vertaald in aanvullend beleid en tactische en operationele richtlijnen en maatregelen. De daaruit voortkomende werkzaamheden worden uitgewerkt in het jaarlijks te schrijven 'Informatiebeveiligings- en privacyplan'.

2.5 Scope informatiebeveiliging en privacy

De scope van deze beleidsnota omvat alle Blink bedrijfsprocessen, organisatieonderdelen, objecten, onderliggende informatiesystemen, procesautomatisering, informatie en (persoons)gegevens(verzamelingen) van Blink, het gebruik daarvan door medewerkers en (keten)partners in de meest brede zin van het woord, ongeacht locatie, tijdstip en gebruikte apparatuur.
Het Dagelijks Bestuur is eindverantwoordelijke voor de informatiebeveiliging en privacy. Dit geldt voor alle Blink informatie- en PA-systemen ongeacht waar deze worden gehost.
Dit strategisch Informatiebeveiligingsbeleid is een algemene basis en dekt tevens aanvullende beveiligingseisen uit wetgeving af zoals voor de AVG, UAVG en NIS2.
Bewust wordt in het strategisch beleid geen uitputtend overzicht van onderliggende documenten opgenomen. In de onderliggende documenten wordt de link naar het strategisch beleid gelegd.

2.6 Uitgangspunten

Het Bestuur, de directie en het afdelingsmanagement spelen een cruciale rol bij het uitvoeren van dit strategische IB&P beleid. Het management[1] maakt een inschatting van het belang dat de verschillende delen van de informatievoorziening voor Blink heeft en de (privacy) risico's (uitgedrukt in kans en impact) die Blink hiermee loopt. Op basis hiervan zet het management dit beleid voor informatiebeveiliging en privacy op, draagt dit uit naar de organisatie en ondersteunt en bewaakt de uitvoering ervan.
Het gehele management geeft een duidelijke richting aan informatiebeveiliging en privacy en demonstreert dat zij informatiebeveiliging en privacybescherming ondersteunt en zich hierbij

[1] Het Management Team van Blink bestaat uit directeur, hoofd Operatie, hoofd P&O, hoofd Financiën en Control, Beleidsadviseur/relatiebeheerder.

betrokken voelt, door het uitdragen en handhaven van een IB&P beleid van en voor de hele organisatie en al haar activiteiten. Het IB&P beleid is in lijn met het algemene beleid en de doelstellingen van Blink en met de relevante landelijke en Europese wet- en regelgeving.

2.6.1 Belangrijkste uitgangspunten

De belangrijkste uitgangspunten van het beleid zijn:

- De uitvoering van de informatiebeveiliging en privacybescherming is een verantwoordelijkheid van het lijnmanagement. Alle informatiebronnen en -systemen die gebruikt worden door Blink hebben een interne eigenaar die de vertrouwelijkheid, privacyeisen en/of waarde bepaalt van de informatie die ze bevatten. De primaire verantwoordelijkheid voor de bescherming van informatie ligt dan ook bij de eigenaar van de informatie. Bij Blink is dit de proceseigenaar, die tevens verantwoordelijk is voor de informatie die in zijn/haar proces wordt gebruikt.
- Door periodieke controle, organisatiebrede planning én coördinatie wordt de kwaliteit van de informatievoorziening en privacy verankerd binnen de organisatie. Het IB&P beleid vormt samen met het IB&P plan het fundament onder een betrouwbare en veilige informatievoorziening en privacybescherming. In het IB&P plan wordt de beschikbaarheid, integriteit en vertrouwelijkheid van de informatievoorziening en privacy organisatiebreed vastgesteld. Het plan wordt periodiek bijgesteld op basis van nieuwe ontwikkelingen, registraties in het incidentenregister, vastgestelde afwijkingen en risicoanalyses voor informatiebeveiliging en privacy.
- Informatiebeveiliging en privacybescherming is een continu verbeterproces. Door middel van de PDCA-cyclus ‘Plan, do, check en act’ geeft Blink hier invulling aan.
- Blink stelt de benodigde mensen en middelen beschikbaar om haar eigendommen en werkprocessen te kunnen beveiligen en te voldoen aan de privacy-eisen volgens de wijze zoals gesteld in dit beleid en de van toepassing zijnde wet- en regelgeving.
- Richtlijnen, procedures, werkwijzen en verantwoordelijkheden voor het IB&P beleid dienen te worden vastgelegd en vastgesteld.
- Iedere medewerker, zowel vast als tijdelijk, intern of extern, is verplicht waar nodig (persoons)gegevens en informatiesystemen te beschermen tegen ongeautoriseerde toegang, gebruik, verandering, openbaring, vernietiging, verlies of overdracht en bij vermeende inbreuken hiervan melding te maken.
- Het borgen van informatiebeveiliging en privacy in de uitvoering van bedrijfsprocessen vindt risico gestuurd plaats. De verantwoordelijken in de organisatie maken afwegingen ter naleving van privacyregels en op basis van een risico-inschatting.

