

Handreiking

Screening personeel

Een operationeel kennisproduct ter ondersteuning van de implementatie van de Baseline Informatiebeveiliging Overheid (BIO)

Colofon

### Naam document

Handreiking screening personeel

### Versienummer

2.01

### Versiedatum

Februari 2020

### Versiebeheer

Het beheer van dit document berust bij de Informatiebeveiligingsdienst voor gemeenten (IBD).



Vereniging van Nederlandse Gemeenten / Informatiebeveiligingsdienst voor gemeenten (IBD) (2018)

Tenzij anders vermeld, is dit werk verstrekt onder een Creative Commons Naamsvermelding-Niet Commercieel-Gelijk Delen 4.0 Internationaal licentie. Dit houdt in dat het materiaal gebruikt en gedeeld mag worden onder de volgende voorwaarden: Alle rechten voorbehouden. Verveelvoudiging, verspreiding en gebruik van deze uitgave voor het doel zoals vermeld in deze uitgave is met bronvermelding toegestaan voor alle gemeenten en overheidsorganisaties.

Voor commerciële organisaties wordt hierbij toestemming verleend om dit document te bekijken, af te drukken, te verspreiden en te gebruiken onder de hiernavolgende voorwaarden:

1. De IBD wordt als bron vermeld;
2. Het document en de inhoud mogen commercieel niet geëxploiteerd worden;
3. Publicaties of informatie waarvan de intellectuele eigendomsrechten niet bij de verstrekker berusten, blijven onderworpen aan de beperkingen opgelegd door de IBD en / of de Vereniging van Nederlandse Gemeenten;
4. Iedere kopie van dit document, of een gedeelte daarvan, dient te zijn voorzien van de in deze paragraaf vermelde mededeling.

Wanneer dit werk wordt gebruikt, hanteer dan de volgende methode van naamsvermelding: “Vereniging van Nederlandse Gemeenten / Informatiebeveiligingsdienst voor gemeenten”, licentie onder: CC BY-NC-SA 4.0.

Bezoek <http://creativecommons.org/licenses/by-nc-sa/4.0> voor meer informatie over de licentie.

### Rechten en vrijwaring

De IBD is zich bewust van haar verantwoordelijkheid een zo betrouwbaar mogelijke uitgave te verzorgen. Niettemin kan de IBD geen aansprakelijkheid aanvaarden voor eventueel in deze uitgave voorkomende onjuistheden, onvolledigheden of nalatigheden. De IBD aanvaardt ook geen aansprakelijkheid voor enig gebruik van voorliggende uitgave of schade ontstaan door de inhoud van de uitgave of door de toepassing ervan.

### Met dank aan

De expertgroep en de reviewgemeenten die hebben bijgedragen aan het vervaardigen van dit product.

### Wijzigingshistorie

|  |  |  |
| --- | --- | --- |
| Versie | Datum | Wijziging / Actie |
| 1.0 | 08-10-2013 | Eerste versie |
| 1.0.1 | 28-06-2015 | Links met meer info over VOG en screening toegevoegd |
| 1.0.2 | Augustus 2016 | Taskforce BID verwijder, WBP vervangen door Wbp, GBA vervangen door BRP |
| 2.0 | Februari 2019 | BIO update |
| 2.01 | Februari 2020 | Enkele wijzigingen naar aanleiding van het wijzigen van overheidsmaatregel 7.1.1.1 (wijzigingen in groen) |

Over de IBD

De IBD is een gezamenlijk initiatief van alle Nederlandse Gemeenten. De IBD is de sectorale CERT / CSIRT voor alle Nederlandse gemeenten en richt zich op (incident)ondersteuning op het gebied van informatiebeveiliging. De IBD is voor gemeenten het schakelpunt met het Nationaal Cyber Security Centrum (NCSC). De IBD ondersteunt gemeenten bij hun inspanningen op het gebied van informatiebeveiliging en privacy / gegevensbescherming en geeft regelmatig kennisproducten uit. Daarnaast faciliteert de IBD kennisdeling tussen gemeenten onderling, met andere overheidslagen, met vitale sectoren en met leveranciers. Alle Nederlandse gemeenten kunnen gebruikmaken van de producten en de generieke dienstverlening van de IBD.

De IBD is ondergebracht bij VNG Realisatie.

Leeswijzer

Dit product is een nadere uitwerking voor gemeenten van de Baseline Informatiebeveiliging Overheid (BIO). De BIO is eind 2018 bestuurlijk vastgesteld als gezamenlijke norm voor informatiebeveiliging voor alle Nederlandse overheden.

**Doel**

Het doel van dit document is het geven van een handreiking over hoe invulling kan worden gegeven aan de verificatie van de achtergrond van alle kandidaten (medewerkers), betrokken medewerkers van leveranciers en ingehuurd personeel. Deze verificatie heet ook screening van personeel en wordt al binnen gemeenten gebruikt voor wat het betreft het verkleinen van integriteitsrisico’s.

**Doelgroep**

Dit document is van belang voor het bestuur, management, de HR-afdeling en de gebruikers.

**Relatie met overige producten**

* Baseline Informatiebeveiliging Overheid (BIO)
* Informatiebeveiligingsbeleid van de gemeente

Verwijzingen naar de Baseline Informatiebeveiliging voor de Overheid (BIO)

7.1.1 Screening.

### Wat is er veranderd ten opzichte van de BIG?

Er is weinig veranderd ten opzichte van de BIG, in de maatregelen en controls is er een kleine nuance.

### Wat is er veranderd in de BIO 1.04?

In de BIO 1.04 is overheidsmaatregel 7.1.1.1 gewijzigd. Het is nu niet meer verplicht om voor alle medewerkers een VOG aan te vragen, maar dat alleen op basis van risicoafweging te doen. Dit moet nader uitgewerkt zijn in een screeningsbeleid.

