BLAD GEMEENSCHAPPELIJKE REGELING

Nr. 1172

2 november 2022

Officiële uitgave van de gemeenschappelijke regeling BAR-organisatie

Informatiebeveiligingsbeleid BAR-organisatie

Colofon

Naam document
Informatiebeveiligingsbeleid BAR-organisatie

Nummer zaaksysteem
536423

Doel
Dit Informatiebeveiligingsbeleid geeft richting aan de manier waarop binnen de BAR-organisatie in opdracht van de gemeenten Barendrecht, Albrandswaard en Ridderkerk wordt gezorgd voor een adequate informatiebeveiliging en de borging daarvan. Dit beleid bevat daarom uitgangspunten, de organisatie en verantwoordelijkheden ten aanzien van informatiebeveiliging.

Bereik
Dit Informatiebeveiligingsbeleid is van toepassing op de BAR-organisatie en alle uit te voeren processen, organisatieonderdelen, objecten, informatiesystemen en gegevens(verzamelingen), inclusief gegevensverwerking door de BAR-organisatie, zowel voor de interne organisatie als voor de gemeenten Barendrecht, Albrandswaard en Ridderkerk. Het is ook van toepassing op de gegevensverwerking die bij leveranciers c.q. in de Cloud zijn of worden ondergebracht.

Dit beleid richt zich op de kaders voor informatiebeveiliging. Voor de nadere invulling daarvan worden aanvullende beleidsstukken opgesteld (zie ook relatie met andere producten).

Dit beleid zal in een per gemeente aangepaste versie ter besluitvorming worden voorgelegd aan de gemeenten Barendrecht, Albrandswaard en Ridderkerk.

Doelgroep
Dit beleid is gericht op degenen die direct betrokken zijn bij het vaststellen en uitvoeren van het informatiebeveiligingsbeleid, zoals: Bestuur en management van de BAR-organisatie en de gemeenten en functionarissen rond informatiebeveiliging en privacy.

Dit document geeft inzicht aan inwoners en anderen hoe er bij de BAR-organisatie met informatiebeveiliging wordt omgegaan.

Dit Informatiebeveiligingsbeleid is openbaar en is beschikbaar voor proceseigenaren (lijnmanagement), applicatiebeheerders, externe partijen, ketenpartners, medewerkers en andere belanghebbende(n).

Versie
v0.7, 10 juni 2022

Versiebeheer
Het beheer van dit document berust bij de Chief Information Security Officer.

Relatie met andere producten
Dit Informatiebeveiligingsbeleid heeft een relatie met:

- De resolutie informatieveiligheid VNG;
- Eenduidige Normatiek Single Information Audit (ENSIA);
- De volgende maatregelen uit de Baseline Informatiebeveiliging Overheid;
  - Control: 5.1.1;
  - Control: 5.1.2;
  - Control: 6.1.1;
  - Overheidsmaatregel: 5.1.1.1;
  - Overheidsmaatregel: 5.1.2.1;
  - Overheidsmaatregel: 6.1.1.1.
- De Algemene verordening gegevensbescherming (Avg), die passende beveiligingsmaatregelen voor persoonsgegevens vereist (Art 5 lid 1 onder f en Art 32 lid 1) en ook aantoonbaarheid, evaluatie en aanpassing van de maatregelen (Art 24 lid 1);

– De Wet Politiegegevens, die passende beveiligingsmaatregelen vereist (Art 4a lid 2), die nader zijn uitgewerkt in:
  - o het Besluit Politiegegevens dat onder andere de evaluatie en actualisering van beveiligingsmaatregelen vereist; (art 6:1a)
  - o het Besluit Politiegegevens Boa's met nadere bepalingen, onder andere omtrent autorisaties. (Art 3 lid 2)

– Mandaatregelingen voor verlening van mandaat en volmacht aan functionarissen van de BAR-organisatie.
– Het privacybeleid.

Dit Informatiebeveiligingsbeleid heeft verder relatie met beleidsdocumenten en procedures, waarin dit beleid nader is uitgewerkt. De Chief Information Security Officer (CISO) houdt een overzicht bij van deze beleidsdocumenten, zoals bijvoorbeeld:

1. Beleid personele beveiliging
2. Gedragsregels/Handreiking "Veilig omgaan met informatie"
3. Fysiek toegangsbeleid
4. Beleid Logisch Toegangsbeleid
5. Beleid mobiele apparatuur en telewerken
6. Loggingbeleid
7. Cryptografiebeleid
8. Bedrijfscontinuïteitsplan
9. Procesbeschrijvingen, zoals die voor incident- en wijzigingsbeheer, datalekken etc.

Tenslotte heeft dit informatiebeveiligingsbeleid een relatie met het Privacybeleid.

Vaststelling en inwerkingtreding
Dit Informatiebeveiligingsbeleid wordt vastgesteld door het Algemeen Bestuur van de BAR-Organisatie en wordt na vaststelling uitgevoerd. Het Informatiebeveiligingsbeleid is vastgesteld door:

Het Algemeen Bestuur van de BAR-organisatie op 18 oktober 2022

1: INLEIDING

De BAR-organisatie werkt met gevoelige gegevens van inwoners en medewerkers. Daarnaast verwerkt zij ook met andere gegevens waarvan de beveiliging belangrijk is voor de rechtmatige uitvoering van gemeentelijke taken. Te denken valt aan het BSN, gegevens in de BRP, gezondheidsgegevens bij Wmo en Jeugdwet, concurrentiegevoelige gegevens bij aanbestedingen en de financiële en betaaladministratie.