2.6.2 IB&P governance

Praktisch wordt als volgt invulling gegeven aan de uitgangspunten:

- Het Dagelijks Bestuur stelt als eindverantwoordelijke het strategisch IB&P beleid vast.
- De directie stelt jaarlijks het IB&P plan vast.
- De directie is verantwoordelijk voor het (laten) uitwerken en uitvoeren van onderwerp specifieke tactische beleidsregels die aanvullend zijn op dit strategisch beleid.
- Vastgestelde beleidsstukken en uitwerkingen daarvan (bijv. procedures, standaarden en werkinstructies) worden centraal beheerd in het managementsysteem voor informatiebeveiliging en privacybescherming.
- De directie is verantwoordelijk voor het vragen om informatie bij de afdelingsmanagers. Dit wordt vormgegeven door het opleggen van een periodieke rapportageverplichting die het voor de directie mogelijk maakt om erop toe te zien dat de afdelingsmanagers adequate maatregelen genomen hebben voor de bescherming van de (persoons)gegevens, informatiesystemen en procesautomatiseringsystemen die onder hun verantwoordelijkheid valt.

- De Chief Information Security Officer (CISO) ondersteunt vanuit een onafhankelijke positie de organisatie bij het bewaken en verhogen van de betrouwbaarheid van de informatiebeveiliging, is als zodanig ook gevraagd en ongevraagd adviseur van het Bestuur en de Directie. De CISO rapporteert ieder kwartaal en voorafgaande aan de P&C gesprekken over de voortgang van activiteiten op het gebied van het bewaken en verhogen van de informatiebeveiliging rechtstreeks aan de directie.
- Van deze P&C gesprekken worden door de directie verslagen gemaakt, die met betrekking tot de aspecten die te maken hebben met informatiebeveiliging worden vastgelegd in het managementsysteem voor informatiebeveiliging.
- De Functionaris voor Gegevensbescherming (FG) is verantwoordelijk voor het intern onafhankelijk toezien op - en gevraagd en ongevraagd adviseren van het Bestuur over de juiste en zorgvuldige omgang met persoonsgegevens zoals de AVG voorschrijft. De FG brengt een jaarverslag aan het Bestuur uit, waarin hij zijn bevindingen en aanbevelingen vastlegt. Indien door hem gewenst of noodzakelijk rapporteert de FG ook met een hogere frequentie of incidenteel aan het Bestuur.
- De directie en de afdelingsmanagers stellen proactief informatie over de bescherming van persoonsgegevens ter beschikking aan de FG. Desgevraagd verstrekken zij aanvullende informatie aan de functionaris gegevensbescherming.
- De FG en de CISO communiceren met elkaar over aspecten van informatiebeveiliging en privacybescherming die van belang zijn in het kader van de juiste uitvoering van hun taken. Zij richten hiervoor zelf de benodigde communicatielijnen in.
- Tijdens Planning & Control-gesprekken dient er aandacht te zijn voor de informatiebeveiliging en privacy n.a.v. de rapportage van de CISO en/of de FG. Dit wordt geborgd door de onderwerpen Informatiebeveiliging en Privacybescherming toe te voegen aan de agenda van de Planning & Control-gesprekken. De onderwerpen, die door de CISO en/of de FG als risicovol worden gezien, moeten tevens worden opgenomen in de auditplannen die minimaal jaarlijks worden opgesteld en goedgekeurd door de directie.
- De afdelingsmanagers zijn verantwoordelijk voor de uitvoering van de informatiebeveiliging voor de processen waarvoor zij verantwoordelijk zijn.
- De afdelingsmanagers zijn verantwoordelijk voor de borging van de AVG binnen de processen waarvoor zij verantwoordelijk zijn en het bijbehorende verwerkingsregister. De kwaliteit van het verwerkingsregister wordt minimaal jaarlijks getoetst door de FG als onderdeel van diens toezichthouden taken. De afdelingsmanagers zijn verplicht om eventuele aanwijzingen van de FG naar aanleiding van deze kwaliteitstoetsing op te volgen.
- De afdelingsmanagers zijn verantwoordelijk voor het oefenen met informatiebeveiligings- en privacy incidenten en bedrijfscontinuïteit. Hiervoor wordt jaarlijks een programma opgesteld en over de verplichte uitvoering van dit programma wordt door de afdelingsmanagers gerapporteerd aan de directie.
- Alle medewerkers van Blink worden getraind in het gebruik van informatiebeveiligings-procedures en procedures voor bescherming van persoonsgegevens en dienen deze procedures steeds toe te passen, zodat er steeds bewust en op een veilige wijze wordt omgegaan met persoonsgegevens en informatie. De genoemde trainings- en bewustwordingsprogramma's worden jaarlijks vastgesteld als onderdeel van het IBP-jaarplan.
- Afdelingsmanagers dienen erop toe te zien dat de controle op het verwerken van persoonsgegevens en informatie regelmatig wordt uitgevoerd, zodat zij kunnen vaststellen dat alleen rechthebbende medewerkers de juiste persoonsgegevens en informatie ingezien en verwerkt hebben.
- De beveiligingsmaatregelen worden bepaald op basis van risicomanagement. Afdelingsmanagers voeren quickscans informatiebeveiliging uit op basis van de BIO en bij het

