Belastingsamenwerking
Oost-Brabant

BSOB

Beleid Informatiebeveiliging

Versie 2.0

Hedwy van de Werf
23-4-2019

Belastingsamenwerking Oost-Brabant

Versiebeheer

Versie	Datum	Auteur	Toelichting
2.0	23 april 2019	Hedwy van de Werf	Nieuwe versie ter vervanging van v1.8 uit 2015

© 2019 Copyright BSOB
Dit document is auteursrechtelijk beschermd en uitsluitend bestemd voor gebruik binnen de organisatie van Belastingsamenwerking Oost-Brabant te Oss.

Inhoudsopgave

1 Managementsamenvatting 3
1.1 Samenvatting 3
1.2 Leeswijzer 4
2 Beveiligingsbeleid 5
2.1 Doel van het beleid 5
2.1.1 Doelstellingen 5
2.1.2 Reikwijdte 6
2.1.3 Uitgangspunten 6
2.2 Risicoanalyse en continuïteit 6
2.2.1 Risicoanalyse 7
2.2.2 Classificatie informatiesystemen 7
2.2.3 Strategie voor continuïteit 7
2.3 Informatieclassificatie 7
2.4 Naleving van wet- en regelgeving 8
3 Organisatie van de informatieveiligheid 9
3.1 Verantwoordelijkheid 9
3.2 Evaluatie & Controle 10
3.3 Verantwoording 10
3.4 Sancties bij inbreuken op het informatiebeveiligingsbeleid 11
4 Beheersing van informatieveiligheid 12
Bijlage A Beschrijving functies 13
Chief Information Security Officer (CISO) 13
Privacy Officer (PO) 14
Functionaris voor de Gegevensbescherming (FG) 15
Bijlage B - Definities 17

1 Managementsamenvatting

1.1 Samenvatting

Voor u ligt het informatieveiligheidsbeleid van BSOB. Het beschrijft het te voeren beveiligingsbeleid binnen BSOB. Hieraan gerelateerd zijn de meer gedetailleerde procedures, maatregelen en richtlijnen die voor het uitvoeren van het beleid van toepassing zijn. Dit beleid beschrijft de richting en ondersteuning zoals deze door het dagelijks bestuur van BSOB is bepaald voor informatiebeveiliging in overeenstemming met de bedrijfsmatige eisen voor effectieve en efficiënte bedrijfsprocessen, betrouwbare financiële verslaggeving en naleving van wet- en regelgeving.

Geldigheidstermijn:
Dit beleid zal na vaststelling een geldigheidstermijn hebben van 4 jaren.

Het DB stelt daarom het volgende informatiebeveiligingsbeleid vast:

- Het informatiebeveiligingsnormenkader *Baseline Informatiebeveiliging Gemeente (BIG)* [1] wordt beschouwd als uitgangspunt voor het ontwikkelen van richtlijnen die specifiek op de organisatie zijn toegesneden. Op sommige punten kan - gemotiveerd - worden afgeweken van de voorgestelde maatregelen en/of zijn er wellicht aanvullende maatregelen nodig.
- Het uit te dragen informatiebeveiligingsbeleid is vastgelegd in dit document.
- De in het informatiebeveiligingsplan beschreven maatregelen geven het ambitieniveau van BSOB weer.
- Alle medewerkers van BSOB conformeren zich aan het Informatiebeveiligingsbeleid.
- Alle medewerkers zijn gehouden gegevens en informatiesystemen te beschermen tegen ongeautoriseerde toegang, gebruik, verandering, openbaring, vernietiging, verlies of overdracht.
- BSOB bevordert actief het beveiligingsbewustzijn van haar medewerkers. Daartoe worden alle onderdelen van dit beleid uitgewerkt in concrete richtlijnen en maatregelen, toegesneden op de taken en verantwoordelijkheden van de betrokken medewerkers.
- Periodiek wordt beoordeeld of voor specifieke gegevens of informatiesystemen aanvullende maatregelen noodzakelijk zijn. De frequentie van de beoordeling is gerelateerd aan de planning & control cyclus van BSOB. De naleving van genomen maatregelen wordt periodiek getoetst.
- Evaluatie / aanpassing van het beleid zal eens per drie jaar plaatsvinden of zoveel eerder als noodzakelijk.

In het Jaarplan Privacy & Informatiebeveiliging wordt het beleid vertaald in concrete maatregelen.

Aldus vastgesteld in de vergadering van het Dagelijks Bestuur van 17 juni 2019.

De voorzitter, De plaatsvervangend secretaris,

H.J. Mak G.J.M. van der Zanden

[1] Op 1 januari 2020 wordt de Baseline Informatiebeveiliging Overheid (BIO) het nieuwe normenkader voor alle overheden en vervangt de Baseline Informatiebeveiliging Gemeenten en Waterschappen (BIG en BIWA).

1.2 Leeswijzer

In Hoofdstuk 1 wordt het beveiligingsbeleid van BSOB beschreven in doelstellingen en uitgangspunten.
Hoofdstuk 2 beschrijft de verantwoordelijkheden en bevoegdheden van de verschillende functies en rollen voor beveiliging.
In Hoofdstuk 3 is de Beheersing van beveiliging opgezet.
Voor de leesbaarheid van dit document is ervoor gekozen om de wijze waarop de invulling van dit beleid plaatsvindt te verwerken in separate documenten.

Deze documenten zijn onderdeel van het ISMS (Information Security Management System).