Onder informatiebeveiliging van de BAR-organisatie verstaan we de passende bescherming van vertrouwelijkheid, integriteit en beschikbaarheid ("BIV") van informatie die door of onder verantwoordelijkheid van de BAR-organisatie wordt verwerkt:

- Vertrouwelijkheid: Dit gaat over de gevoeligheid van gegevens en de schade wanneer deze "op straat" komen te liggen of in handen van onbevoegden. Een hoge vertrouwelijkheid is bijvoorbeeld nodig voor gezondheidsgegevens in Wmo- en Jeugdwetaanvragen.
- Integriteit: Dit gaat over de juistheid, actualiteit en authenticiteit van gegevens en de schade wanneer gegevens onbevoegd worden gewijzigd. Een hoge integriteit is bijvoorbeeld nodig bij betalingsgegevens met een frauderisico.
- Beschikbaarheid: Dit gaat over de beschikbaarheid van informatie voor de bedrijfsprocessen en de schade die ontstaat wanneer een bedrijfsproces tijdelijk niet uitgevoerd kan worden. Een hoge beschikbaarheid is bijvoorbeeld nodig bij de basisregistraties.

Onder het verwerken van informatie wordt ook het verzamelen, bewaren, raadplegen, gebruiken, verstrekken en vernietigen van informatie verstaan.

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

RELATIE TUSSEN INFORMATIEBEVEILIGING EN PRIVACY

Er is nauwe samenhang tussen informatiebeveiliging en privacy. De burger heeft recht op eerbiediging en bescherming van zijn persoonlijke levenssfeer en een zorgvuldige omgang met zijn persoonsgegevens. Dit vraagt een adequate beveiliging van deze persoonsgegevens en het respecteren van de geldende

privacywetgeving. Het beschermen van persoonsgegevens is het gemeenschappelijke domein waar informatiebeveiliging en privacy samenkomen.

Dit informatiebeveiligingsbeleid beschrijft hoe alle informatie van de organisatie wordt be-schermd, waaronder persoonsgegevens. Het borgen van de privacyaspecten van per-soonsgegevens is gevat in een afzonderlijk privacybeleid.

In de praktijk is er een nauwe samenwerking tussen informatiebeveiliging en privacy, bij-voorbeeld bij bewustwording en training van medewerkers en bij het adviseren over en beoordelen van nieuwe applicaties.

2: ROLLEN EN VERANTWOORDELIJKHEDEN

BAR-ORGANISATIE [1]

Het dagelijks bestuur is bestuurlijk eindverantwoordelijke voor de Informatieveiligheid & Privacy (I&P) die door de BAR-organisatie wordt uitgevoerd voor de gemeenten. Met andere woorden zij bewaakt of gemeentelijke informatiebeveiligingsdoelstellingen worden/zijn gerealiseerd door de BAR-organisatie. In die hoedanigheid stelt zij beleid vast, waarin wordt aangegeven hoe zij met die verantwoordelijkheid wil omgegaan.
De directieraad van de BAR-organisatie is ambtelijk eindverantwoordelijk voor de uitvoering van het informatiebeveiligingsbeleid. De directie geeft invulling aan die verantwoordelijkheid door het omzetten

1) NB t.a.v. de rol van College van burgemeesters en wethouders bij vertaling van het beleid naar de gemeenten:Het college van burgemeester en wethouders van elk van de deelnemende gemeenten is eindverantwoordelijk voor informatiebeveiliging binnen de gemeentelijke organisatie en legt daarover extern verantwoording af. Het college geeft richting aan het informatiebeveiligingsbeleid, bepaalt op hoofdlijnen welke informatiebeveiligingsrisico's acceptabel zijn en welke informatiebeveiligingsrisico's ze wil afdekken. De uitvoering van het informatie-beveiligingsbeleid is belegd bij het bestuur van de BAR-organisatie, conform de convenanten die de deelnemende gemeenten met de BAR-organisatie hebben afgesloten (zie privacybeleid bijlage 2). Daartoe is een mandaatbesluitregeling van toepassing (zie privacybeleid bijlage 3). Het college houdt toezicht op de uitvoering. Daarnaast legt het college van burgemeester en wethouders verantwoording af over de status van de informatiebeveiliging binnen de gemeente aan de landelijke toezichthouders en de gemeenteraad. Deze verantwoording bestaat in ieder geval uit een jaarlijkse zelfevaluatie (ENSIA), de IT-audit in het kader van ENSIA, een verklaring van het college van burgemeester en wethouders (collegeverklaring) en een passage over informatiebeveiliging in het jaarverslag.

van het beleid in doelstellingen en plannen, de integratie daarvan in de processen van de organisatie, toewijzing van rollen en verantwoordelijkheden, het ter beschikking stellen van middelen, het bekendmaken van het beleid en het belang daarvan, het aansturen en ondersteunen van medewerkers bij en het toezien op uitvoering van het beleid, evaluatie en bijstelling van de aanpak van informatiebeveiliging en beheersingsmaatregelen.

