BLAD GEMEENSCHAPPELIJKE REGELING

Nr. 1034

4 mei

2026

Officiële uitgave van de gemeenschappelijke regeling Belastingsamenwerking Gemeenten en Waterschappen

Stategisch Informatiebeveiligings- en Privacybeleid BsGW

1. Inleiding

Deze nota beschrijft het strategisch Informatiebeveiligings- en Privacybeleid (IB&P-beleid) voor de jaren 2026 tot en met 2029 en vervangt het in 2020 vastgestelde 'Strategisch Baseline Informatiebeveiligingsbeleid 2020 t/m 2023, beter safe dan sorry'. De looptijd van dit strategisch beleidsplan is op 22 februari 2023 door het MT verlengd tot en met 2025.
Dit strategisch Informatiebeveiligings- en Privacybeleid is richtinggevend en kaderstellend voor alle informatiebeveiligings- en privacyactiviteiten. De basis voor dit strategisch beleid zijn de Baseline Informatiebeveiliging Overheid versie 2 (BIO2) en het VNG Borgingsproduct AVG. De principes die zijn gehanteerd bij het opstellen van dit strategisch beleid, zijn gebaseerd op de 10 bestuurlijke principes voor informatiebeveiliging zoals uitgewerkt door de VNG en de beginselen uit de Algemene Verordening Gegevensbescherming (AVG) voor het verwerken van persoonsgegevens. Het wettelijk kader voor de BIO2 wordt gevormd door de Cyberbeveiligingswet.
Deze nota geeft richting aan de organisatie en biedt ondersteuning aan het bestuur, het managementteam en BsGW-medewerkers bij de sturing op de planning, de uitvoering, het beheer van en de controle op informatieveiligheid en privacy.

1.1 Het belang van informatiebeveiliging en privacy

In vrijwel alle bedrijfsprocessen van BsGW wordt informatie verwerkt. Het betreft ook informatie die vertrouwelijk en privacygevoelig is.
Verlies, misbruik van en/of schade aan informatie kan gevaar opleveren voor de continuïteit van de bedrijfsvoering en kan ook andere consequenties met zich meebrengen, zoals inbreuk op het vertrouwen in (de overheid in het algemeen en) BsGW in het bijzonder, imagoschade, financiële schade, fraude of overtreding van wet- en regelgeving. Voorts kunnen rechten en vrijheden van betrokkenen (belastingplichtigen, medewerkers etc.) in het geding komen.
Met een steeds complexer dreigingsbeeld door toenemende cybercapaciteiten wereldwijd, de snelle ontwikkelingen van (generatieve) AI en de steeds veranderende geopolitiek hebben invloed op de afhankelijkheden en versterken (bestaande) dreigingen voor digitale veiligheid. Het monitoren van het dreigingsbeeld en het nemen van passende organisatorische en technische maatregelen is essentieel voor informatiebeveiliging en de bescherming van persoonsgegevens. Risicomanagement vormt dan ook de kern van informatiebeveiliging en privacy voor BsGW.

1.2 Informatiebeveiliging

Informatiebeveiliging creëert waarde, voorkomt schade en draagt bij aan de organisatiedoelstellingen van BsGW. 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. Bovendien is de controleerbaarheid van belang.
Het informatiebeveiligingsbeleid geldt voor alle processen van BsGW en borgt daarmee de informatievoorziening gedurende de hele levenscyclus van informatiesystemen, ongeacht de toegepaste technologie en ongeacht het karakter van de informatie. Het beperkt zich niet alleen tot de ICT, maar heeft ook betrekking op bestuur, medewerkers, burgers, bezoekers en externe relaties.
Informatiebeveiligingsdienst (IBD)
BsGW sluit zoveel mogelijk aan bij de BIO2-aanpak van de IBD, dat wil zeggen dat BsGW begint met de belangrijkste primaire processen. BsGW volgt de IBD in de verdere stappen, die in gezamenlijkheid uitgewerkt worden. BsGW volgt zo de kracht van het collectief.