2 Beveiligingsbeleid

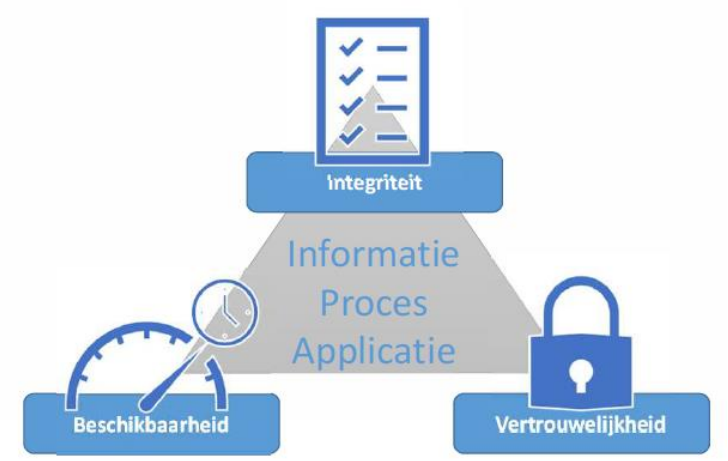
Alle medewerkers van BSOB zijn zich bewust van hun handelen (professionaliteit) ten aanzien van de informatiebeveiligingsaspecten en op welke wijze dit bijdraagt om als BSOB een betrouwbare taakuitvoerder te zijn die met vakmanschap en passie, continu kan anticiperen en inspelen op ontwikkelingen in het fysieke veiligheidsdomein.

Deze doelstelling heeft betrekking op de organisatie-, technische- en mensaspecten.

2.1 Doel van het beleid

Beschikken over juiste en betrouwbare informatie, maar ook het delen ervan met ketenpartners en belastingplichtigen, is essentieel voor het succes van BSOB. Hierbij is het belangrijk dat vanuit een strategisch oogpunt wordt bepaald, vastgelegd en gecommuniceerd hoe BSOB informatie ontvangt, gebruikt en uitwisselt.

Voor een effectieve beveiliging is het noodzakelijk dat gegevens, die aan de basis liggen van informatie, voldoen aan de gestelde eisen ten aanzien van *vertrouwelijkheid*, *integriteit* en *beschikbaarheid*. Effectieve beveiliging wordt ook bereikt door te werken met gepaste gedragsregels, in overeenstemming met de wetgeving, navolgen van het vastgesteld beleid en de gewenste richtlijnen uit de praktijk.



Dit beleid beschrijft het te voeren beveiligingsbeleid en geeft richting aan de meer gedetailleerde maatregelen en richtlijnen die van toepassing zijn binnen BSOB. Het beschrijft de fysieke- en informatiebeveiliging voor wat betreft de organisatorische aspecten en de uitvoering. Voor de leesbaarheid van dit document is ervoor gekozen om verdere invulling van dit beleid te verwerken in separate documenten en/of procesbeschrijvingen.

2.1.1 Doelstellingen

De doelstellingen van dit beleid zijn:

1. Het voldoen (compliant zijn) aan geldende wet- en regelgeving.
2. Het beschermen van alle fysieke en digitale informatiesystemen binnen BSOB (met inbegrip van, maar niet beperkt tot, alle computers, netwerkapparatuur, software en data) en het beperken van de risico's van diefstal, verlies, misbruik, of beschadiging van deze systemen.
3. De bewustwording creëren met betrekking tot de bekendheid en naleving van alle huidige en relevante interne procedures en richtlijnen, alsmede van wetgeving op het gebied van informatieveiligheid. Met het doel te zorgen dat alle gebruikers hun eigen verantwoordelijkheden begrijpen voor de bescherming van de vertrouwelijkheid en integriteit van de gegevens die zij behandelen.
4. Het zorgen voor een veilige en betrouwbare werking van de informatiesystemen voor het personeel en andere geautoriseerde gebruikers.
5. De borging ten aanzien van het beheer (exploitatie) van informatiesystemen om onbedoelde wijzigingen, met mogelijke nieuwe risico's, te voorkomen.

6. BSOB te beschermen tegen aansprakelijkheid of schade door het misbruik van haar informatiesystemen en faciliteiten.
7. Zorgen voor een systematiek van incidentenregistratie, analyse en selecteren van gepaste maatregelen om informatieveiligheid te vergroten.
8. Het bieden van kader voor een adequate continuïteitstrategie om onderbrekingen van activiteiten tegen te gaan en kritieke processen te beschermen tegen de gevolgen van omvangrijke storingen in informatiesystemen of rampen en om tijdig herstel te bewerkstelligen.

2.1.2 Reikwijdte

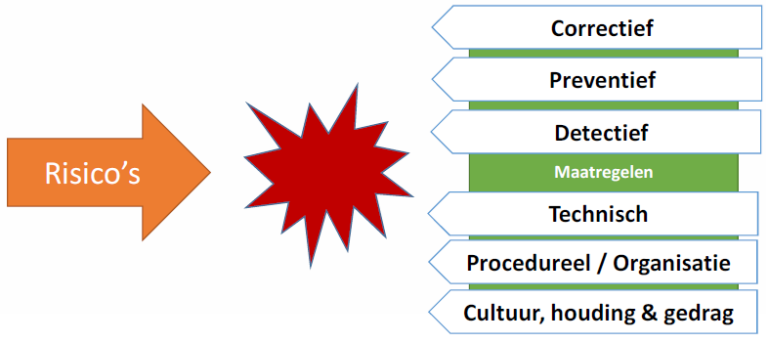
Het beleid heeft betrekking op alle door BSOB gebruikte gegevens en hieraan gerelateerde informatiesystemen, de fysieke aspecten met betrekking tot deze gegevens, privé-systemen welke zijn aangesloten op het netwerk van BSOB (bijvoorbeeld beveiligde thuiswerk-omgeving) én op software in eigendom van BSOB of via licentie verkregen.