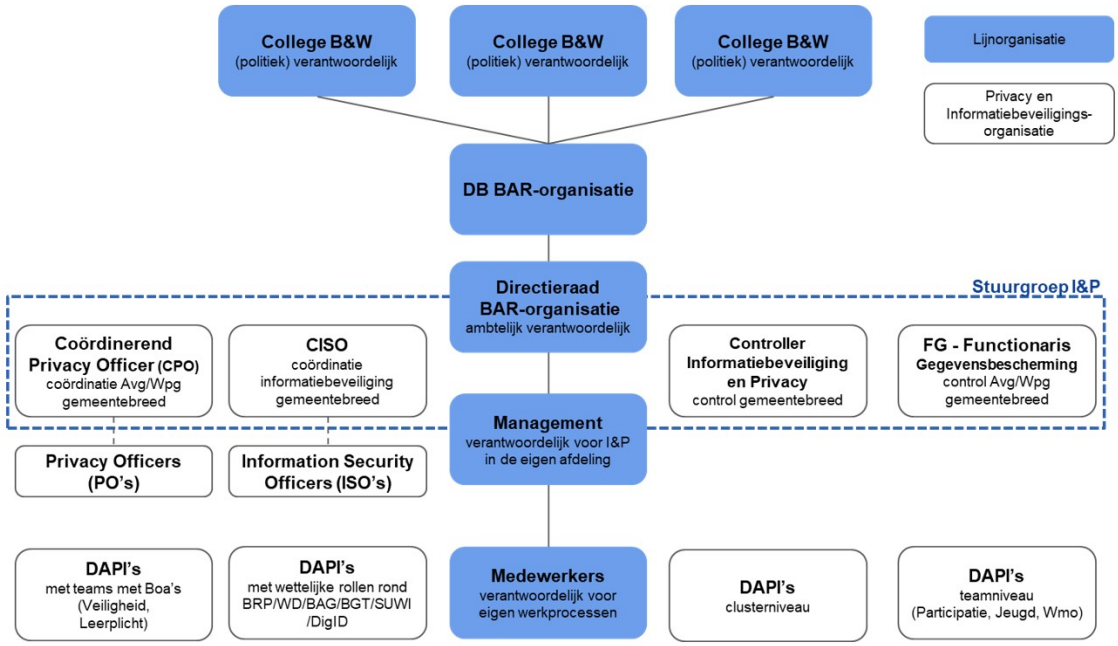
Daarbij wordt de directie ondersteund door de organisatie, namelijk door:

- alle **medewerkers** die elk verantwoordelijk zijn voor het uitvoeren van het informatiebeveiligingsbeleid als onderdeel van hun professionele verantwoordelijkheid. Om hen daarbij te ondersteunen is er een beleidsdocument "Veilig omgaan met informatie en bedrijfsmiddelen", waarin gedragsregels staan voor medewerkers, en worden medewerkers bewust gemaakt van hun rol/bijdrage en geïnformeerd over hoe zij deze kunnen uitvoeren/leveren, zowel bij indiensttreding als op basis van regelmatige bewustwordings- en leerinterventies. Daarvoor wordt jaarlijks een programma opgesteld door de Coördinerend Privacy Officer en de CISO;
- **leidinggevenden**/proceseigenaren die
    - verantwoordelijk zijn voor de uitvoering van het informatiebeveiligingsbeleid en beheersmaatregelen binnen hun afdeling. Informatiesystemen die door meerdere organisatieonderdelen worden gebruikt vallen onder de verantwoordelijkheid van de door de directie aangewezen systeemeigenaar;
    - zorgen voor adequate inrichting van werkprocessen en aansturing van medewerkers (1e verdedigingslinie);
    - toezien op de naleving van het beleid en bevorderen van beveiligingsbewustzijn;
    - onderdelen van beheersmaatregelen uitvoeren, zoals (het bevestigen van) de dataclassificatie voor processen en applicaties van de afdeling, het beoordelen van toegangsrechten, etc.;
    - relevante wettelijke, statutaire, regelgevende en contractuele eisen voor hun informatiesystemen vaststellen, documenteren en actueel houden;
    - processpecifieke borgings-/controleactiviteiten uitvoeren, vaak samenhangend met processpecifieke applicaties;
    - processpecifieke beheersmaatregelen uitvoeren, bijvoorbeeld voortvloeiend uit wetgeving, zoals over basisregistraties, waardedocumenten (zoals reisdocumenten/rijbewijzen), DigiD en SUWI;
    - verantwoordelijk zijn voor het nemen van maatregelen om beveiligingsincidenten binnen hun afdeling te voorkomen.
- **Decentrale Aanspreekpunten voor Privacy en Informatiebeveiliging (DAPI)** benoemen, die de leidinggevende ondersteunen bij het uitvoeren van de bovengenoemde taken (op welk niveau van de organisatie de benoeming van een DAPI wenselijk is hangt af van de omvang van de afdeling en de hoeveelheid gevoelige gegevens die daarin wordt verwerkt). Onder deze taken vallen het signaleren van beveiligings-/privacyissues binnen de afdeling, aanleveren van rapportageinformatie aan CISO en Coördinerend Privacy Officer (CPO), informatieverzameling voor DPIA's, het aanleveren van informatie voor het register van verwerkingen en verzoeken van betrokkenen, bevorderen van het bewustzijn binnen de afdeling. De DAPI zijn aanspreekpunt bij audits, zoals ENSIA. De leidinggevende behoudt de eindverantwoordelijkheid.
- de **Chief Information Security Officer (CISO)**, die
    - het opstellen, de uitvoering, evaluatie en bijstelling van het beleid en de jaarlijkse verbetercycli coördineert;
    - de implementatie, uitvoering en borging van beheersmaatregelen coördineert;
    - rapporteert daarover en over beveiligingsincidenten aan de Stuurgroep I&P en is bevoegd rechtstreeks te verslag te doen aan de gemeentesecretaris en het bestuur;
    - de Stuurgroep I&P en management gevraagd en ongevraagd adviseert over informatiebeveiliging in brede zin;
    - beveiligingsincidenten registreert in een incidentenregister en de afhandeling en evaluatie hiervan coördineert;
    - beveiligingsbewustzijn bevordert in de gehele organisatie;
    - coördineert de activiteiten van ISO's en DAPI's, ook inhoudelijk.
- **de Information Security Officer(s) (ISO's)** , die:
    - op operationeel niveau gevraagd en ongevraagd adviseert en ondersteunt bij de uitvoering van het informatiebeveiligingsbeleid en jaarplan en de implementatie en uitvoering van