Inhoudsopgave

[1. Inleiding 6](#_Toc14780880)

[2. Functieclassificatie 7](#_Toc14780881)

[2.1. Inleiding 7](#_Toc14780882)

[2.2. Vertrouwensfuncties 7](#_Toc14780883)

[2.3. Kwetsbare functies 8](#_Toc14780884)

[2.4. Algemene functies 9](#_Toc14780885)

[3. Screeningsinstrumenten 10](#_Toc14780886)

[4. Samenvatting 11](#_Toc14780887)

[Bijlage 1 Tips screeningsinstrumenten 12](#_Toc14780888)

# Inleiding

De Baseline Informatiebeveiliging Overheid (BIO) beschrijft in hoofdstuk 7 op welke wijze informatiebeveiliging geïntegreerd dient te worden in de HR-cyclus (van werving tot uitdiensttreding). Het operationele product ‘Handreiking personeelsbeleid gemeente’ gaat hier op in. Voorliggend document focust zicht op de screening van alle kandidaten (medewerkers), betrokken medewerkers van leveranciers en ingehuurd personeel.

### Doelstelling screening

Bewerkstelligen dat alle kandidaten (medewerkers), betrokken medewerkers van leveranciers en ingehuurd personeel hun verantwoordelijkheden begrijpen, geschikt zijn voor de rollen waarvoor zij worden overwogen, en om het risico van diefstal, fraude of misbruik van faciliteiten te verminderen.

Dit document geeft een handreiking over hoe invulling kan worden gegeven aan de verificatie van de achtergrond voor alle kandidaten (medewerkers), betrokken medewerkers van leveranciers en ingehuurd personeel. Deze verificatie heet ook screening van personeel en wordt al binnen gemeenten gebruikt voor wat betreft het verkleinen van integriteitsrisico’s.

### De indeling van dit document is als volgt:

Hoofdstuk 2 ‘Functie classificatie’: In dit hoofdstuk wordt een aantal typen functies en een aantal aandachtspunten beschreven waar bij screening rekening gehouden kan worden.

Hoofdstuk 3 ‘Screeningsinstrumenten’: In dit hoofdstuk worden de verschillende screeningsinstrumenten besproken.

Hoofdstuk 4 ’Samenvatting’: In dit hoofdstuk staat een checklist met een overzicht van de belangrijkste punten ten aanzien van screening.

Bijlage: De bijlage bevat tips ten aanzien van de verschillende screeningsinstrumenten

### Relatie met integriteit(sprotocol)

Als een gemeente al een integriteitsprotocol beschreven heeft:

Deze handreiking is qua opzet geschreven om informatiebeveiligingsmaatregelen te laten samenvallen binnen het bestaande integriteitsprotocol van gemeenten. Gemeenten kunnen er ook voor kiezen om het eigen integriteitsprotocol aan te vullen met het aspect informatiebeveiliging. In wezen hebben de informatiebeveilgingsmaatregelen betrekking op de integriteitsrisicofactor ‘Omgaan met vertrouwelijke informatie’.

### Belangrijke opmerking

Een goede screening van personeel vraagt de nodige tijd en aandacht. Een zorgvuldig aanstellingsbeleid waarin uitgebreid aandacht wordt besteed aan de integriteit van de sollicitant maakt echter vanaf het begin de verhouding tussen de gemeente en de sollicitant helder. Punten van verschil in inzicht of belangenverstellingen dienen op het moment van aanname te worden uitgesloten of duidelijk te zijn gemaakt. Zo komen sollicitant en de gemeente niet voor onaangename verrassingen te staan.

# Functieclassificatie

## Inleiding

Door het screenen van personeel worden integriteits- en beveiligingsrisico’s verkleind bij de aanstelling van ambtenaren en het in dienst nemen van overig personeel. Door een objectieve vaststelling of bevestiging van het (werk)verleden van de betrokkene worden aanwijzingen verkregen omtrent de moraliteit en de reputatie van de betrokkene.

Voordat wordt overgegaan tot het aannemen van personeel is het van belang dat de risico’s verbonden aan een functie kenbaar zijn. Alleen als deze risico’s helder zijn, kan onder meer in de wervingsadvertentie, de functiebeschrijving en de sollicitatieprocedure aandacht worden besteed aan bepaalde eigenschappen waarover de functionaris/sollicitant al dan niet moet beschikken met betrekking tot integriteit en beveiligingseisen. Daarna kunnen integriteits- en beveiligingsaspecten geborgd worden in de organisatie door aan beide onderwerpen blijvend aandacht te besteden tijdens onder meer werkoverleggen, functionerings- en beoordelingsgesprekken en bij functiewijziging.

In deze handreiking wordt gewerkt met de volgende indeling van functies:

* Vertrouwensfuncties
* Kwetsbare functies
* Algemene functies

Deze handreiking zal niet per functie voorschrijven in welke categorie een functie moet worden ingedeeld. De gemeente kent daarvoor ook per afdeling, dienst, bedrijf of stadsdeel een te grote variëteit aan functies. Ook zal niet per categorie aangegeven worden welke screeningsinstrumenten moeten worden ingezet. De hieronder beschreven functiecategorieën geven een beeld van (grote of meerdere) risico’s die aan sommige functies zijn verbonden. Zo kan een organisatie zelf bepalen of zulke functies aanwezig zijn, en hier bij het screenen rekening mee houden.

In alle functies geldt overigens, of nu al dan niet risicofactoren aanwezig zijn, dat verwacht mag worden dat integer wordt gehandeld en ook dat de geheimhoudingsplicht in acht wordt genomen. Daarmee wordt gedoeld op een algemene professionele verantwoordelijkheid van de ambtenaar op zijn vakgebied.