2.1.3 Uitgangspunten

- De inhoud van dit beleid dient bekend te zijn bij alle geautoriseerde gebruikers van BSOB en de oplegging tot naleving ervan. Om dit te bereiken zal het onderwerp 'informatiebeveiliging' deel uitmaken van het inwerkprogramma van nieuwe medewerkers. Daarnaast wordt periodiek, maar minimaal één keer per vier maanden, het onderwerp op het (werk-)overleg geagendeerd en besproken.
- Informatiebeveiliging is een continu proces. Daarom is het nodig periodiek het vastgestelde beleid te herijken. Technologische en organisatorische ontwikkelingen binnen en buiten BSOB maken het noodzakelijk om periodiek te beoordelen of de organisatie op adequate wijze de (informatie-)beveiliging weet te waarborgen. Audits maken het mogelijk het beleid en de genomen maatregelen te controleren op effectiviteit.
- BSOB is eigenaar van de informatie die onder haar verantwoordelijkheid wordt geproduceerd, tenzij dit op basis van wettelijke gronden anders is overeengekomen.
- Elke medewerker van BSOB behoort de waarde van informatie te kennen en daarnaar te handelen. Deze waarde wordt bepaald door de schade als gevolg van verlies van beschikbaarheid, integriteit en vertrouwelijkheid. Het classificeren van gegevens kan hierbij behulpzaam zijn. Zie ook paragraaf 2.3.
- Bij veranderingen, zoals infrastructurele wijzigingen of de aanschaf van nieuwe systemen, wordt het onderwerp informatiebeveiliging zowel in de voorbereidingen als in de uitvoering meegenomen.
- Door BSOB wordt de BIG (en vanaf 2020 de BIO) als normenkader gehanteerd, waartegen toetsing van de uitvoering van het beleid en genomen maatregelen mogelijk is.

2.2 Risicoanalyse en continuïteit

Beveiligen gebeurt met een duidelijk beeld van de waarde van datgene wat beveiligd wordt. Dat betekent dat bewustzijn van die waarde en van de risico's van mogelijke schade, de grondslag is van dit beleid en daarmee sturend moet zijn in het nemen van maatregelen. Het is de taak van de verantwoordelijke bestuurder(s) en lijnmanagement om ervoor te zorgen dat dit bewustzijn aanwezig is.



2.2.1 Risicoanalyse

Om reproduceerbaar en eenduidig de waarde van informatie(-systemen) en gepaste beheersmaatregelen te kunnen bepalen wordt er gebruik gemaakt van een kwalitatieve risicoanalyse om onderbouwd de belangrijkste risico's te identificeren. De risicoanalyse wordt, in beginsel, elke drie jaar herhaald, of tussentijds in het geval van substantiële wijzigingen.

2.2.2 Classificatie informatiesystemen

Elk informatiesystemen heeft een eigenaar. De waarde van de informatiesystemen wordt vastgesteld door de eigenaar o.b.v. een uniforme methodiek voor classificatie van beveiligingsniveaus voor informatiesystemen, zie paragraaf 2.3. De waarde wordt bepaald door de schade die verlies van beschikbaarheid, integriteit en vertrouwelijkheid toebrengt aan de mogelijkheid tot het kunnen organiseren van de risicobeheersing.

2.2.3 Strategie voor continuïteit

Informatiebeveiliging heeft als doel om risico's met betrekking tot informatiebeveiligingsincidenten te reduceren tot een, door management vastgesteld, acceptabel niveau. Ondanks goede beheersmaatregelen kan een incident zich voordoen.

Voor kritieke ICT-diensten en informatiesystemen is een continuïteitsplan aanwezig. Hierin is opgenomen hoe, in geval van calamiteiten, de getroffen ICT-dienst of het getroffen informatiesysteem, binnen de door BSOB vastgestelde tijd, operationeel gemaakt kan worden. Een continuïteitsplan kan variëren van een goede back-upvoorziening of het geografisch spreiden van de ICT-dienst tot een complete uitwijk. Continuïteitsplannen worden minimaal **één** keer per jaar op actualiteit geëvalueerd.

2.3 Informatieclassificatie

Alle belangrijke informatie binnen BSOB wordt geclassificeerd naar één van de drie niveaus van beschikbaarheid, integriteit en vertrouwelijkheid, zoals hieronder vermeld.

Gegevens-classificatie	Kenmerken van informatie
Publiek	Deze informatie kent veelal lage eisen ten aanzien van de vertrouwelijkheid en beschikbaarheid en is daardoor voor **iedereen** binnen en buiten BSOB beschikbaar en toegankelijk.
Intern	Dit betreft de informatie die toegankelijk mag of moet zijn voor alle **medewerkers** van BSOB. De eisen ten aanzien van vertrouwelijkheid zijn beperkt maar aanwezig.
Vertrouwelijk	Dit betreft informatie die alleen toegankelijk mag zijn voor een **beperkte** groep gebruikers. Hieronder worden ook documenten of informatie verstaan die vanwege geldende wetgeving of opgelegde geheimhouding niet openbaargemaakt mogen worden. De informatie wordt beschikbaar gesteld op basis van het '*need to know*' [2] principe. Schending van deze classificatie kan direct of indirecte schade toebrengen aan BSOB, onderdelen van BSOB of personen binnen en buiten BSOB.

Voor informatie geclassificeerd als 'Intern' of 'Vertrouwelijk' dienen, additioneel aan het basis beveiligingsniveau, extra beschermende maatregelen te worden getroffen.

De proceseigenaar (vaak een afdelingshoofd) bepaalt welke maatregelen genomen moeten worden op basis van een risicoanalyse, waarbij de kans en het effect het risico bepalen.

[2] Need to know principe. Dit principe houdt in dat functionarissen slechts toegang hebben tot die informatie die zij nodig hebben voor het uitoefenen van hun functie.