beheersmaatregelen, zoals het beoordelen van kwetsbaarheden, de afhandeling en evaluatie van datalekken, het bevorderen van veiligheidsbewustzijn;
  - optreedt als coördinator ENSIA.

- de **Functionaris Gegevensbescherming** (FG), die toezicht houdt, kaders aangeeft, informeert en adviseert vanuit zijn/haar wettelijke taak conform de Avg en de Wpg en daarover rapporteert aan de Stuurgroep I&P en bevoegd is rechtstreeks verslag te doen aan de gemeentesecretaris en het dagelijks bestuur van de BAR-organisatie;
- de **Coördinerend Privacy Officer (CPO)**, die
  - het opstellen, de uitvoering, evaluatie en bijstelling van het beleid en de jaarlijkse verbetercycli coördineert;
  - de implementatie, uitvoering en borging van beheersmaatregelen coördineert;
  - De Stuurgroep I&P en management gevraagd en ongevraagd adviseert over privacy/gegevensbescherming in brede zin;
  - De afhandeling en evaluatie van datalekken, verzoeken van betrokkenen en van de Autoriteit Persoonsgegevens coördineert;
  - daarover en over datalekken rapporteert aan de Stuurgroep I&P;
  - privacybewustzijn bevordert in de gehele organisatie;
  - de activiteiten van PO's en DAPI's, ook inhoudelijk coördineert.
- de stafafdeling **Concerncontrol**, die:
  - interne audits coördineert, bijvoorbeeld: de Verbijzonderde Interne Controles (VIC) en het onderzoeksplan doelmatigheid en doeltreffendheid op basis van art. 213a van de Gemeentewet en interne audits op basis van art. 33 van de Wet Politiegegevens;
  - externe audits coördineert, bijvoorbeeld de IT-audit in het kader van de controle van de jaarrekening en de externe audit op basis van art. 33 van de Wet Politiegegevens.
- **andere medewerkers** die verantwoordelijk zijn voor specifieke onderdelen van het beleid, zoals het uitvoeren van specifieke beveiligingsmaatregelen en de bewaking daarvan. Deze specifieke taken en verantwoordelijkheden worden benoemd in de beschrijving van de beheersmaatregelen van de BIO.

Een en ander is hieronder schematisch weergegeven:



Besturing door de Stuurgroep Informatieveiligheid en privacy (I&P)
De Stuurgroep Informatieveiligheid en privacy (I&P) geeft namens de directie sturing aan de uitvoering van het informatiebeveiligingsbeleid en heeft daarnaast een beleidsvoorbereidende rol. De Stuurgroep I&P bestaat uit:

– Algemeen Directeur BAR-Organisatie
– Manager Concern control (CCC)
– Directeur met portefeuille Juridische Zaken en Inkoop (JZI) / Informatie en Automatisering (IFA) / Dienstverlening (DVL)
– Manager Juridische Zaken en Inkoop (JZI)
– Manager Cluster Maatschappij
– Manager Informatie en automatisering (IFA)
– Functionaris Gegevensbescherming (FG)
– Coördinerend Privacy Officer (CPO)
– Chief Information Security Officer (CISO)

De voorzitter van de Stuurgroep I&P, tevens lid van de directieraad, gehoord de leden van de Stuurgroep[2]:

– wijst de verantwoordelijkheden voor beheersmaatregelen toe aan functies binnen de organisatie;
– besluit over uitwerkingen van het informatiebeveiligingsbeleid in technische beleidsstukken, zoals toegangsbeleid, cryptografiebeleid, patchbeleid, etc.
– adviseert de directieraad over besluiten met betrekking tot de implementatie van beheersmaatregelen en acceptatie van (rest-)risico's.

De CISO rapporteert functioneel in de Stuurgroep I&P aan de directieraad.
De CISO wordt ondersteund door:

– Information Security Officer(s) (ISO's);
– verantwoordelijken voor beheersmaatregelen die door de Stuurgroep I&P aan hen zijn toegewezen;
– leidinggevenden en hun Decentrale aanspreekpunten Privacy en Informatiebeveiliging (DAPI) voor de implementatie en borging binnen de afdelingen.

Taken en verantwoordelijkheden zijn hier op hoofdlijnen beschreven en worden nader uitgewerkt in de documentatie van beheersmaatregelen, procedures etc.