## Vertrouwensfuncties

Vertrouwensfuncties zijn functies als bedoeld in de Wet op de Veiligheidsonderzoeken (WVO). Dit zijn functies waarin de mogelijkheid bestaat de veiligheid of andere gewichtige belangen van de staat te schaden. In een vertrouwensfunctie werkt men met informatie die als vertrouwelijk of geheim geclassificeerd wordt. Het openbaar maken van deze informatie kan grote gevolgen hebben voor de staatsveiligheid en de maatschappij ontregelen. Of een functie een vertrouwensfunctie is wordt bepaald door de Minister die verantwoordelijk is voor het beleidsterrein waartoe een vertrouwensfunctie, gezien de aard daarvan, behoort. Als een functie wordt aangewezen als vertrouwensfunctie voert de Algemene Inlichtingen- en Veiligheidsdienst (AIVD) een zogenaamd veiligheidsonderzoek uit om vast te stellen of de kandidaat de verplichtingen in deze functie onder alle omstandigheden loyaal zal vervullen. Is er niet of nauwelijks sprake van een risico, dan ontvangt de kandidaat-vertrouwensfunctionaris een schriftelijke verklaring van geen bezwaar[[1]](#footnote-2).

De gemeente kan een aantal functies aan laten wijzen als vertrouwensfunctie. Dit betreft dan over het algemeen functies die van nationaal belang zijn en die bijvoorbeeld een rol hebben binnen de crisisbeheersingsstructuur van Nederland.[[2]](#footnote-3)

## Kwetsbare functies

Kwetsbare functies hebben vooral te maken met het aspect integriteit en daarvoor zijn verschillende factoren in kaart gebracht welk hieronder opgesomd zijn. Met behulp van onderstaande opsomming van risicofactoren kan elke organisatie zelf beoordelen welke factoren voorkomen in welke functies, en derhalve welke functies te kwalificeren zijn als kwetsbare functies voor die specifieke dienst of dat specifieke stads- of gemeentedeel.

De opsomming van risicofactoren heeft primair tot doel dat men zich bewust wordt van mogelijke integriteitrisico’s in bepaalde functies. Tabel 1 geeft een indicatieve opsomming.

Hoe meer risicofactoren voorkomen in een functie (of hoe belangrijker deze factor voor de functie is), hoe belangrijker het is dat al in het werving- en selectieproces aandacht wordt besteed aan integriteit, bij voorkeur met behulp van de instrumenten die in hoofdstuk 3 van deze handreiking worden beschreven. Geprobeerd is bij elk van de onderstaande risicofactoren die een functie meer kwetsbaar kunnen maken te beschrijven welk risico kan worden gelopen. De voorbeeldfuncties zijn illustratief, maar geven een beeld van kwetsbaarheden in functies; soms zijn functies meer risicovol dan ze op het eerste gezicht lijken. Bij twijfel is de verantwoordelijk manager die bepaalt in hoeverre een kwetsbaarheid in een functie manifest zou kunnen zijn, of dat er mitigerende maatregelen worden getroffen (bijvoorbeeld het 4-ogen principe bij beslissingen, of extra controle in de vorm van een audit).

|  |  |  |  |
| --- | --- | --- | --- |
| Risicofactor | Criterium | Risico | Voorbeeld van functies |
| Vertrouwelijke informatie | De beschikking hebben over vertrouwelijke en/of strategische informatie | Doorspelen/verkopen informatie, wijzigen, manipuleren of misbruik van informatie | Systeembeheerder, personeelsadviseur, medewerker communicatie |
| Omgaan met geld | Zich bezighouden met het ontvangen / declareren of uitgeven of toekennen van gelden | Fraude / diefstal / verduistering / omkoping / belangenverstrengeling | (hoofd) kassier, medewerker Inkoop, buschauffeur, medewerker Burgerzaken |
| Machts- en monopoliepositie | Het hebben van een positie waarbij op basis van status/deskundigheid invloed kan worden uitgeoefend op besluitvorming en/of personen | Machtsmisbruik | Leidinggevende functies |
| Toekennen rechten/ bevoegdheden (aan personeel of burgers) | Toegang voor bevoegde gebruikers bewerkstelligen en onbevoegde toegang tot informatiesystemen voorkomen | Misbruik van bevoegdheden, fraude. | Systeembeheerder, vergunningen-verstrekker, medewerker Sociale Dienst |
| Beoordelen en adviseren (met grote gevolgen) | In de positie zijn om beoordelingen uit te voeren en adviezen te verstrekken waar grote belangen mee gemoeid gaan. | Machtsmisbruik, omkoping, ongewenste beïnvloeding (kwetsbaar voor derden die grote belangen hebben bij oordeel/ advies in een specifieke richting, en die op allerlei mogelijke manieren zullen proberen besluitvorming hierover te beïnvloeden) | Adviseurs B&W, medewerker Juridische Zaken |
| Aanschaffen goederen/diensten/ aanbestedingen | Ambtenaren belast met de inkoop van goederen en diensten | Diefstal, fraude, omkoping | Projectleiders, medewerker Inkoop, medewerker projectbureau |
| Handhaven | Zich bezighouden met het handhaven van gemeentelijk beleid | Omkoping | Parkeercontroleurs, milieuagenten, gemandateerd toezichthouders, accountant, BWT-inspecteurs[[3]](#footnote-4) |
| Solistisch handelen | Ambtenaren voeren alleen of zeer zelfstandig kwetsbare handelingen uit, of nemen alleen of zeer zelfstandig besluiten, waarbij de kwaliteit van de besluitvorming en de controle op uitgevoerde handelingen onvoldoende is gewaarborgd | Omkoping, machtsmisbruik, misbruik van bevoegdheden, fraude et cetera (alle vormen van integriteitschendingen (of de schijn daarvan) zijn mogelijk doordat iemand alleen opereert/ besluiten neemt en er geen controle/ direct toezicht plaatsvindt | Directeur, opzichter, medewerker buitendienst |
| Werken in de directe invloedssfeer van burgers/ bedrijven | Ambtenaren bevinden zich structureel of zeer regelmatig in de directe invloedsfeer van burgers en bedrijven waardoor beïnvloeding van de beoordeling en/of beslissing (inhoudelijk, qua timing en/of argumentatie) door de ambtenaar plaatsvindt | Diverse vormen van belangenverstrengeling | Medewerker buitendienst, loketfuncties. |

Tabel 1 Opsomming risicofactoren

## Algemene functies

De algemene functies vormen de restgroep. In deze functies komen de in paragraaf 2.3 genoemde risicofactoren niet of nauwelijks voor. Dat wil zoals gezegd niet zeggen dat integriteit in deze functies geen rol speelt. Ook bij de algemene functies is een goede screening en het informatiebeveiligingsaspect van belang.