1.3 Privacy en gegevensbescherming

BsGW werkt met (persoons)gegevens van inwoners, ondernemers, medewerkers en (keten)partners. Deze gegevens verzamelt BsGW voor het goed kunnen uitvoeren van de aan BsGW gedelegeerde en gemandateerde (wettelijke) taken en om een efficiënte en effectieve bedrijfsvoering te kunnen voeren. Om deze taken goed uit te kunnen voeren zijn persoonsgegevens noodzakelijk.
In de omgang met persoonsgegevens van inwoners en medewerkers heeft BsGW een grote verantwoordelijkheid. Privacy is een essentieel en complex vraagstuk. Dit komt onder andere door de toenemende digitalisering van de samenleving en dienstverlening van BsGW, de overdracht van overheidstaken aan BsGW, de gegevensuitwisseling met (keten)partners, de technische mogelijkheden en veranderende

wetgeving. Privacy raakt de hele organisatie en verdient, samen met informatiebeveiliging, continu aandacht. De klant, van belastingplichtige tot deelnemer, moet erop kunnen vertrouwen dat BsGW zorgvuldig, transparant en veilig met deze persoonsgegevens omgaat.
Waar mogelijk sluit BsGW aan bij de privacyaanpak van de IBD. BsGW maakt ook voor dit aspect gebruik van de kracht van het collectief.

1.4 Leeswijzer
In hoofdstuk 2 worden de doelen en uitgangspunten van het strategisch beleid uiteengezet. Het strategisch beleid wordt vastgesteld door het Dagelijks Bestuur BsGW (Dagelijks Bestuur). Dit wordt aangevuld met onderwerpspecifieke tactische beleidsregels, welke worden opgesteld in opdracht van het verantwoordelijke afdelingshoofd en vastgesteld door het managementteam (MT).
Hoofdstuk 3 beschrijft vervolgens hoe diverse taken en verantwoordelijkheden in de organisatie belegd zijn.

2. Doelen en uitgangspunten

2.1 Ambitie
BsGW wil een digitaal veilige organisatie zijn, die het vertrouwen van inwoners, deelnemende gemeenten en Waterschap Limburg en andere relevante partijen waarborgt.

2.2 Visie
Privacy en informatieveiligheid zijn een gedeelde verantwoordelijkheid binnen de hele BsGW-organisatie. Niet alleen technologie, maar met name ook menselijk gedrag speelt hierin een cruciale rol. Door risico's vroegtijdig te herkennen, bewust vragen te stellen over gegevensgebruik en passende maatregelen te treffen, wordt informatieveiligheid een continu en integraal onderdeel van het werk.

2.3 Missie
BsGW beschermt dagelijks privacygevoelige gegevens van inwoners, organisaties en partners door zorgvuldig, veilig en verantwoord met deze informatie om te gaan. BsGW-medewerkers worden ondersteund in het veilig uitvoeren van hun werk, zodat de continuïteit van processen gewaarborgd blijft.

2.4 Strategische doelen
BsGW is belast met de heffing en inning van lokale heffingen voor zowel de deelnemende gemeenten als het waterschap en is verantwoordelijk voor de uitvoering van de Wet WOZ. Om de hieruit voortvloeiende taken en werkzaamheden uit te voeren is informatie (w.o. persoonsgegevens) nodig. Deze informatie komt in veel vormen voor. Het is een bedrijfsmiddel dat net als andere bedrijfsmiddelen van waarde is voor BsGW en op een passende manier beveiligd moet zijn. Informatiebeveiliging is geen doel op zich maar een integraal onderdeel van het geheel aan processen en informatievoorziening van BsGW.

Het doel van informatiebeveiliging en privacy is het waarborgen van de beschikbaarheid, integriteit, vertrouwelijkheid en controleerbaarheid van persoonsgegevens en ander informatie, die gebruikt wordt binnen het geheel aan processen en informatiesystemen van BsGW, door het opstellen, implementeren en onderhouden van een stelsel van maatregelen.

In deze beleidsperiode richt BsGW zich op de volgende drie pijlers met subdoelen:
1. Risico's beheersen en incidenten voorkomen
- Het managen van informatiebeveiliging.
- Het voorkomen van ongeautoriseerde toegang.
- Het garanderen van correcte en veilige informatievoorzieningen.
- Het beheersen van de toegang tot informatiesystemen.