3: UITGANGSPUNTEN EN KADERS

ORGANISATIEKADERS

Beleidsdocumenten en procedures

Dit Informatiebeveiligingsbeleid heeft een relatie met beleidsdocumenten en procedures, waarin dit beleid nader is uitgewerkt. De CISO houdt een overzicht bij van deze beleidsdocumenten, zoals bijvoorbeeld:

1. Gedragsregels/Handreiking "Veilig omgaan met informatie".
2. Beleid Logische Toegangsbeveiliging.
3. Cryptografiebeleid.

UITGANGSPUNTEN

Voor informatiebeveiliging gaat het Dagelijks Bestuur van de BAR-organisatie uit van de volgende uitgangspunten.

Naleving

Het Dagelijks Bestuur van de BAR-organisatie, de directieraad, de Chief Information Security Officer en de proceseigenaren (lijnmanagers) bevorderen de naleving van dit informatiebeveiligingsbeleid, de algehele communicatie en bewustwording (awareness) rondom informatieveiligheid.

Drie verdedigingslinies / Three lines of defense

Bij de toepassing van informatiebeveiliging staat het faciliteren van de werkprocessen van de organisatie voorop. Informatiebeveiliging dient hieraan een bijdrage te leveren door het veilig werken met informatie te faciliteren. Dat betekent dat Maatregelen zijn in balans met de te beschermen waarde of het belang zijn. Er moeten 'doelmatige, zakelijke' argumenten zijn om beveiligingsmaatregelen te treffen. Als er geen doelmatige argumenten zijn, worden er geen nieuwe maatregelen getroffen. Deze balans

2) Conform mandaatbesluit

wordt gevonden op basis van een expliciete risicoafweging, d.w.z. de te nemen maatregelen voor informatieveiligheid zijn risico gedreven.

De organisatie wil aantoonbaar voldoen aan wet- en regelgeving. Het gaat daarbij met name om de Algemene verordening gegevensbescherming (AVG), de Wet Politiegegevens (Wpg), wetten met betrekking tot basisregistraties, zoals de Basisregistratie Personen (BRP), de Archiefwet, maar ook om wetgeving met betrekking tot specifieke taken van de gemeente zoals de Wet Structuur Uitvoeringsorganisatie Werk en Inkomen (SUWI), de Wet maatschappelijke ondersteuning (Wmo) en de Jeugdwet.

De Avg vereist in dit kader passende organisatorische en technische beveiligingsmaatregelen rekening houdend met de stand van de techniek, de kosten alsook de aard, omvang, context en de waarschijnlijkheid en ernst van risico's (zie Avg art 32 lid 1) en ook aantoonbaarheid, evaluatie en aanpassing van de maatregelen en andere verplichtingen van de Avg (Art 5 lid 2; Art 24 lid 1).

De organisatie wil "in control" zijn, dat wil zeggen overzicht hebben en risico's bewust nemen vanuit bestuurlijk niveau. Dit betekent dat eventuele (rest-)risico's die niet afgedekt (kunnen) worden door beheersmaatregelen, bijvoorbeeld omdat zij niet proportioneel worden geacht, ter acceptatie worden voorgelegd aan de directieraad van de organisatie.

De organisatie past daarvoor de drie verdedigingslijnen toe vanuit Interne Controle:

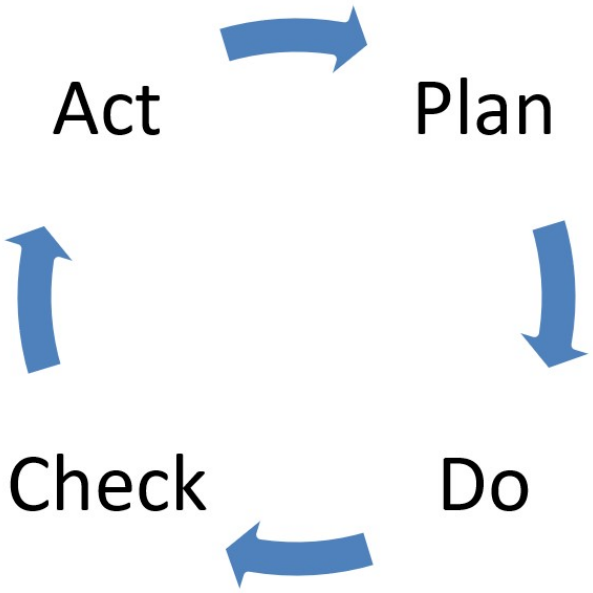
1) De beheersing van werkprocessen binnen de afdeling onder verantwoordelijkheid van de lijnmanager. Dat wil zeggen: werkprocessen op orde, passende werkinstructies en werken volgens afspraken.
2) Borging/controle van beheersmaatregelen in de lijn, bijvoorbeeld door kwaliteitsfunctionarissen of teamleiders. Deze borgingsmaatregelen/controles hebben als doel vast te stellen en aan te tonen dat werkprocessen conform de afspraken verlopen en deze te evalueren en waar nodig aan te passen. Deze borging wordt voor informatiebeveiliging gecoördineerd door de CISO en uitgevoerd in de lijn op basis van een controleplan. Dit omvat ook de diverse audits vanuit ENSIA (Eenduidige Normatiek Single Information Audit).
3) Interne en externe audits vanuit de stafafdeling Concerncontrol, onder andere de Verbijzonderde Interne Controles (VIC) en controles/audits op basis van art. 213a van de Gemeentewet en art. 33 van de Wet Politiegegevens. Daaronder valt ook de evaluatie van de opzet, bestaan en werking van de 1e en de 2e verdedigingslinie.