# Screeningsinstrumenten

Het vorige hoofdstuk biedt handvatten om de risico’s van functies te bepalen. Voordat er geworven gaat worden voor een functie moeten de integriteit- en de veiligheidsrisico’s van die functie in kaart zijn gebracht, welke vervolgens meegenomen worden in de sollicitatieprocedure. De sollicitatieprocedure biedt een aantal screeningsinstrumenten die hieronder kort beschreven worden. In de bijlage worden deze instrumenten meer gedetailleerd uitgewerkt. De screeningsinstrumenten zijn manieren om te controleren of het beeld dat de sollicitant wil oproepen klopt en of de instrumenten onderling in samenhang zijn. Een hiaat bij de een kan verduidelijkt of juist versterkt worden door andere controles uit het instrumentarium.

### Het sollicitatiegesprek

Het sollicitatiegesprek is de manier om de sollicitant in persoon te ontmoeten en middels interactie antwoorden te krijgen op allerhande vragen. Het gesprek biedt mogelijkheden om te onderzoeken of de sollicitant weet en begrijpt wat er verwacht wordt met betrekking tot integriteit en geheimhouding. Daarnaast kunnen er vragen gesteld worden over de motivatie/sollicitatiebrief en het curriculum vitae (CV) en kan er een eerste inschatting gemaakt worden op de zachte kant van de match.

### Identificatie

Voor wat betreft de identificatie is er een wettelijke verplichting dit te controleren. In deze fase is het belangrijk geen genoegen te nemen met bijvoorbeeld een kopie van een identiteitsbewijs.

### Diploma’s/ Certificaten/ Cijferlijsten/ CV

De sollicitant heeft verschillende manieren om aan te tonen of zijn kennis en kunde in overeenstemming is met de functie-eisen. Het is belangrijk om geen genoegen te nemen met kopieën van deze documenten, omdat de kans bestaat dat deze anders aangepast zijn waarmee de sollicitant zich beter wil doen laten voorkomen dan hij in werkelijkheid is.

### Ontslagbrieven, getuigschriften

Ontslagbrieven en getuigschriften geven een direct beeld over het werkverleden van de sollicitant. Bedenk hierbij dat getuigschriften altijd een subjectief beeld zijn van (vaak) een leidinggevende. Ze kunnen daarentegen wel een beeld geven van de werkzaamheden die in het CV genoemd staan. De ontslagbrief kan bijdragen in de controle van de in het CV opgegeven werkervaringsperioden.

### Referenties

Referenties zijn een belangrijk instrument om een beeld te krijgen van de sollicitant. Referenties kunnen gevraagd worden om een algemeen beeld, maar beter is het om de referentie te gebruiken om te controleren of de werkzaamheden van de sollicitant ook kloppen met de werkelijkheid. Bedenk goed dat de sollicitant alleen die personen opgeeft waarmee hij ook daadwerkelijk een klik had. De meeste referenties zullen dus altijd positief zijn over de sollicitant.

### Verklaring omtrent het gedrag (VOG)[[4]](#footnote-5)

Een VOG is een verklaring waaruit blijkt dat het gedrag van de sollicitant in het verleden geen bezwaar vormt voor het vervullen van een specifieke taak of functie in de samenleving. Justis screent het gedrag van personen die een VOG aanvragen en geeft de VOG's af. Alle sollicitanten die gaan werken bij een gemeente moeten voor aanvang een VOG aangevraagd hebben en deze kunnen overleggen. Een VOG wordt altijd afgegeven als er geen strafbaar feit is gepleegd dat relevant is voor de betreffende functie. Een VOG heeft geen einddatum, maar het is goed om geen VOG te accepteren die ouder is dan een jaar.

# Samenvatting

In het kader van het gemeentelijke integriteitbeleid en informatiebeveiligingsbeleid is het van belang dat integriteit en informatiebeveiliging geborgd worden in de organisatie. Het is belangrijk al tijdens het werving- en selectieproces van personeel oog te hebben voor integriteits- en informatiebeveiligingsaspecten. Door een goede screening van nieuw personeel wordt preventief opgetreden en kunnen mogelijk integriteitschendingen en informatiebeveiligingsincidenten worden voorkomen. De handreiking geeft inzicht in de (bestaande) screeningsinstrumenten en beschrijft op welke wijze deze het meest effectief kunnen worden ingezet.

Hieronder nog even kort op een rij de belangrijkste punten:

* Nagaan aan de hand van de risicofactoren (zoals beschreven in de handreiking) in hoeverre de functie kwetsbaar is. Hoe meer risicofactoren er aanwezig zijn, hoe kwetsbaarder de functie en des te belangrijker het is om aandacht te besteden aan het aspect integriteit en informatiebeveiliging tijdens het werving- en selectieproces, de verantwoordelijk manager heeft hier een belangrijke stem in.
* De door de sollicitant aangeleverde documenten, bijvoorbeeld cv, diploma’s en cijferlijsten, getuigschriften checken op bijvoorbeeld echtheid en consistentie (zie voor een uitgebreider beschrijving de bijlage met tips screeningsinstrumenten).
* Voor de functie specifieke integriteit- en informatiebeveiligingsrisico’s kunnen aan de orde worden gesteld tijdens het sollicitatiegesprek. Checken of de sollicitant zich van de risico’s bewust is en of hij/zij daar mee om weet te gaan.
* Als er een keuze is gemaakt voor een sollicitant dan de door de sollicitant opgegeven referenties inwinnen (in- of extern).
* Bij een interne kandidaat kan – na goedkeuring van de sollicitant – het binnen de gemeente aanwezige personeelsdossier worden opgevraagd/ingezien. Vraag om het volledige dossier!
* Voor de aanstelling een VOG aanvragen. Maak bij de aanvraag duidelijk om wat voor soort functie het gaat en welke integriteit- en beveiligingsrisico’s aan de orde zijn. Alleen dan kan bij de afweging om een VOG al dan niet af te geven, hiermee rekening worden gehouden en dit verhoogt de waarde van de VOG.
* Controleer het identiteitsbewijs van de sollicitant aan de hand van de tips en richtlijnen genoemd in de handreiking.