2. De veiligheid van bedrijfsmiddelen en persoonsgegevens waarborgen
- Adequate bescherming van bedrijfsmiddelen en persoonsgegevens.
- Het toepassen van dataminimalisatie.
- Het waarborgen van veilige informatiesystemen.
- Het beschermen van (kritieke) bedrijfsprocessen.
- Het beschermen en correct verwerken van persoonsgegevens van burgers, medewerkers en andere betrokkenen.

3. Naleving en reactievermogen optimaliseren
- Het minimaliseren van risico's van menselijk gedrag.
- Het adequaat reageren op incidenten.

- Voldoen aan de wettelijke verplichtingen voortvloeiend uit de vigerende kaders en dit op ieder moment met bewijs kunnen aantonen.
- Het waarborgen van de naleving van dit beleid waarbij wordt uitgegaan van de kracht van het collectief.

2.5 Beleidsuitgangspunten

De belangrijkste uitgangspunten van het beleid zijn:

1. BsGW ziet informatie als strategisch bedrijfsmiddel.
   Informatie (w.o. persoonsgegevens) is een bedrijfsmiddel dat net als andere bedrijfsmiddelen op een passende manier beveiligd moet zijn. Hierbij gaat het met name om de beschikbaarheid, de integriteit en de vertrouwelijkheid van de informatie. Aan de hand van classificatie wordt het beveiligingsniveau bepaald en worden passende organisatorische en technische maatregelen getroffen.
   De uitvoering van de informatiebeveiliging en privacybescherming is een verantwoordelijkheid van de afdelingshoofden. Alle informatiebronnen en -systemen die gebruikt worden hebben een gegevens- en systeemeigenaar die de vertrouwelijkheid, beschikbaarheid, integriteit, privacyeisen en/of waarde bepaalt van de informatie die ze bevatten. Medewerkers van de afdeling Bedrijfsvoering bieden hierbij ondersteuning.
2. BsGW voldoet aan en conformeert zich aan geldende wet- en regelgeving.
   Op informatiebeveiliging en privacybescherming is Europese en nationale wet- en regelgeving en overige kaders van toepassing. BsGW conformeert zich aan dit geheel van geldende wet- en regelgeving en treft, indien nodig, maatregelen om hieraan te voldoen.

Kader	*Onderwerp en doel*	*Certificering*
Network and Information Systems-richtlijn (NIS2-richtlijn)	Verhogen van cyberveiligheid binnen de Europese Unie	
Cyberbeveiligingswet (Cbw)	Implementeert de NIS2 in nationale wetgeving	
Baseline Informatiebeveiliging Overheid (BIO2)	Uniforme werkwijze voor informatiebeveiliging (business impact analyse en maatregelensets)	ISO 27001
10 bestuurlijke principes informatiebeveiliging	Aanvulling op de BIO2 van de VNG	
Dreigingsbeeld Informatiebeveiliging Nederlandse Gemeenten	Dit dreigingsbeeld geeft een actueel zicht op incidenten en factoren uit het verleden, aangevuld met een verwachting voor het heden en de nabije toekomst t.b.v. het actualiseren van (uitvoerings)beleid.	
Algemene Verordening Gegevensbescherming (AVG)	Europese wetgeving over de bescherming van persoonsgegevens.	
Uitvoeringswet AVG (UAVG)	Nationale nadere uitwerking van de AVG met specifieke bepalingen en uitzonderingen.	
AI-verordening	Europese wetgeving over het verantwoord ontwikkelen en gebruiken van AI door o.a. overheidsorganisaties, zodat iedereen in Europa erop kan vertrouwen dat AI-systemen veilig werken en dat grondrechten zijn beschermd.	ISO 42001