Managementsysteem voor informatiebeveiliging (ISMS)

De BAR-organisatie doorloopt een plan-do-check-act cyclus voor de verbetering en beheersing van de verwerking van persoonsgegevens. Het doorlopen van deze cyclus vormt het managementsysteem voor informatiebeveiliging (ISMS). De plan-do-check-act cyclus wordt op het niveau van de BAR-organisatie en op het niveau van de beheersmaatregelen toegepast:

- *Plan*: inrichten en documenteren van de beheersmaatregelen en de organisatiebrede aanpak van informatiebeveiliging op basis van geldende normen, wettelijke eisen en risico's voor de organisatie. (in termen van interne controle: de opzet, 1e verdedigingslinie)
- *Do*: aantonen van de uitvoering van beheersmaatregelen en de organisatie-brede aanpak van informatiebeveiliging. (in termen van interne controle: het bestaan, 1e verdedigingslinie)
- *Check*: de borging/controle en evaluatie van de beheersmaatregelen en de organisatiebrede aanpak van informatiebeveiliging met als criteria de volledige uitvoering van de maatregelen en de effectiviteit hiervan. Daarbij wordt ook rekening gehouden met de voortschrijdende ontwikkeling van de techniek en bedreigingen. Hieronder vallen ook interne en externe audits. (de werking, 2e en 3e verdedigingslinie)
- *Act*: het aanpassen en/of verbeteren van beheersmaatregelen en de organisatiebrede aanpak van informatiebeveiliging op basis van bovengenoemde evaluatie.

Het doorlopen van deze cyclus zorgt voor een adequate beheersing waarbij de organisatie aantoonbaar voldoet aan de BIO.



Beheersmaatregelen / Control Framework

De organisatie committeert zich aan de Baseline Informatiebeveiliging Overheid (BIO) die is vastgesteld voor alle overheidslagen. De BIO is gebaseerd op de beheersmaatregelen van de internationale norm ISO27001, die deels nader zijn uitgewerkt in overheidsmaatregelen.

Keuzes bij implementatie en aanpassing van de beheersmaatregelen, zoals die uit de BIO, zijn gebaseerd op een risicoafweging en worden proportioneel getroffen. Daarbij wordt onder andere rekening gehouden met de financiële mogelijkheden van de organisatie respectievelijk de deelnemende gemeenten. Voor de proportionele toepassing van maatregelen wordt gebruik gemaakt van een dataclassificatie. Daarmee kunnen beheersmaatregelen worden afgestemd op het risicoprofiel van de gegevens ten aanzien van de vertrouwelijkheid, integriteit en beschikbaarheid ("BIV") van de gegevens.

De organisatie houdt een overzicht bij van de implementatie van de beheersmaatregelen uit de BIO. Wanneer gekozen wordt af te wijken van de BIO, wordt daarover besloten door de directieraad van de BAR-organisatie.

Conform de eisen van de BIO wordt, waar van toepassing en indien mogelijk, gebruik gemaakt van de standaarden van het Forum Standaardisatie van de Nederlandse Overheid (https://www.forumstandaardisatie.nl/open-standaarden).

De organisatie werkt nauw samen met landelijke diensten voor gemeenten, zoals de In-formatiebeveiligingsdienst (IBD).

Zowel in het overkoepelend (strategisch) informatiebeveiligingsbeleid en aanvullende beveiligingsbeleidsdocumenten moet ook verankering plaatsvinden naar aanvullende wet- en regelgeving of specifieke onderwerpen zoals beveiliging van Procesautomatisering (PA) en IoT.

Externe partijen

De BAR-organisatie verlangt dat externe partijen die gegevens in opdracht van de organisatie verwerken en ketenpartners waarmee gegevens van inwoners worden uitgewisseld aantoonbaar voldoen aan een vergelijkbaar niveau van informatiebeveiliging als de BAR-organisatie zelf. Het gaat daarbij bijvoorbeeld om IT-leveranciers, maar ook ketenpartners in bijvoorbeeld Wmo en Jeugdzorg, zoals zorginstellingen. Dit wordt gewaarborgd in juridische overeenkomsten, zoals verwerkersovereenkomsten.

MEDEWERKERS

Wanneer dit beleid en/of beheersmaatregelen eisen stellen aan taken en verantwoordelijkheden van medewerkers dan worden deze opgenomen in aanvullende individuele afspraken op functieniveau tussen de leidinggevende en de medewerker. Immers in de HR21 normfuncties zijn de werkzaamheden

met betrekking tot informatiebeveiliging niet expliciet opgenomen. Deze specifieke werkzaamheden passen niet bij het karakter van een generieke functiebeschrijving waarin de werkzaamheden op hoofdlijnen zijn beschreven. Conflicterende taken en verantwoordelijkheden behoren hierbij te worden gescheiden.