2.4 Naleving van wet- en regelgeving

BSOB dient zich te houden aan alle relevante wet- en regelgeving die van toepassing zijn op het uitvoeren van de dagelijkse werkzaamheden. De relevante wet- en regelgeving is vertaald naar richtlijnen en gedragscodes die van toepassing zijn op alle medewerkers van BSOB en voor het overige van toepassing zijn op inhuurpersoneel, stagiaires van BSOB of derden (zoals leveranciers) die gebruik maken van informatievoorzieningen van BSOB.

In het bijzonder gelden in dit verband de volgende richtlijnen en codes:
- Gedragscode telefonie-, e-mail- en internetgebruik [3].
- Richtlijn telefonie en e-mail en Protocol Datalekken [4].
- Privacy beleid medewerkers BSOB van 29-5-2018.

Wettelijke voorschriften welke opgevolgd dienen te worden:
- Wet op computercriminaliteit.
- Algemene Verordening Gegevensbescherming (AVG).
- Eisen die Logius als beheerder van DigiD stelt.
- Archiefwet.
- Meldplicht datalekken.
- Algemene wet inzake rijksbelastingen (AWR, inzake de geheimhoudingsplicht).

Daarnaast gelden de afspraken die contractueel gelden met leveranciers waarmee BSOB afspraken heeft gemaakt.
Indien BSOB schade ondervindt door nalatigheid bij het gebruik of het opzettelijke misbruik van informatievoorzieningen (plichtsverzuim) zullen de vigerende wet- en regelgeving worden toegepast en op basis daarvan maatregelen worden genomen door of namens de directie van BSOB.

Informatiebeveiliging is meer dan alleen privacy en privacy is meer dan alleen informatiebeveiliging:



[3] Informatiebeveiliging BSOB Gebruikersinformatie van 29-12-2015.
[4] Intranet documenten van 24-9-2018.

3 Organisatie van de informatieveiligheid

Informatiebeveiliging dient als proces te worden ingericht. Het onderwerp moet tevens een duidelijk benoemd onderdeel zijn van alle processen van BSOB. Informatiebeveiliging is onderdeel van de planning- en control cyclus. Aansluitend hierbij worden jaarplannen opgesteld, belegd in de organisatie en uitgevoerd. De resultaten ervan worden geëvalueerd en vertaald naar nieuwe jaarplannen (Plan, Do, Check, Act).

3.1 Verantwoordelijkheid

Verschillende actoren binnen BSOB verrichten gezamenlijk de activiteiten binnen het beveiligingsproces. Elke actor heeft een bepaalde rol binnen het proces. Een goede verdeling van de taken, bevoegdheden en verantwoordelijkheden (TBV's) tussen de verschillende actoren is cruciaal voor een effectief en efficiënt procesverloop.

Voor beveiliging worden binnen BSOB de volgende actoren onderkend:

Actor	Verantwoordelijkheid / rol
Dagelijks Bestuur	Integraal verantwoordelijk
Directie	Strategische verantwoordelijkheid, kaderstelling en implementatie
Afdelingshoofden/ proceseigenaren	Tactische verantwoordelijkheid, sturing op informatieveiligheid eigen processen inclusief controle, risico-afweging en naleving
CISO	Stelt informatiebeleid op en coördineert de uitvoering ervan, beheerst risico's en rapporteert aan management en bestuur.
PO	Vormgeven en bewaken van het privacybeleid
FG	Borgt en houdt toezicht op het beleid in samenwerking met de CISO en de PO
Kwaliteitsadviseur	Bewakende en adviserende verantwoordelijkheid
Medewerkers (iedereen)	Operationele verantwoordelijkheid en uitvoering
Externe partijen	Onafhankelijk toetsen en beoordelen, Compliance

Het DB is verantwoordelijk voor het vaststellen van het beleid en de directie voor het vaststellen van de richtlijnen die ten grondslag liggen aan een adequaat systeem van informatiebeveiliging en voor het beoordelen van de efficiëntie en effectiviteit hiervan. Als verantwoordelijke voor het onderwerp informatiebeveiliging is een portefeuillehouder informatiebeveiliging aangewezen. Het DB legt jaarlijks verantwoording af over informatiebeveiliging aan het AB middels het jaarverslag.

Vanuit de rol van CISO (Chief Information Security Officer) is de functionaris verantwoordelijk voor beleidsvorming, controle en registratie, communicatie en voorlichting en stelt verbetervoorstellen op voor de informatiebeveiliging. Dit gebeurt in nauw overleg met de kwaliteitsadviseur. Voor meer informatie zie Bijlage A Beschrijving functies.

De kwaliteitsadviseur bewaakt de samenhang met het kwaliteitssysteem van BSOB. Belangrijke taken vanuit de kwaliteitsadviseur BSOB zijn informeren, borging van de integrale kwaliteit en doelmatigheid van BSOB activiteiten, naleving van wet- en regelgeving en het eigen beleid en het uitvoeren van audits om van daaruit te komen tot verbetervoorstellen.

De dagelijkse verantwoordelijkheid berust bij de lijnmanagers van BSOB die voortdurend toezien op naleving van de vastgestelde richtlijnen. Daarnaast wordt van hen verwacht om de risico's te beoordelen waarmee hun afdeling wordt geconfronteerd. Om meer draagvlak te creëren op medewerker niveau is het aan te bevelen om per afdeling of proces een ambassadeur aan te stellen, die samen met de lijnmanager zorgt voor continue aandacht voor IB op de werkvloer.