3. BsGW werkt risicogestuurd.
   BsGW kiest voor een risicogestuurde aanpak conform de aanpak van de IBD. Dit biedt een realistisch groeipad. Bovendien wordt zo voldaan aan de algemeen geldende set aan basismaatregelen conform bovengenoemde kaders. Uit eventuele eigen aanvullende risicoanalyses en Data Protection Impact Assessments (DPIA's) kunnen extra maatregelen voortvloeien. De bevindingen die voortvloeien uit deze methodiek, eventuele eigen aanvullende risicoanalyses en DPIA's worden vastgelegd in het Privacy Security Management System (PSMS) en Information Security Management System (ISMS). Hiermee kunnen concrete risicoprofielen worden gemaakt ten behoeve van de overweging en onderbouwing van besluitvorming. Zowel het Dagelijks Bestuur, de directeur als het MT maken bij alle besluitvorming afwegingen op basis van een risico-inschatting. Passende en tijdige betrokkenheid van belanghebbenden maakt het mogelijk dat hun kennis, opvattingen en percepties in aanmerking worden genomen. Dit resulteert in een verbeterd bewustzijn en goed geïnformeerd risicomanagement.
4. Medewerkers van BsGW zijn bewust bekwaam op het gebied van privacy en informatiebeveiliging. Menselijk gedrag en cultuur beïnvloeden op significante wijze alle aspecten van risicomanagement op elk niveau en in elk stadium. Het is dan ook essentieel dat medewerkers zich bewust zijn van de risico's van het gebruik van analoge en digitale gegevensdragers (applicaties en bestanden). Kennis en bewustwording van informatiebeveiliging en privacy en de naleving ervan heeft continu aandacht. Een gestructureerd communicatie- en bewustwordingsplan is essentieel om deze bewustwording te borgen in de organisatie.
5. BsGW ziet toe op de naleving door ketenpartners en leveranciers.

Van leveranciers van BsGW wordt verwacht dat zij bijdragen aan informatiebeveiliging en privacybescherming van BsGW. Er wordt gewaarborgd dat geleverde producten en diensten niet in strijd zijn met deze beleidsnota en de daaraan ten grondslag liggende wet- en regelgeving. Informatiebeveiligings- en privacyeisen maken deel uit afspraken met ketenpartners, leveranciers en deelnemers en worden periodiek geëvalueerd en gecontroleerd.

6. BsGW maakt de informatievoorziening beheersbaar.
   BsGW voorkomt en beperkt schade door onder meer de impact van een verstoring van (informatie)voorzieningen tijdig in beeld te krijgen zodat adequate maatregelen getroffen kunnen worden. Enerzijds betekent dit dat bij de aanschaf en bij de ontwikkeling van onderdelen van de informatievoorziening rekening gehouden wordt met informatiebeveiligings- en privacyaspecten. Dit uitgangspunt wordt ook wel aangeduid als 'security- en privacy-by-design en by default'. Anderzijds betekent dit dat de bestaande informatievoorziening continu gemonitord wordt op kwetsbaarheden binnen de digitale infrastructuur van BsGW. In geval van kwetsbaarheden wordt actie ondernomen om de risico's zo klein mogelijk te houden. Dit kan betekenen dat de informatievoorziening voor een bepaalde periode op een lager niveau van beschikbaarheid functioneert.
7. BsGW zorgt voor bedrijfscontinuïteit.
   Naast vertrouwelijkheid en integriteit is beschikbaarheid een belangrijk aspect van informatiebeveiliging en privacy. De juiste informatie moet op het juiste moment en op de juiste plaats beschikbaar zijn voor de uitvoering van het betreffende proces. Er worden afspraken gemaakt over de vereiste beschikbaarheid met betrokken partijen bij de levering van de informatievoorziening. De continuïteit van de informatievoorziening maakt integraal onderdeel uit van de bedrijfscontinuïteit. Regels en verantwoordelijkheden worden vastgelegd en vastgesteld.
8. BsGW zet de PDCA-cyclus in voor het bewaken en evalueren van de voortgang.
   Informatiebeveiliging en privacy is een continu verbeterproces. 'Plan, do, check en act' vormen samen het managementsysteem van informatiebeveiliging en privacybescherming. BsGW herijkt bij nieuwe dreigingen of bij wijzigingen in wet- en regelgeving. Aan de hand van deze PDCA-cyclus worden maatregelen ingevoerd, getoetst en indien nodig bijgesteld in een Information Security Management System (ISMS). Onderdeel van het ISMS is ook de registratie van incidenten, inbreuken op de beveiliging en datalekken en de lering uit deze informatie. Het MT wordt hier periodiek over geïnformeerd.
9. BsGW meet voortgang op basis van duidelijke KPI's.
   De voortgang wordt gemeten op basis van duidelijke KPI's. Deze indicatoren vormen de basis voor het Jaarplan Informatiebeveiliging en Privacy. Hierin worden de tactische en operationele aspecten van informatiebeveiliging en privacy verder uitgewerkt en daarmee uitvoering gegeven aan het strategisch beleid. Dit wordt gedaan op basis van input van de afdelingshoofden, de Chief Information Security Officer (CISO), de privacyfunctionarissen (PO en FG), het dreigingsbeeld Nederlandse gemeenten van de Informatiebeveiligingsdienst (IBD) en de uitkomsten van risicoanalyses en DPIA's.
10. BsGW legt verantwoording af over informatiebeveiliging en privacy.
    Het Dagelijks Bestuur legt aan het Algemeen Bestuur van BsGW verantwoording over informatiebeveiliging en privacy af middels de reguliere Planning- en Controlcyclus (P&C-cyclus) op kwartaalbasis in bestuursrapportages en jaarlijks in de (ontwerp)begroting, jaarstukken en het jaarverslag.