Iedere medewerker, zowel vast als tijdelijk, intern of extern, (keten)partner of betrokkene, is verplicht waar nodig gegevens en applicaties te beschermen tegen ongeautoriseerde toegang (naleven informatiebeveiligingsbeleid), gebruik, verandering (manipulatie), openbaring, vernietiging, verlies of ongeautoriseerde overdracht. Bij (vermeende) inbreuken hierop dienen medewerkers dit te melden bij de helpdesk.

Iedere medewerker wordt geacht de gedragsregels van de organisatie te kennen en uit te dragen bij het uitoefenen van zijn of haar functie. We gaan uit van de eigen verantwoordelijkheid van medewerkers zowel vast als tijdelijk, intern of extern en overige betrokkene(n) voor hun gedrag binnen het vastgestelde beleid, de basisregels en geldende normenkaders.

4: DE AANPAK VAN INFORMATIEBEVEILIGING

JAARCYCLUS

Om de borging van het informatieveiligheidsbeleid en de daarvan afgeleide plannen te realiseren, doorloopt de BAR-organisatie de onderstaande Plan, Do, Check, Act (PDCA) cyclus, zowel organisatiebreed als per beheersmaatregel, resulterend in een Information Security Management System (ISMS).

Het ISMS wordt toegepast door in aansluiting bij (bestaande) bestuurs- en P&C-cycli jaarlijks:

– **Plan**: Een jaarplan met verbeterpunten op te stellen, rekening houdend met de organisatiestrategie en -doelstellingen, risico's, regelgeving, de stand van de techniek en beschikbare middelen.

  Het jaarplan voor informatiebeveiliging wordt opgesteld op basis van:

  - evaluatie van de uitvoering en resultaten van het vorige verbeterplan;
  - risicoanalyse t.a.v. informatiebeveiliging op basis van de separaat beschreven aanpak voor risicoanalyse die het identificeren, analyseren/beoordelen, evalueren en het nemen van maatregelen omvat;
  - evaluatie van de implementatie van beheersmaatregelen ten opzichte van de BIO (GAP-analyse);
  - informatiebeveiligingsincidenten;
  - trends ten aanzien van bedreigingen, kwetsbaarheden en technologische mogelijkheden en maatschappelijke ontwikkelingen;
  - het informatiebeveiligingsbeleid en evaluatie van de naleving daarvan;
  - de strategie en doelstellingen van de organisatie.

  Het plan bevat meetbare doelen en een activiteitenplanning met verantwoordelijken, benodigde middelen, tijdslijnen en resultaten.

– **Do**: het jaarplan en beheersmaatregelen uit te voeren, waarbij beveiligingsmaatregelen worden ingevoerd en stapsgewijs worden verbeterd. De uitvoering van het jaarplan en de beheersmaatregelen wordt bewaakt. De CISO rapporteert daarover elk kwartaal via de Stuurgroep I&P aan de directie. Waar nodig worden er aanvullende maatregelen genomen.
– **Check**: borgings-/controleacties uit te voeren om vast te stellen of de beheersmaatregelen volledig zijn geïmplementeerd en of zij effectief zijn. De borgings-/controle acties worden opgenomen in een controleplan, zodat alle geïmplementeerde maatregelen passend worden afgedekt. Ook de jaarlijkse controle op de technische naleving van beveiligingsnormen bij informatiesystemen, zoals kwets-baarheidsanalyses/-scans en penetratietesten zijn onderdeel van dit controleplan. De CISO rapporteert elk kwartaal daarover en over incidenten en andere relevante gebeurtenissen via de Stuurgroep I&P aan de directie, vergezeld van verbetervoorstellen, waar van toepassing.

  Voor geïmplementeerde onderdelen van het ISMS en geïmplementeerde beheersmaatregelen wordt bepaald of en zo ja hoe deze worden opgenomen in het audit-plan van de organisatie. Jaarlijks wordt een auditplan (intern controleplan) opgesteld waarin wordt vastgelegd welke interne controles en audits in het komende jaar plaatsvinden en op welke informatiesystemen deze betrekking hebben.

Op basis van de rapportages van de CISO en audits wordt de informatieveiligheid geëvalueerd door de Stuurgroep. De voorzitter van de stuurgroep I&P en neemt deze op basis daarvan besluiten over de verbetering van het managementsysteem en beheersingsmaatregelen. Dit mondt uit in het jaarverslag. Daarin wordt in lijn met de P&C-cyclus en ondersteund door een In Control Verklaring (ICV) gerapporteerd over het doorlopen van de beschreven PDCA-cyclus met betrekking tot in-formatieveiligheid. In deze rapportage worden ook andere voor informatieveiligheid en privacy relevante onderwerpen – zoals auditresultaten en de uitkomsten van interne controles – behandeld.

– **Act**: bij te sturen, te herprioriteren en/of aanvullende maatregelen te nemen of aanbevelingen te doen voor het volgende verbeterplan naar aanleiding van afwijkingen van plannen en beheersmaatregelen en andere ontwikkelingen, bijvoorbeeld in de maatschappij, wet- en regelgeving of techniek. Dit gebeurt met name in de Stuurgroep I&P op basis van de adviezen van de CISO. Waar nodig vindt besluitvorming in de directie of op bestuurlijk niveau plaats. Daarmee zorgt de organisatie voor een continue verbetering van een passende informatiebeveiliging.