Gebleken is dat uitzendkrachten een kwetsbare groep vormen ten aanzien van integriteit. De werving- en selectie wordt voor een groot deel door het uitzendbureau gedaan omdat de uitzendkracht bij het uitzendbureau in dienst is en niet bij de gemeente. De inlenende organisatie (i.c. de gemeente) kan ook een elektronische VOG-aanvraag initiëren (zie hiervoor de website van de dienst Justis)[[5]](#footnote-6). Zeker bij kwetsbare functies is dit aan te raden. Praktisch gezien heeft dit slechts nut als de uitzendkracht voor langere tijd wordt ingehuurd. Navraag bij het uitzendbureau, bijvoorbeeld welke referenties zij hebben gecheckt, of vragen stellen tijdens het sollicitatiegesprek met betrekking tot integriteit kan natuurlijk wel altijd. Aan de uitzendbureaus is overigens wel de verplichting opgelegd om de uitzendkrachten een geheimhoudings- en een integriteitsverklaring te laten ondertekenen. Check of dit ook daadwerkelijk is gebeurd en of de werkingssfeer zich uitstrekt tot de inlenende organisatie. Vraag altijd om een kopie van de verklaring.

Een goede screening kost de nodige tijd. Een zorgvuldig aanstellingsbeleid waarin uitgebreid aandacht wordt besteed aan de integriteit van de sollicitant maakt echter vanaf het begin de verhouding tussen de gemeente en de sollicitant helder en kan mogelijk voor een deel integriteitsschendingen voorkomen.

Bijlage 1 Tips screeningsinstrumenten

### Het sollicitatiegesprek

Het sollicitatiegesprek geeft een aantal mogelijkheden om te testen of de kandidaat zich bewust is van de risico’s die verbonden zijn aan de functie met betrekking tot integriteit, geheimhouding en informatieveiligheid. Tijdens het gesprek kan men de sollicitant ‘live’ testen door de volgende onderwerpen te behandelen:

* Door middel van het voorleggen van enkele dilemma’s met betrekking tot integriteit en informatieveiligheid. Vooral bij kwetsbare functies is het zinvol om een casus voor te leggen die gaat over integriteitrisico’s die zijn verbonden aan die specifieke functie. Uit de reactie kan opgemaakt worden of de sollicitant zich al dan niet bewust is van de risico’s die zijn verbonden aan de functie. Is dit niet zo, dan biedt dit de mogelijkheid om hierover verder te praten. Het is namelijk voor de sollicitant ook van belang dat deze weet wat er van hem verwacht wordt en dat deze ook de kans krijgt om zelf ook in te schatten of daaraan voldaan kan worden.
* Het onderwerp nevenwerkzaamheden. De gemeente ambtenaar is volgens een Collectieve Arbeidsvoorwaardenregeling en Uitwerkingsovereenkomst (CAR-UWO) verplicht toestemming te vragen voor zijn nevenwerkzaamheden als die de belangen van de gemeente kunnen raken. In dit gesprek kunnen eventuele nevenwerkzaamheden besproken worden en voorts of die een belemmering zouden kunnen opleveren voor de uitoefening van de functie.
* De verplichting tot het afleggen van de ambtseed of de belofte vormt een ingang om het belang dat de gemeente hecht aan integriteit, geheimhouding en informatieveiligheid van haar ambtenaren, te bespreken.

### Identificatie

Vanaf 1 juni 1994 is er in Nederland een wettelijke identificatieplicht, die is geregeld in de Wet op de identificatieplicht (WID). Dit is een verplichting voor betrokkene om in een aantal gevallen te bewijzen dat de gegevens die iemand over zichzelf opgeeft, juist zijn. Om aan deze verplichting te voldoen moet men een identiteitsbewijs overleggen. Met de komst van de identificatieplicht is het veel lastiger geworden om bijvoorbeeld een verkeerde naam op te geven (bijvoorbeeld bij zwartrijden in het openbaar vervoer). De identificatieplicht is een middel om fraude en overige criminaliteit te bestrijden.

Eén van de momenten waarop een geldig identiteitsbewijs moet worden overlegd is op het moment van indiensttreding. Op de werkgever rust de verplichting om een kopie van het identiteitsbewijs in zijn administratie (het personeelsdossier) op te nemen.

Bij indiensttreding zijn de volgende soorten identiteitsbewijs geldig:

* Paspoort (Nederlands of Buitenlands)
* Nederlandse Identiteitskaart

Let op: Het rijbewijs is dus geen geldig identiteitsbewijs bij indiensttreding, omdat de nationaliteit moet kunnen worden vastgesteld.

Voor het controleren en kopiëren van bovenstaande identiteitsbewijzen gelden de volgende tips en richtlijnen:

* Neem geen genoegen met een door de sollicitant zelf gemaakte kopie, maar vraag altijd om het origineel en maak zelf een kopie (dit bent u verplicht ingevolge de WID).
* Zorg dat er een goed leesbare kopie wordt gemaakt. Let er vooral op dat de pasfoto op de kopie nog herkenbaar is. Kopieer van een paspoort de relevante bladzijden en kopieer van een identiteitskaart altijd beide kanten.
* Bekijk of het identiteitsbewijs nog geldig is. Indien de geldigheidsduur van het identiteitsbewijs is verstreken, dan is het document geen identiteitsbewijs meer in de zin van de WID.
* Wees kritisch en zorgvuldig bij het bekijken van het document in verband met valse en vervalste documenten die in omloop zijn. Let hierbij onder andere op de volgende punten:
  + Komt de foto op het document overeen met de aanbieder.
  + Komt de leeftijd in het document overeen met de aanbieder.
  + Komt de lengte in het document overeen met de aanbieder (zorg voor een referentiemaat, bij voorbeeld uw eigen lengte).
  + Kijk of het document er netjes en onbeschadigd uit ziet. Let vooral op het gebied rondom de foto.