2.6 Randvoorwaarden

De basis voor de inrichting van het beveiligingsbeleid is de BIO2. De BIO2 schrijft voor dat risicomanagement ingericht moet worden volgens de norm NEN-EN-ISO/IEC 27001:2023.
De maatregelen worden op basis van best practices bij (lokale) overheden en de norm NEN-EN-ISO/IEC 27002:2022 genomen en zijn aangevuld met de overheidsmaatregelen uit de BIO2. BsGW maakt hierbij gebruik van het ondersteuningsaanbod van de IBD.
Naast de BIO2 en andere kaders op het gebied van informatiebeveiliging en privacy geldt voor overheden ook aanvullende wet- en regelgeving, zoals Wet open overheid (Woo), Wet modernisering elektronisch berichtenverkeer (Wmebv), Wet digitale overheid (Wdo) en de Archiefwet 1995, en voor BsGW als belastingsamenwerking specifieke wet- en regelgeving, zoals de Wet waardering onroerende zaken (Wet WOZ) en de Invorderingswet 1990.
Dit vergt dat jaarlijks de actualiteit van dit strategisch beleid moet worden beoordeeld op basis van veranderende risico's en veranderende wet- en regelgeving.
De CISO en FG stellen jaarlijks het IB&P-plan op. Dit is gebaseerd op:

- dit strategisch IB&P-beleid;
- aanpalend beleid;
- het toezichtplan van de FG;
- de bevindingen uit het toezicht door de FG;
- andere auditresultaten;
- het dreigingsbeeld gemeenten van de IBD;

- bevindingen en uitkomsten uit risicoanalyses en DPIA's (waaronder door de afdelingshoofden ingebrachte onderwerpen over de informatievoorzieningen waarvoor zij verantwoordelijk zijn).

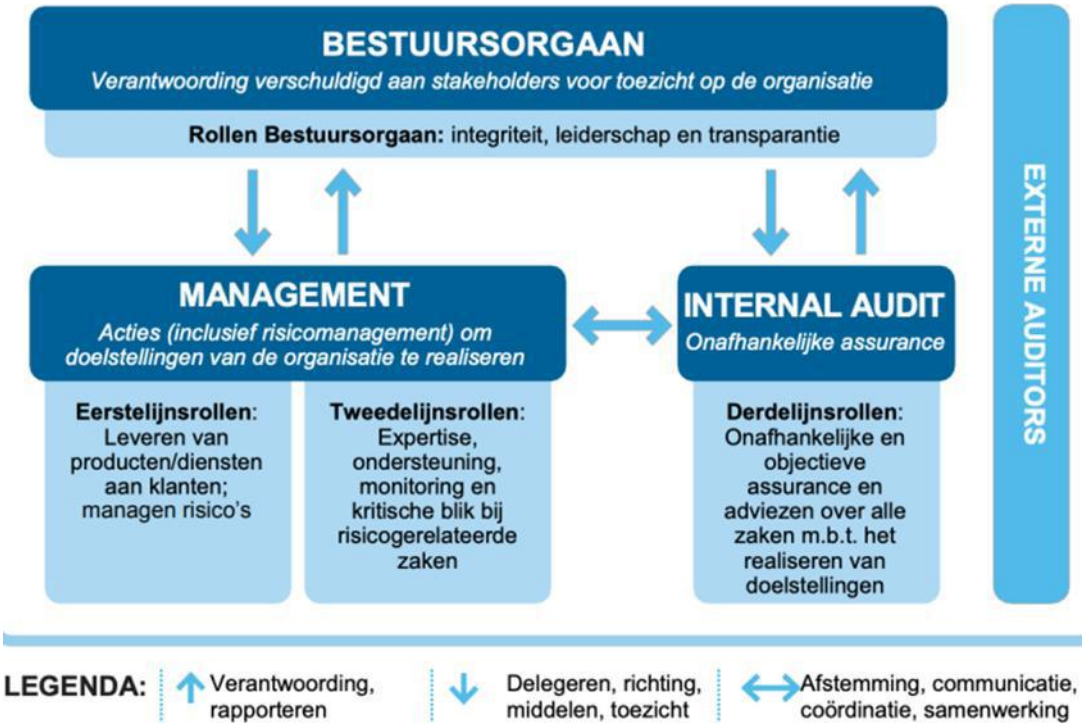
Om uitvoering te kunnen geven aan dit strategisch IB&P-beleid en het IB&P-plan moeten voldoende financiële middelen en uitvoeringscapaciteit door Dagelijks Bestuur ter beschikking worden gesteld.