verwerken van persoonsgegevens tevens (Pre-)DPIA's uit op basis van de AVG om deze risico-afwegingen te kunnen maken.
- Informatiebeveiliging en privacybescherming maakt deel uit van de beoordelingssystematiek en wordt besproken tussen de manager en de medewerker. Van deze bespreking vindt vastlegging plaats.
- De directie zorgt ervoor dat in plannen voor bedrijfscontinuïteit aandacht wordt besteed aan informatiebeveiliging en privacybescherming en dat deze ook tijdens een crisissituatie moet worden gehandhaafd.

2.6.3 Randvoorwaarden

Belangrijke randvoorwaarden zijn:
- Informatiebeveiliging- en privacy-eisen maken deel uit van afspraken met ketenpartners, leveranciers en gemeenschappelijke regelingen en worden periodiek geëvalueerd/ gecontroleerd. Hierover wordt door het management gerapporteerd aan de directie.
- Kennis en bewustzijn van informatiebeveiliging en privacybescherming en omgaan met persoonsgegevens binnen de organisatie dienen actief bevorderd en geborgd te worden.
- Jaarlijks wordt een IB&P plan opgesteld door de directie, gebaseerd op:
  - Dit IB&P beleid;
  - Andere audit resultaten;
  - Uitkomsten van de behandeling van informatiebeveiligings- en privacy incidenten;
  - het dreigingsbeeld gemeenten van de IBD;
  - Uitkomsten risicoanalyses en DPIA's
  - De door de afdelingsmanagers ingebrachte onderwerpen voor de informatievoorziening waarvoor zij verantwoordelijk zijn, bijvoorbeeld als uitkomst van een risicoanalyse of een privacy analyse (DPIA).
- Jaarlijks wordt een plan opgesteld voor communicatie over informatiebeveiliging en privacybescherming. In dit plan worden inhoud, frequentie, doelgroepen en middelen van deze communicatie opgenomen.
- Om uitvoering te kunnen geven aan dit strategisch beleid en het IB&P plan worden voldoende financiële middelen en uitvoeringscapaciteit ter beschikking gesteld.

3. Organisatie, taken & verantwoordelijkheden

In dit hoofdstuk wordt uiteengezet welke taken en verantwoordelijkheden met betrekking tot informatiebeveiliging en privacy op welke plaats belegd zijn binnen de organisatie. De methodiek sluit aan bij het in de bedrijfsvoering bekende 'Three Lines Model' (eerder bekend als 'Three Lines of Defense'). In dit model is het lijnmanagement verantwoordelijk voor het realiseren van informatiebeveiliging en privacy binnen de eigen processen. De tweede lijn (bijvoorbeeld CISO, security officers, PO) ondersteunt, adviseert, coördineert en bewaakt of het management zijn verantwoordelijkheden ook daadwerkelijk neemt. In de derde lijn wordt het geheel door een (interne) auditor en/of FG van een objectief oordeel voorzien met mogelijkheden tot verbetering.