Lees de op het identiteitsbewijs vermelde identiteitsgegevens. Controleer of de naam, (familienamen, voornamen), het adres, de geboortedatum, de geboorteplaats, het geslacht en het Burgerservicenummer (BSN) overeenkomen met de gegevens op het sollicitatieformulier/brief.

### Diploma’s/ Certificaten/ Cijferlijsten/ CV

Bij het merendeel van de functies binnen de gemeente wordt een bepaald opleidingsniveau als eis gesteld. Er zijn verschillende manieren om vast te stellen of de kandidaat voldoet aan het vereiste niveau en of de kandidaat geschikt is voor de functie:

* Door middel van een 'assessment' kan onder ander het intellectuele werk- en denkniveau van de kandidaat en daarmee zijn of haar geschiktheid voor de functie worden vastgesteld.
* Daarnaast kan worden vastgesteld of de kandidaat bepaalde opleidingen met goed gevolg heeft afgesloten. Diploma's, cijferlijsten, certificaten en dergelijke dienen daarbij als schriftelijk bewijs. Nog meer dan bij een identificatiebewijs is het tegenwoordig mogelijk diploma's, cijferlijsten en certificaten na te maken of te manipuleren. Veel mensen beschikken over computers, scanners en kleurenprinters waarmee gemakkelijk documenten zijn te vervaardigen die bedrieglijk echt lijken. De meest eenvoudige manier van vervalsen is het scannen of kopiëren van een origineel document en het daarop aanbrengen van de gewenste veranderingen (zoals voor- of familienamen en de geboortedatum). Ook het opwaarderen van cijfers op cijferlijsten komt voor (als iemand voor een bepaalde opleiding zakt dan krijgt hij meestal wel een cijferlijst).

Een veel gebruikte techniek voor het verhullen van een minder geslaagde werkervaring (vooral als er sprake is geweest van ontslag in de proeftijd) is het in het CV 'oprekken' van de werkervaring van een voorgaande werkgever en het ‘naar voren halen' van de datum indiensttreding van de volgende werkgever. Door goed opletten en vergelijken kunnen deze praktijken wellicht worden ontdekt.

Wat kunt u er aan doen om een redelijke zekerheid te hebben dat de getoonde documenten echt zijn? Hieronder een paar tips:

* + Vraag en bekijk altijd originele diploma’s en cijferlijsten en neem geen genoegen met door de kandidaat zelf gemaakte kopieën. Het komt in de praktijk wel eens voor dat originele documenten niet kunnen worden overlegd omdat ze bij voorbeeld 'bij een brand verloren zijn gegaan'. Bedenk dat bijna elke opleidingsinstantie in dergelijke gevallen een gewaarmerkte kopie van het document zal verstrekken.  
    Maak altijd zelf een kopie van de getoonde documenten.
  + Bekijk de afgiftedatum van een document en vergelijk deze met de door de sollicitant op het sollicitatieformulier opgegeven opleidingsperiode.
  + Controleer bij twijfel of de genoemde onderwijsinstelling bestaat (of bestaan heeft in de periode dat het document is verstrekt). Dit geldt met name bij Universitaire- of HBO-opleidingen.
  + Controleer of de naam en de geboortedatum overeenstemmen met die op het sollicitatieformulier/ CV of op een geldig identiteitsbewijs.
  + Controleer of de cijferlijst wel bij het diploma hoort dat wordt overlegd.
  + Vreemde fluctuaties in cijfers (bijvoorbeeld een zeer hoog cijfer voor de ene vreemde taal maar een zeer laag cijfer een andere vreemde taal) zouden kunnen vragen om een nadere uitleg van de sollicitant (een 3 is vrij eenvoudig in een 8 te veranderen, een 5 in een 6 en een 4 in een 9).
  + Indien op de cijferlijst 'vreemde' afkortingen voorkomen van geëxamineerde vakken, vraag dan aan de sollicitant waar deze voor staan (ook al weet je het zelf). Het zou vreemd zijn als de sollicitant zelf niet zou weten waarin hij examen heeft gedaan.

### Ontslagbrieven en getuigschriften

Naast het opleidingsniveau is ook het arbeidsverleden en de daarbij opgedane ervaring van de sollicitant van belang. Hoewel ervaring deels vast te stellen is door middel van een 'assessment' is een daadwerkelijke check van het arbeidsverleden een nuttige aanvulling. Een pre-employment check kan op verschillende manieren.

Zo kunnen (met toestemming van de sollicitant) referenties worden nagetrokken of kan schriftelijk geïnformeerd worden bij de personeelsafdeling van een eerdere werkgever om vast te stellen of de sollicitant daadwerkelijk bij het bedrijf in dienst is geweest gedurende de opgegeven periode. Aanvullend hierop kan aan een sollicitant gevraagd worden om getuigschriften of ontslagbrieven mee te nemen bij een gesprek.

Hieronder een aantal tips m.b.t. de controle van getuigschriften en dergelijke:

* Vraag en bekijk altijd originele documenten. Maak altijd zelf een kopie van de getoonde documenten.
* Bekijk de in het getuigschrift/ontslagdocument genoemde periode van dienstverband. Vergelijk deze met de door de sollicitant op het CV opgegeven periode. Let vooral ook op de afgiftedatum van het document ten opzichte van de datum 'uitdiensttreding'. Het is met name verdacht als het document een maand of meer voor de opgegeven ontslagdatum is afgegeven.
* Let op lacunes in het arbeidsverleden en vraag wat de betrokkene in die periode heeft gedaan.
* De inhoud, of beter de toon, van een getuigschrift kan een reden zijn om eens bij de vorige werkgever te informeren (toestemming van de sollicitant is daarvoor wel vereist).
* Controleer of het getuigschrift op briefpapier van het betreffende bedrijf is gemaakt. Let daarbij met name op het Kamer van Koophandel (KvK)-nummer dat in bijna alle externe correspondentie ergens op de brief vermeld zal staan. Indien het een niet zo bekend bedrijf is dan kan later aan de hand van dit nummer KVK informatie worden opgevraagd.
* Controleer of de in het document vermelde naam en eventueel de geboortedatum overeenstemmen met de door de sollicitant verstrekte informatie. Let er ook op of de in het document genoemde functienaam en omschrijving kloppen met de informatie op het CV.