Elke medewerker (al dan niet in vaste dienst) van BSOB is gehouden mee te werken aan de informatiebeveiliging. Zij zijn op individueel niveau verantwoordelijk voor een effectieve informatiebeveiliging van de aan hen toevertrouwde gegevens. Ook wordt van alle medewerkers verwacht dat zij eventuele beveiligingsincidenten direct melden bij hun leidinggevende (of hiervan een melding maken bij de applicatiebeheer helpdesk).

Voor sommige (werk-)processen geldt dat deze (deels) worden uitgevoerd door externe partijen. Met de externe dienstverleners worden concrete en toetsbare afspraken gemaakt over de door hen te treffen beveiligingsmaatregelen. Deze afspraken worden vastgelegd in externe dienstverleningsovereenkomsten. In elke dienstverleningsovereenkomst worden de door de dienstverlener te treffen beveiligingsmaatregelen beschreven. BSOB controleert periodiek de correcte naleving van de gemaakte afspraken.

3.2 Evaluatie & Controle

Onder controle wordt verstaan zowel interne controle door de eigen organisatie als toetsing door een onafhankelijke derde. De toetsing richt zich zowel op het beveiligingsbeleid als op de maatregelen die uit dit beleid voortvloeien. Dit betekent dat de toetsing zich richt op de volgende drie punten:

1. Juiste naleving van het beleid en de interne werkafspraken;
2. Correcte werking van de beveiligingsorganisatie;
3. Toereikendheid van de vastgestelde beveiligingsmaatregelen gedurende een bepaalde periode.

Onder evaluatie wordt verstaan het nagaan of de kaders van de beveiliging inhoudelijk nog toereikend zijn. Hierbij worden twee niveaus onderscheiden: de evaluatie van het beleid en de evaluatie van het beheer.
De evaluatie van het beleid is een heroriëntatie op de beleidsuitgangspunten. Bij de evaluatie van het beheer wordt nagegaan of het vastgestelde beleid nog toereikend is.

De periodieke controle (opgenomen in het jaarplan) op beveiliging bestaat uit drie onderdelen:

1. Toetsing beveiligingsmaatregelen
   Om ervoor te zorgen dat geïmplementeerde beveiligingsmaatregelen worden nageleefd dient er periodiek worden gemeten, naast de dagelijkse controle door teamleiders. De interne auditors (eventueel kwaliteitsmedewerkers) zullen op basis van een nader vast te stellen werkprogramma (inclusief uitgewerkte kwaliteitseisen) een audit uitvoeren.

2. Functiescheiding bij audits
   Om ervoor te zorgen dat de beveiligingsorganisatie (actoren, rollen, TBV's) correct werkt, wordt dit opgenomen in de interne auditstructuur. Er moet hierbij rekening gehouden worden met noodzakelijke functiescheiding. De functionarissen die zelf deel uitmaken van de beveiligingsorganisatie mogen geen deel uitmaken van het auditteam. Dit om belangenverstrengeling te voorkomen.

3. Evaluatie van het beleid
   Driejaarlijks wordt het vastgestelde beleid (inclusief maatregelen) op de toereikendheid beoordeeld. Concreet betekent dit dat beoordeeld wordt of het beleid en de maatregelen zorgen voor een afdoende beveiliging van de processen en de informatiestromen van BSOB.

3.3 Verantwoording

Afdelingshoofden leggen verantwoording af over de wijze waarop zij informatiebeveiliging borgen. BSOB zet een ISMS-tool in om hen hierbij te ondersteunen. ISMS staat voor Information Security Management System en is het geheel van maatregelen en processen dat de informatiebeveiliging borgt, anders gezegd: het 'kwaliteitssysteem informatiebeveiliging'. In de ISMS-tool worden maatregelen en taken toegewezen aan functionarissen, die daar vervolgens het resultaat en bijbehorende bewijslast aan koppelen.
Vanuit de ISMS-tool kan gerapporteerd worden over de stand van de informatiebeveiliging binnen BSOB.

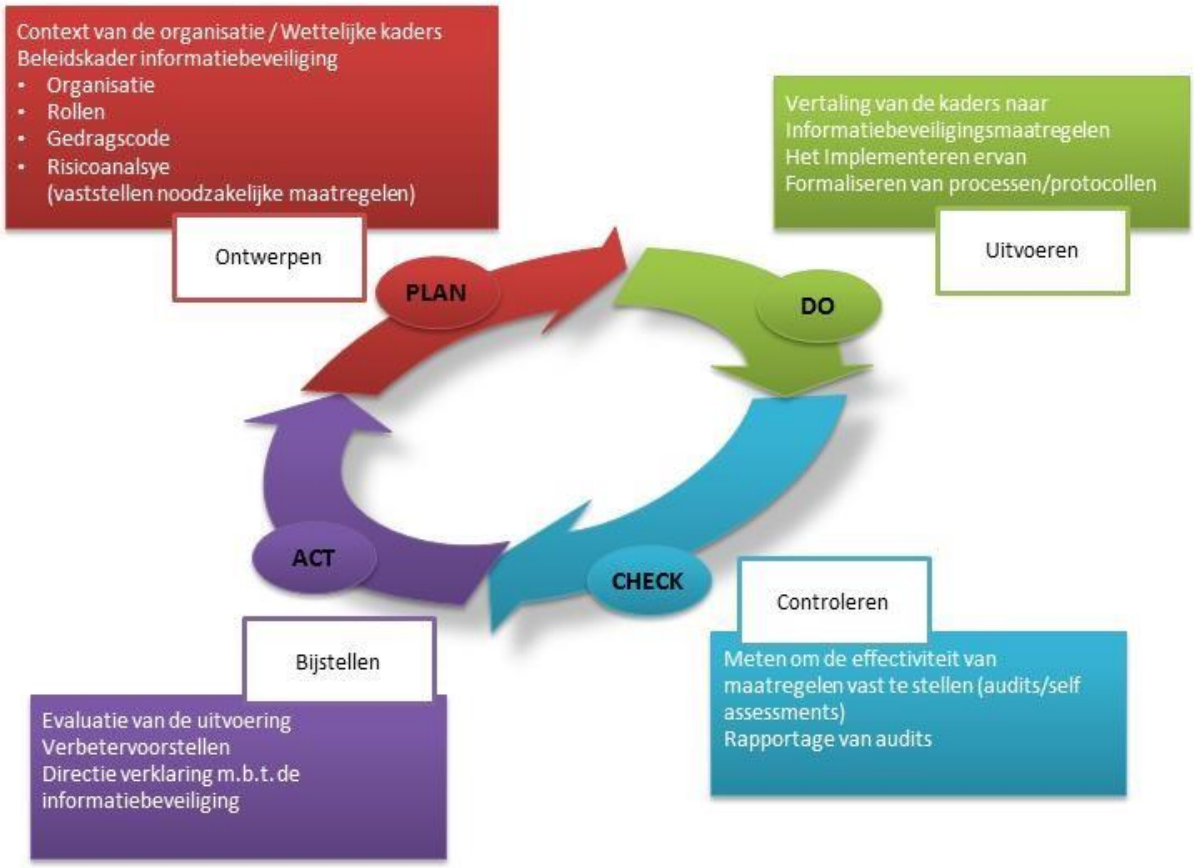
3.4 Sancties bij inbreuken op het informatiebeveiligingsbeleid