3. Organisatie, taken en verantwoordelijkheden

Informatiebeveiliging en privacy maken integraal onderdeel uit van alle processen, informatiesystemen, procesautomatisering, informatie en gegevens van BsGW en externe partijen. Informatiebeveiliging en privacy beperken zich dan ook niet alleen tot ICT-gerelateerde zaken.

3.1Three Lines Model

De taken en verantwoordelijkheden met betrekking tot informatiebeveiliging en privacy worden belegd conform 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 (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.



3.2 Verantwoordelijkheden

3.2.1 Dagelijks Bestuur en MT: aansturing

Het Dagelijks Bestuur:

- is integraal verantwoordelijk voor de beveiliging van informatie en de bescherming van persoonsgegevens binnen de werkprocessen van BsGW;
- stelt het strategisch IB&P-beleid vast;
- zorgt ervoor dat ze voldoende kennis heeft om te sturen op dit beleid;
- stelt aanvullend beleid in het kader van informatiebeveiliging en privacy vast;
- wijst de nodige middelen en budget voor de implementatie van het beleid en het bereiken van de doelstellingen toe.

De directeur/het MT:

- stuurt op concernrisico's middels een risicoprofiel van de organisatie en draagt zorg voor het risicomanagementproces op organisatieniveau;
- is verantwoordelijk voor de naleving van alle relevante wet- en regelgeving op strategisch niveau;

- geeft duidelijke richting aan informatiebeveiliging en privacy en draagt deze mee uit;
- stelt het Jaarplan Informatiebeveiliging & Privacy vast en biedt dit ter kennisname aan het Dagelijks Bestuur aan;
- is verantwoordelijk voor de totstandkoming van aanvullend (uitvoerings)beleid;
- evalueert periodiek beleid;
- is verantwoordelijk voor de verantwoording aan het Dagelijks Bestuur over de voortgang van de uitvoering van het strategisch beleid in periodieke rapportages;
- bespreekt minimaal vier keer per jaar het onderwerp informatiebeveiliging en privacy in MT-verband;
- wordt hierbij ondersteund door de betreffende functionarissen van Bedrijfsvoering.

3.2.2 Afdelingshoofden: uitvoering

Informatiebeveiliging en privacy vallen onder de verantwoordelijkheden van de afdelingshoofden. 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.
De afdelingshoofden:

- zijn verantwoordelijk voor de uitvoering van het IB&P-beleid binnen hun afdelingen en zorgen dat de doelstelling op operationeel niveau worden behaald;
- signaleren en identificeren afdelingsspecifieke risico's en implementeren de nodige risicobeheersmaatregelen;
- organiseren en faciliteren trainingen en bewustwordingscampagnes in afstemming met HRM, de CISO, PO en FG voor medewerkers binnen hun afdelingen, gericht op risico's, beveiliging en compliance (of laten dit doen);
- zorgen ervoor dat toegangscontrole en de beveiliging van bedrijfsmiddelen en persoonsgegevens effectief wordt uitgevoerd en zien erop toe dat regelmatig -voor zover nodig en voor zover mogelijk- loggingcontrole op het verwerken van persoonsgegevens wordt uitgevoerd;
- betrekken de CISO en PO vroegtijdig bij nieuwe of gewijzigde processen;
- voeren risicoanalyses en (pre-)DPIA's uit voor de processen waar zij verantwoordelijk voor zijn (of laten dit doen);
- rapporteren periodiek aan de directeur c.q. het MT over de door hen tactisch en operationeel uitgevoerde informatiebeveiligings- en privacybeschermende activiteiten en incidenten;
- zijn -in geval van een incident binnen hun afdeling- verantwoordelijk voor de implementatie van het incidentresponsplan en het coördineren van de eerste reactie.

3.2.3 CISO/PO: ondersteuning en advisering

De CISO is verantwoordelijk voor de coördinatie van informatiebeveiliging en de PO is verantwoordelijk voor de coördinatie van de privacybescherming.
De CISO en PO:

- ondersteunen het Dagelijks Bestuur c.q. de directeur en MT en afdelingshoofden bij het bewaken en verhogen van de betrouwbaarheid van de informatievoorziening en de bescherming van (persoons)gegevens;
- geven gevraagd en ongevraagd advies inzake informatiebeveiliging en privacy aan het Dagelijks Bestuur c.q. de directeur en MT.
- vertalen wet- en regelgeving en bedrijfsdoelstellingen naar een (integraal) Strategisch IB&P-beleid en aanvullende beleidsdocumenten;
- werken nauw samen met de afdelingshoofden in de uitvoering van het Strategisch IB&P-beleid en in het bijzonder de uitvoering van risicoanalyses en DPIA's;
- doen verbetervoorstellen op het gebied van privacy en informatiebeveiliging;
- verzorgen monitoring en rapportage conform het Strategische IB&P-beleid;
- dragen mee uit in het vergroten van de kennis en bewustwording over informatiebeveiliging en privacy bij medewerkers van BsGW;
- rapporteren via de directeur c.q. het MT aan het Dagelijks Bestuur hoe het lijnmanagement informatiebeveiliging en privacy implementeert en op welke wijze wordt voldaan aan dit beleid en de onderliggende wetgeving, zodat het Dagelijks Bestuur goed onderbouwde en gemotiveerde besluiten kan nemen over de behandeling van informatiebeveiliging- en privacyrisico's.

3.2.4 Controle en verantwoording: Auditing en Compliance

Er vindt periodieke rapportage plaats over de belangrijkste aspecten inzake informatiebeveiliging en de bescherming van (persoons)gegevens binnen BsGW. De controlefunctie heeft hier ook een bepaalde rol in. De controlefunctie wordt bekleed door onder andere de FG, de VIC-functionaris (Verbijzonderde Interne Controle), de concern controller en interne auditor.
De controlefunctie:

- is verantwoordelijk voor het uitvoeren van regelmatige interne audits en compliance beoordelingen om te controleren of het IB&P-beleid effectief wordt uitgevoerd;
- verifieert of risicobeheersmaatregelen en controles daadwerkelijk effectief zijn;
- ziet erop toe dat het IB&P-beleid in alle afdelingen en processen wordt nageleefd (compliance met beveiligings- en toegangscontrolemaatregelen, gegevensbeschermingsvereisten e.d.);

- rapporteert aan de directeur c.q. het MT over de bevindingen, inclusief aanbevelingen voor verbetering;
- initieert -in geval van ernstige incidenten of een nalevingsprobleem- een grondig onderzoek en stelt een verbeterplan op;
- draagt zorg voor een correcte documentatie van alle compliance- en controleactiviteiten.

4. Evaluatie

Dit beleid wordt jaarlijks geëvalueerd op basis van de geldende kaders. Het MT en Dagelijks Bestuur worden op de hoogte gebracht van de bevindingen. Indien nodig wordt voorgesteld om het beleid te herzien.

5. Intrekking

Het in 2020 vastgestelde 'Strategische baseline Informatiebeveiligingsbeleid, beter safe dan sorry' wordt ingetrokken.