### Referenties

Het inwinnen van referenties kan een belangrijk screeningsinstrument zijn. Volgens de meeste sollicitatiecodes[[6]](#footnote-7) mag slechts informatie worden ingewonnen in de eindfase van de procedure, met andere woorden als de keuze al bijna bepaald is. Vraag in ieder geval aan iedere sollicitant, ook bij interne sollicitaties, nadrukkelijk toestemming om informatie te mogen inwinnen bij de opgegeven vorige werkgevers, scholen of andere opleidingsinstituten. Een weigering van een sollicitant om toestemming te geven kan een reden zijn om de betreffende sollicitant maar niet verder in het sollicitatieproces mee te nemen, tenzij de weigering betrekking heeft op het opvragen van referenties bij de huidige werkgever. Vaak is de huidige werkgever niet op de hoogte van de sollicitatie.

Belangrijk is om kritisch te zijn op de functie van de als referenties opgegeven personen en hun relatie met de kandidaat. Zo is het bijvoorbeeld van belang dat zoveel mogelijk de laatste werkgever van de kandidaat als referentie wordt opgegeven. Daarnaast is het van belang om de kandidaat te vragen op basis van welke criteria hij is gekomen tot zijn referenties. Zorg ervoor dat er – zo mogelijk - meer dan één referentie wordt opgegeven.

Als referenties telefonisch worden benaderd is het van belang dat er een functieomschrijving en een CV binnen handbereik liggen, en ook eventuele opmerkingen die de sollicitant tijdens het sollicitatiegesprek over de referentie zelf heeft gemaakt.

Neem voor het gesprek ruim de tijd. Het gesprek heeft bij voorkeur het karakter van een combinatie van een ongestructureerd interview met veel open vragen waarbij men de referentie laat praten en een gestructureerd interview waarbij van tevoren wordt bedacht op welke vragen men tenminste een antwoord zou willen hebben. Belangrijke vragen tijdens een gesprek met een referentie zijn:

* Wat is uw naam en positie binnen de organisatie?
* Wat is uw relatie met de kandidaat, hoe lang kent u de kandidaat?
* Van wanneer tot wanneer was de kandidaat bij u werkzaam?
* Wat was zijn functie?
* Wat hield deze functie in (taken, verantwoordelijkheden en bevoegdheden)?
* Hoe heeft de kandidaat in deze functie(s) gefunctioneerd?
* Wat zijn kenmerkende persoonlijke eigenschappen van de kandidaat?
* Werkte de kandidaat in een team? Hoe verliep de omvang met collega’s?
* Zijn er ooit problemen geweest die betrekking hadden op de integriteit van de kandidaat (met collega’s, bedrijfsmiddelen, klanten et cetera)?
* Zou u met uw huidige kennis de kandidaat opnieuw aannemen?

### Referentieformulier

Het is ook mogelijk referenties te vragen schriftelijk vragen te beantwoorden over de kandidaat. Het ondertekende en teruggezonden formulier kan bijvoorbeeld worden opgenomen in het personeelsdossier. Het is niet verstandig het referentieformulier aan de sollicitant zelf mee te geven, maar rechtstreeks te verzenden naar het (werk)adres van de referentie. Daar waar referenties wellicht mondeling nog wel de waarheid enigszins willen ’aanpassen’, zal hiertoe wellicht schriftelijk minder snel toe worden overgegaan, zeker als op het formulier wordt aangegeven dat dit in het personeelsdossier wordt bewaard.

### Interne informatie

Bij interne sollicitaties – bijvoorbeeld bij een overstap van de ene dienst naar een andere – is er een personeelsdossier aanwezig. Ook als een sollicitant eerder bij de gemeente heeft gewerkt, daarna bijvoorbeeld in het bedrijfsleven, en nu weer solliciteert bij de gemeente is, afhankelijk van de bewaartermijn van het personeelsdossier, nog een personeelsdossier opgeslagen in het archief. In het kader van screening is het natuurlijk zinvol om die informatie te achterhalen die binnen de gemeentelijke organisatie al voorhanden is.

Bij sollicitanten die voorheen al eens bij de gemeente hebben gewerkt is het bijvoorbeeld belangrijk te weten op welke wijze de ambtenaar destijds de gemeente heeft verlaten. Als dit is vanwege een strafontslag als gevolg van een integriteitschending, zeker als deze schending raakvlakken heeft met de functie waarop de sollicitant thans solliciteert, is dit een aspect dat niet genegeerd mag worden.

Bij interne sollicitaties is het de praktijk dat bij binnengemeentelijke sollicitaties in het algemeen de personeelsdossiers niet mee overgaan naar een nieuwe dienst of stadsdeel. Er kan wel een verzoek worden gedaan om het personeelsdossier te verkrijgen, maar in dat geval wordt niet meer dan het aanstellingsbesluit en overige vaste gegevens (voor wat betreft salaris en pensioen) toegezonden. Beoordelingen en bijvoorbeeld vastgelegde disciplinaire maatregelen gaan niet mee over, terwijl dit voor de ontvangende dienst of stadsdeel wel relevante informatie kan zijn. De ontvangende dienst krijgt derhalve een ‘blanco’ ambtenaar, terwijl bij de vorige dienst of stadsdeel van de gemeente er een personeelsdossier voorhanden is/was.

Voor nu geldt dat het verstandig is alvorens de interne sollicitant definitief aan te nemen om referenties in te winnen bij de dienst of het stadsdeel waar de sollicitant tot dan toe werkt. Overigens geldt ook hier de eerder genoemde sollicitatiecode en mag dit laatste dus slechts met toestemming van de interne sollicitant.

### Verklaring Omtrent het Gedrag (VOG)

Op dit moment hoeft volgens de rechtspositieregeling een VOG alleen te worden overgelegd bij de aanstelling.