Het beleid is uitgewerkt in verschillende processen, procedures en richtlijnen die van toepassing zijn binnen BSOB. Bij inbreuk op het informatiebeveiligingsbeleid zullen door of namens de directie (passende) maatregelen worden getroffen.

Indien BSOB wordt aangesproken op de overtreding van eigendomsrechten, auteursrechten of overtreding van andere wettelijke bepalingen, zijn de wettelijke en binnen BSOB geldende regelingen van toepassing. In geval er door het onrechtmatig handelen schade ontstaat, wordt of kan de overtreder daarvoor aansprakelijk gesteld.

4 Beheersing van informatieveiligheid

De informatiebeveiliging van BSOB is een cyclisch proces. Via de zogenaamde Plan-Do-Check-Act cyclus wordt gestreefd naar een adequaat niveau van informatiebeveiliging. De tussentijdse controles of constateringen kunnen aanleiding zijn bij te sturen op de bestaande maatregelen.



De cyclus wordt jaarlijks minimaal één keer doorlopen. Het procesonderdeel toetsing wordt jaarlijks uitgevoerd wat betreft de toetsing van de opzet en het bestaan, en **twee**-jaarlijks wat betreft de toetsing van de werking (het bestaan gedurende een vastgestelde periode).

Bijlage A Beschrijving functies

Chief Information Security Officer (CISO)

Doel van de functie
Het op basis van de Baseline Informatiebeveiliging voor Nederlandse Gemeenten (BIG), zorgdragen voor een samenhangend pakket van maatregelen ter waarborging van de vertrouwelijkheid, integriteit en beschikbaarheid van de informatie binnen een gemeente.

Plaats in de organisatie
Het betreft een staffunctie. De CISO taken, bevoegdheden en verantwoordelijkheden zijn belegd bij de Informatiemanagement adviseur.

Resultaatgebieden (taken, werkzaamheden)
- Beleid en coördinatie
- Controle en registratie
- Communicatie en voorlichting
- Advies en rapportage

Verantwoordelijkheden en bevoegdheden
De belangrijkste bevoegdheid is om op elke plek binnen de organisatie gevraagd en ongevraagd onderzoek te kunnen (laten) doen en zo nodig zaken voor te schrijven.

Contacten
Zowel interne als externe contacten opnemen.

Opleiding, kennis en ervaring
- HBO/Academisch werk- en denkniveau
- Kennis en ervaring op het gebied van bestuurs-/bedrijfskunde en/of informatica
- Kennis van de actuele stand van zaken en mogelijkheden van ICT (besturingssystemen, netwerken, standaarden, ontwikkel- en beheermethoden)
- Kennis en ervaring op het gebied van informatiebeveiliging en risicoanalyse
- Kennis van de Baseline Informatiebeveiliging voor Nederlandse Gemeenten (BIG)
- Kennis van specialistische beveiligingstechnieken, zoals encryptie
- Kennis en ervaring op het gebied van adviseren en organisatiekunde
- Kennis van technische infrastructuur samen met de business inschatting van de kwetsbaarheid
- Kennis en ervaring met projectmatig werken en projectmanagement.

Competenties
- Goede communicatieve vaardigheden, zowel mondeling als schriftelijk
- Goed kunnen samenwerken met verschillende disciplines op verschillende niveaus
- Alert, initiatiefrijk, omgevingsbewust
- Integer
- Overtuigingskracht
- Bereid tot permanente scholing

Bron: https://www.informatiebeveiligingsdienst.nl/product/handreiking-ciso-functieprofiel/

Met ingang van 2020 wordt de BIG vervangen door de Baseline Informatiebeveiliging Overheid - de BIO. In de basis blijft de functiebeschrijving van de CISO gelijk, maar vraagt de BIO nadrukkelijker aandacht voor risico gestuurd denken en handelen.

Privacy Officer (PO)

Doel van de functie
De PO is verantwoordelijk voor het vormgeven en bewaken van het privacybeleid binnen BSOB.

Plaats in de organisatie
Het betreft een staffunctie. De PO taken, bevoegdheden en verantwoordelijkheden zijn belegd bij de Juridisch medewerker binnen afdeling Klant.