IMPLEMENTATIE OF VERNIEUWING VAN BEDRIJFSPROCESSEN

Naast deze jaarlijkse cyclus wordt bij de implementatie of vernieuwing van bedrijfsprocessen de beveiliging van informatie geborgd. Het gaat daarbij bijvoorbeeld om de implementatie van nieuwe taken, werkprocessen of nieuwe (versies van) applicaties. De CISO en CPO stellen daarvoor een proces op dat waarborgt dat nieuwe of vernieuwde bedrijfsprocessen voldoen aan het informatiebeveiligingsbeleid en dat de vereiste beheersmaatregelen daarvoor zijn geïmplementeerd. Dit proces bevat ten minste de volgende onderdelen:

– een dataclassificatie, waarin de eisen aan vertrouwelijkheid, integriteit en beschikbaarheid van de gegevens in het nieuwe of vernieuwde proces worden vastgesteld;
– een DPIA (Data Protection Impact Assessment, dan wel, Gegevensbeschermingsef-fectbeoordeling) wordt alleen uitgevoerd als deze verplicht is. De DPIA bestaat onder andere uit een analyse van risico's voor betrokkenen en een onderbouwing van de rechtmatigheid van de nieuwe verwerking van persoonsgegevens;
– bij een hoge dataclassificatie wordt een risicoanalyse uitgevoerd, tenzij deze al in het kader van een DPIA is of wordt uitgevoerd. In een risicoanalyse worden risico's geïdentificeerd en beoordeeld. Op basis daarvan beslist de proceseigenaar om een risico te accepteren, te beperken (te mitigeren), over te dragen (te verzekeren) of te vermijden (door de activiteit te staken);
– keuze van passende maatregelen om de informatiebeveiligingsrisico's te beperken;
– acceptatie van eventuele restrisico's door de directieraad;
– bewaking van de uitvoering van de gekozen maatregelen ten aanzien van de risico's die in de DPIA of in de risicoanalyse zijn vastgesteld.

SAMENWERKING

Specifieke informatie op het gebied van informatiebeveiliging van relevante expertise-groepen, leveranciers van hardware, software en diensten en de informatiebeveiligings-dienst voor gemeenten (IBD) wordt gebruikt om de informatiebeveiliging te verbeteren.

De organisatie heeft uitgewerkt met welke instanties contact wordt onderhouden en door wie. Dit overzicht wordt door de CISO beheerd en minimaal jaarlijks bijgewerkt.

EVALUATIE EN HERZIENING

Het Informatiebeveiligingsbeleid wordt ten minste elke drie jaar herzien op basis van:

– een evaluatie van het beleid;
– maatschappelijke ontwikkelingen en ontwikkelingen in de organisatiestrategie, wet- en regelgeving, de stand van de techniek en bedreigingen;
– organisatiestrategie en -doelstellingen;
– documentatie van de jaarlijkse verbetercycli (zie boven);
– terugkoppeling van belanghebbende partijen, bijvoorbeeld de gemeenteraad en de medezeggenschap;
– onafhankelijke beoordelingen (audits);
– aanbevelingen van relevante instanties, zoals toezichthouders (bijvoorbeeld de Autoriteit Persoonsgegevens), de VNG en de IBD.

5: PUBLICATIE EN WIJZIGINGEN

Dit document staat voor iedereen binnen de BAR-organisatie ter inzage op het intranet en wordt op aanvraag ter beschikking gesteld aan andere belanghebbenden. Dit document wordt periodiek geactualiseerd. De geactualiseerde versie wordt op het intranet gepubliceerd en de medewerkers worden daarop geattendeerd.

Het Algemeen Bestuur van de BAR-organisatie op 18 oktober 2022

De heer H.W.J. Klaucke
Secretaris

Mevrouw A. Attema
Voorzitter BAR-organisatie

BIJLAGE 1: ROLLEN EN NAMEN

Dit overzicht wordt ingevuld en bijgehouden door de CPO en de CISO, mede op basis van de benoemingen van DAPI door de Cluster-managers en teamleiders en gepubliceerd op intranet. Hier is afgezien van het invullen van namen in verband met wijzigingen en de verspreiding van dit beleid.

Rol	Naam	Vervanger
Chief Information Security Officer (CISO)		
Operationeel/Technisch ISO (TISO)		
Operationeel ISO Maatschappij en Veiligheid, Ensia en projecten		
Coördinerend Privacy Officer (CPO)		
Operationeel Privacy Officer		
Operationeel PO Maatschappij en Veiligheid en Projecten		
Controller Informatiebeveiliging en Privacy		
Functionaris Gegevensbescherming		
DAPI Cluster Staf (Concerncontrol, Financiën en Strategie)		
DAPI Dienstverlening (incl. BRP, WD)		
DAPI Cluster I&A		
DAPI Juridische Zaken en Inkoop		
DAPI Cluster Uitvoering		
DAPI Cluster Voorbereiding en Beheer		
DAPI Cluster Facilitair		
DAPI Cluster Ontwikkeling leefomgeving en regio		
DAPI Cluster Ruimtelijke Ontwikkeling		
DAPI Cluster Vastgoed		
DAPI Cluster Ontwikkeling Mens en Organisatie		
DAPI Cluster Veiligheid – team BOA		
DAPI Cluster Veiligheid – APV en OOV		
DAPI Cluster Maatschappij – Team Participatie, schulddienstverlening & wijkteams incl. SUWI		
DAPI Cluster Maatschappij – Team Leerplicht & Jeugd		
DAPI Cluster Maatschappij – Team WMO		