3.1 Aansturing: directieteam

De directie zorgt dat alle (persoons)gegevens, processen en systemen en de daarbij behorende middelen altijd onder de verantwoordelijkheid vallen van een afdelingsmanager. De directie zorgt dat de afdelingsmanagers zich verantwoorden over de beveiliging en bescherming van de privacy van de (persoons)gegevens of andere informatie die onder hen berust. De directie zorgt dat het Dagelijks Bestuur gevraagd en ongevraagd geïnformeerd wordt over de mate waarin informatiebeveiliging en privacybescherming een onderdeel is van het handelen van de bedrijfsvoering. Op die manier kan het Dagelijks Bestuur zich ook verantwoorden naar het Algemeen Bestuur.

De directie stelt het gewenste niveau van continuïteit en vertrouwelijkheid vast. De directie draagt zorg voor het uitwerken van tactische informatiebeveiligings- en privacybeleidsonderwerpen en laat zich hierin bijstaan door de CISO en PO van Blink. De directie autoriseert de benodigde procedures en uitvoeringsmaatregelen. Het onderwerp informatiebeveiliging en privacybescherming wordt binnen Blink gezien als een integraal onderdeel van risicomanagement.

3.2 Uitvoering: afdelingsmanagers

Informatiebeveiliging en privacy valt onder de verantwoordelijkheden van alle afdelingsmanagers. Om deze verantwoordelijkheid waar te maken dienen zij goed ondersteund te worden vanuit de tweede lijn. Deze verantwoordelijkheid kunnen zij niet delegeren, uitvoerende werkzaamheden wel. De bedoeling is dat alle processen, systemen, (persoons)gegevens, applicaties altijd minimaal één eigenaar hebben; er moet dus altijd iemand verantwoordelijk zijn. Afdelingsmanagers rapporteren aan de directie over de door hen tactisch en operationeel uitgevoerde informatiebeveiligings- en privacybeschermende activiteiten. Afstemming met de afdelingen over de inhoudelijke aanpak vindt plaats door minimaal 2 keer per jaar het onderwerp informatiebeveiliging en privacy te bespreken in een bedrijfsvoeringsoverleg (een structureel intern overleg, gericht op de interne organisatie en ondersteuning).

Taken van de afdelingsmanagers in het kader van informatiebeveiliging en privacybescherming zijn:

- Het leveren van input voor wijzigingen op maatregelen en procedures.
- Het voldoen aan wet- en regelgeving die op hun processen van toepassing is en invulling geven aan de rollen die binnen die wet- en regelgeving bedacht is.

- Het binnen de eigen afdeling uitdragen van het IB&P beleid, de daaraan gerelateerde procedures.
- Het vroegtijdig signaleren van de voornaamste (privacy)bedreigingen waaraan de bedrijfsinformatie is blootgesteld.
- Het vroegtijdig betrekken van CISO en PO bij nieuwe of gewijzigde processen
- Het (laten) uitvoeren van risicoanalyses en (pre-)DPIA's voor de processen waar zij verantwoordelijk voor zijn.
- Bespreking van beveiligingsincidenten, privacy inbreuken en geconstateerde afwijkingen en de consequenties die dit moet hebben voor beleid en maatregelen.

3.3 Controle en verantwoording

Dit Strategisch IB&P Beleid is een verantwoordelijkheid van het Dagelijks Bestuur van Blink. De bestuurders en directeur van Blink zullen werken volgens de 10 principes voor informatiebeveiliging en de beginselen voor het verwerken van persoonsgegevens. Zij geven sturing geven aan het onderwerp informatiebeveiliging en privacy door het geven van voorbeeldgedrag en het vragen om informatie.
De directie is verantwoordelijk voor het gevraagd en ongevraagd rapporteren over informatiebeveiliging en privacy aan het Dagelijks Bestuur. De directie rapporteert daarnaast over de mate waarin zij invulling hebben gegeven aan het uitwerken van tactische (deel)beleidsonderwerpen die aanvullend zijn op dit strategische beleid.

4. Vaststelling, eigenaarschap, herziening

Dit beleid is vastgesteld op: [datum] door het Dagelijks Bestuur van Gemeenschappelijke regeling Blink.

De eigenaar van dit beleid is het Dagelijks Bestuur van Gemeenschappelijke regeling Blink.

De eigenaar laat dit beleid minimaal 1 maal per 4 jaar, of zoveel vaker als nodig of gewenst is actualiseren door de directie.