Resultaatgebieden (taken, werkzaamheden)
- De privacy awareness binnen BSOB waarborgen.
- Contactpunt binnen de organisatie voor privacyvraagstukken.
- Met FG en CISO verantwoordelijk voor het verder ontwikkelen, implementeren en het onderhouden van het privacy beleid en de hieraan gerelateerde activiteiten met betrekking tot de verwerking van persoonsgegevens.
- Risico's in kaart brengen en actief inspelen door aanbevelingen te doen en acties uit te zetten.
- Sturen op conformeren van werkinstructies en procesbeschrijvingen met privacywet- en regelgeving en intern beleid
- Afhandeling van mogelijke datalekken: beoordelen, managen en inschatten of er melding gemaakt moet worden bij AP.
- De oorzaak van het datalek identificeren en waar mogelijk in de toekomst weten te voorkomen.
- Opstellen en/of bewaken van verwerkersovereenkomsten.
- Bewaken/ aanvullen/ wijzigen verwerkingsregister per (werk) proces. Sturen op integreren privacy in werkprocessen en de procesbeschrijvingen.
- Uitvoeren van DPIA's (data protection impact assessment).
- Richtlijnen opstellen en waarborgen.
- Behandelen van verzoeken van betrokkene (privacyvraagstukken, inzageverzoeken etc).
- Rapporteren aan FG en vereiste documenten ter besluitvorming voorleggen.
- Op de hoogte blijven van ontwikkelingen in de wet, regelgeving en jurisprudentie rondom privacy.
- Stimuleert de bewustwording / basis deskundigheid over privacy in de organisatie en ziet toe op organisatie brede naleving (bewustwordingsacties).

Verantwoordelijkheden en bevoegdheden
De belangrijkste bevoegdheid is om op elke plek binnen de organisatie gevraagd en ongevraagd onderzoek te kunnen (laten) doen en zo nodig zaken voor te schrijven.

Contacten
Zowel interne als externe contacten opnemen.

Opleiding, kennis en ervaring
- HBO/Academisch werk- en denkniveau in een juridische, bedrijfskundige en/of bestuurlijke richting.
- Kennis van de laatste wet- en regelgeving op het gebied van privacy in het bijzonder de Algemene Verordening Gegevensbescherming.
- Kennis en ervaring op het gebied van informatiebeveiliging en risicoanalyse
- Kennis en ervaring op het gebied van adviseren en organisatiekunde
- Kennis en ervaring met projectmatig werken en projectmanagement.

Competenties
- Goede communicatieve vaardigheden, zowel mondeling als schriftelijk
- Goed kunnen samenwerken met verschillende disciplines op verschillende niveaus
- Juridische vraagstukken vertalen naar praktische voorschriften
- Brede kijk op de privacy binnen de organisatie
- Alert, initiatiefrijk, omgevingsbewust
- Integer
- Overtuigingskracht en organisatiesensitiviteit
- Bereid tot permanente scholing

Functionaris voor de Gegevensbescherming (FG)

Overheidsinstanties en publieke organisaties zijn op grond van de AVG verplicht om een FG aan te stellen. BSOB is op grond van de AVG verwerkingsverantwoordelijke voor de persoonsgegevens die door BSOB of door de strategische partners van BSOB worden verwerkt. De verwerkingen moeten in overeenstemming met de AVG zijn.

Doel van de functie
Het informeren en adviseren over de verplichtingen die BSOB heeft op grond van de AVG en het onafhankelijk toezicht houden op de organisatie over de juiste en zorgvuldige omgang met persoonsgegevens.

Plaats in de organisatie
De FG betreft een staffunctie. BSOB kan een medewerker benoemen tot FG, maar kan ook de functie beleggen bij een externe.

Verder is voor de positionering van de FG van belang dat:
- BSOB de FG tijdig betrekt bij alle aangelegenheden die verband houden met de bescherming van persoonsgegevens.
- de FG geen instructies ontvangt met betrekking tot de uitvoering van zijn FG-taken.
- de FG kan niet worden ontslagen of gesanctioneerd als gevolg van de uitoefening van zijn FG-taken.
- er mag geen belangenverstrengeling zijn tussen de FG-taken en de eventuele andere taken of functies van de FG.
- BSOB zorg draagt voor mogelijkheden dat betrokkenen direct contact kunnen opnemen met de FG (zoals via fg@bs-ob.nl) over alle aangelegenheden die verband houden met de verwerking van hun gegevens en met de uitoefening van hun rechten uit hoofde van de AVG.

Resultaatgebieden (taken, werkzaamheden)
- Het steekproefsgewijs controleren van het register gegevensverwerkingen.
- Het controleren en bewaken van de verwerkersovereenkomsten.
- Het monitoren en handhaven van de verwerking van persoonsgegevens conform de AVG.
- Het toezien op naleving van de AVG en andere EU wet- en regelgeving en nationale bepalingen omtrent gegevensbescherming.
- Het beheren van de stand van zaken en hierover rapporteren aan het Bestuur.
- Het samenwerken met de Autoriteit Persoonsgegevens en optreden als contactpersoon.
- Het fungeren als aanspreekpunt voor de PO, om advies uit te brengen over beleid en stukken, zoals opgesteld door de PO.
- Het fungeren als aanspreekpunt voor de betrokkenen wanneer zij gebruik maken van de mogelijkheid om contact op te nemen met de FG over de verwerking van hun persoonsgegevens.
- Het beoordelen van mogelijke data incidenten en het melden van gedetecteerde data incidenten.
- Het uitbrengen van advies aan de organisatie omtrent de afhandeling daarvan.
- Het adviseren over de wijze waarop de verwerking van persoonsgegevens in overeenstemming met de AVG plaatsvindt of ingericht kan worden, bijvoorbeeld in het geval van projecten of nieuwe vormen van gegevensverwerking.
- Steekproefsgewijze toetsing op relevante onderdelen van de organisatie en/of techniek ten behoeve van de uitvoering van de AVG in de organisatie.
- Het uitbrengen van advies wanneer betrokkenen hun rechten uitoefenen, zoals omschreven in Hoofdstuk III AVG.
- Stimuleert de bewustwording en deskundigheid van medewerkers over privacy in de organisatie.
- Blijft op de hoogte van ontwikkelingen en de wet, regelgeving en jurisprudentie rondom privacy.

Verantwoordelijkheden en bevoegdheden
De FG is verantwoordelijk voor het houden van onafhankelijk toezicht op, en adviseren van de organisatie over de juiste en zorgvuldige omgang met persoonsgegevens. Daarnaast loopt de formele communicatielijn van BSOB naar de Autoriteit Persoonsgegevens met betrekking tot

vragen en klachten over de verwerking van persoonsgegevens via de FG. Dit is tevens de escalatielijn voor de FG als deze een escalatie nodig acht.

De FG is bevoegd om op elke plek binnen de organisatie gevraagd en ongevraagd onderzoek te kunnen (laten) doen en gevraagd en ongevraagd advies uit te brengen over de juiste omgang met persoonsgegevens. De FG is niet bevoegd om besluiten te nemen namens BSOB. Hoewel de FG geen bindende adviezen kan geven, zijn deze adviezen wel zwaarwegend voor BSOB. De FG kan escaleren naar de Autoriteit Persoonsgegevens, die wel bindende adviezen kan geven en die rechtsmiddelen bezit om maatregelen af te dwingen.

De FG is niet persoonlijk aansprakelijk als er binnen de organisatie of bij verwerkers een overtreding van de AVG is. De naleving van de privacywet is een verantwoordelijkheid van de verwerkingsverantwoordelijke of de verwerker.

Contacten
Zowel interne als externe contacten opnemen.

Opleiding, kennis en ervaring
- HBO/Academisch werk- en denkniveau in een juridische, bedrijfskundige en/of bestuurlijke richting.
- Kennis van de laatste wet- en regelgeving op het gebied van privacy in het bijzonder de Algemene Verordening Gegevensbescherming.
- Kennis en ervaring op het gebied van informatiebeveiliging en risicoanalyse
- Kennis en ervaring op het gebied van adviseren en organisatiekunde.
- Kennis en ervaring met projectmatig werken en projectmanagement.

Competenties
- Politiek en bestuurlijk sensitief.
- Communicatief sterk en diplomatiek, waarbij de FG weerstand tegen cultuurverandering kan verminderen.
- Inhoudelijk expert op het gebied van de AVG en andere wetgeving over gebruik van informatie en data door de overheid, maar ook op het gebied van bijvoorbeeld informatietechnologie.

Bijlage B - Definities

In deze bijlage worden enkele definities nader toegelicht.

Algemene Verordening Gegevensbescherming (AVG)
De AVG is de Europese privacy verordening die per 25 mei 2018 van toepassing is. De AVG vervangt de huidige privacy wetten van de verschillende EU-lidstaten.

Beveiliging
Het brede begrip van informatiebeveiliging, d.w.z. inclusief fysieke beveiliging, continuïteitbeheer, ofwel beschikbaarheid van bedrijfsprocessen en persoonlijke veiligheid en integriteit.

Beveiligings-incident
Het manifest worden van een beveiligingsrisico (dreiging, oorzaak) als gevolg van een overtreding van beveiligingsregel, bijv. onbevoegde toegang tot ICT-voorzieningen.

Chief Information Security Officer (CISO)
De CISO is verantwoordelijk voor het implementeren van, en toezicht houden op het informatie-beveiligingsbeleid binnen BSOB. De CISO heeft een centrale rol in het beheren van alle processen die daarmee te maken hebben en moet daarbij voldoen aan de BIG/BIO.

Continuïteitsplan
Een plan om bij (ernstige) verstoringen de informatievoorziening gericht op het primaire proces, binnen de door BSOB aangegeven tijd, weer beschikbaar te hebben.

Compliant
Compliance betekent dat de organisatie moet (en wil) voldoen aan de wet- en regelgeving. Het niet voldoen aan compliancy-eisen brengt risico's met zich mee zoals:

- imagoschade die kan worden opgelopen;
- financiële schade in de vorm van boetes of claims.

Functionaris Gegevensbescherming (FG)
De FG is de functionaris die binnen BSOB verantwoordelijk is voor naleving van de regelgeving die voortvloeit uit de AVG.

Fysieke en digitale informatiesystemen
Informatiesystemen met het doel vanuit gegevensbronnen voor een gebruiker relevantie informatie te generen. Dit kan een digitaal systeem (bijvoorbeeld: een applicatie) zijn of een fysiek systeem (bijvoorbeeld: het HRM-dossier in een kast)

Incidentenregistratie
Een systeem, bij voorkeur digitaal, waar meldingen over de informatiebeveiliging in worden geregistreerd zodat de organisatie adequaat kan reageren en de opvolging kan worden gemonitord.

ISMS
Het Information Security Management System. Door het inrichten van een ISMS behoud de organisatie grip op het onderwerp Informatiebeveiliging.

Privacy Officer (PO)
De PO is verantwoordelijk voor het verder ontwikkelen, implementeren en het onderhouden van het privacy beleid en de hieraan gerelateerde activiteiten met betrekking tot de verwerking van persoonsgegevens. Daarnaast kan de PO ondersteunen bij het in kaart brengen van de risico's en heeft een adviserende rol naar de verschillende afdelingen en medewerkers.