Het Centraal Orgaan Verklaring Omtrent het Gedrag (COVOG) onderdeel van de Dienst Justis van het Ministerie van Veiligheid en Justitie is belast met de afhandeling van de VOG. Zij hebben een aantal vaste groepen aanvragers benoemd aan de hand van een aantal herkenbare, specifieke criteria van bijvoorbeeld een branchegroep. Hierbij kan bijvoorbeeld gedacht worden aan taxichauffeurs, onderwijs en Bijzonder Opsporing Ambtenaren (BOA). Voor de functies die niet in dergelijke vaste groepen onder te brengen zijn, is een speciaal aanvraagformulier ontwikkeld. Op dit formulier moet worden aangegeven wat de specifiek aan de functies verbonden risico’s zijn. Ook moet een functietypering worden bijgevoegd. Daarnaast kunnen specifiek aan de werkzaamheden verbonden omstandigheden worden vermeld, bijvoorbeeld of de medewerker veel solistisch handelt of onder zware politieke en of tijdsdruk zal moeten opereren.

Afhankelijk van de functie en de daarbij aangegeven risico’s raadpleegt het COVOG de diverse bestanden van politie en justitie. De risicocategorieën corresponderen met delicten en wetsovertredingen. Aan de hand van de beschikbare gegevens wordt een afweging gemaakt, indien nodig worden meer gegevens opgevraagd, bijvoorbeeld bij de Reclassering. Over het algemeen zijn alleen gegevens uit Nederland bekend. Wanneer een sollicitant slechts een half jaar in Nederland woonachtig is, kan alleen naar deze periode gekeken worden. Met sommige Europese landen worden wel gegevens uitgewisseld, maar dat geldt maar voor een klein aantal landen.

Bij de afweging wordt door het COVOG gekeken naar de relevante zaken op het strafblad en de openstaande zaken, maar ook naar de gehanteerde strafmaat. Ook wordt gekeken naar de antecedenten die niet direct iets te maken hebben met de functie die de persoon gaat vervullen.

Dit alles wordt gelegd naast de functie die de betrokkenen zal gaan vervullen en de omstandigheden waaronder hij dit gaat doen (solistisch, tijdsdruk, et cetera). Bij de afweging wordt vooral gekeken naar feiten en veroordelingen. Openstaande zaken kunnen van doorslaggevende betekenis zijn, maar zullen als er alleen sprake is van een openstaande zaak, zelden leiden tot een afwijzing. Ook is een niet te onderbouwen vermoeden onvoldoende om een aanvraag af te kunnen wijzen.

Indien het COVOG voornemens is om de aanvraag af te wijzen, wordt de betrokkene uitgenodigd voor een zienswijze gesprek waarin de aanvrager zijn kant van de zaak voor het voetlicht kan brengen.

### Uitzendkrachten

Ook voor uitzendkrachten kan een VOG worden aangevraagd. Het aanvraagformulier moet dan door de inlenende organisatie, in dit geval de gemeente, worden ingevuld. Gelet op het feit dat uit onderzoek blijkt dat integriteitschendingen vaak begaan worden door uitzendkrachten of dat zij hierbij betrokken zijn, is dit een belangrijke wijziging ten opzichte van de huidige situatie. Vooral bij kwetsbare functies die tijdelijk door een uitzendkracht worden ingevuld, is het aanbevolen om een VOG aan te vragen. Wanneer een uitzendkracht slechts een korte periode – bijvoorbeeld een paar dagen - bij de gemeente komt werken, is het aanvragen van een VOG uiteraard praktisch niet haalbaar.

Bij uitzendbureaus ligt de prioriteit in het algemeen bij het uitzenden van gekwalificeerd personeel (voldoen aan de functie-eisen), waarbij de integriteit van de uitzendkracht vaak niet aan de orde komt. Het uitzendbureau dient er voor te zorgen dat zij alleen uitzendkrachten aan de gemeente uitleent waarover geen twijfel bestaat ten aanzien van hun integriteit. Het uitzendbureau dient hiervoor bijvoorbeeld minimaal één referentie na te trekken. Belangrijk is voorts dat het uitzendbureau ervoor waakt dat uitzendkrachten die door de gemeente als ‘ongewenst’ zijn bestempeld, niet opnieuw binnen de gemeente worden aangeboden. Voorts zullen de uitzendkrachten een zogenaamde integriteits- of geheimhoudingsverklaring moeten ondertekenen.[[7]](#footnote-8)

Bovenstaande maatregelen bieden meer houvast ten aanzien van de achtergrond van uitzendkrachten. De gemeente zal zelf ook steeds alert moeten blijven en heeft er met de mogelijkheid tot het aanvragen van een VOG voor uitzendkrachten in de nabije toekomst in ieder geval een screeningsinstrument erbij.



Nassaulaan 12

2514 JS Den Haag

CERT: 070 204 55 11 (9:00 – 17:00 ma – vr)

CERT 24x7: Piketnummer (instructies via voicemail)

[info@IBDGemeenten.nl](mailto:info@IBDGemeenten.nl) / [incident@IBDGemeenten.nl](mailto:incident@IBDGemeenten.nl)

Kijk voor meer informatie op:

www.informatiebeveiligingsdienst.nl

1. Zie: <https://www.aivd.nl/onderwerpen/veiligheidsonderzoeken/voor-de-werknemer/veiligheidsonderzoek-wat-houdt-een-vgb-in> [↑](#footnote-ref-2)
2. Meer informatie over het aanwijzen van vertrouwensfuncties: <https://www.aivd.nl/onderwerpen/veiligheidsonderzoeken/voor-de-werknemer/vertrouwensfunctie-wat-is-dat> [↑](#footnote-ref-3)
3. BWT staat voor Bouw- Woningtoezicht. [↑](#footnote-ref-4)
4. <https://justis.nl/producten/vog/index.aspx> [↑](#footnote-ref-5)
5. http://www.justis.nl/producten/vog/ [↑](#footnote-ref-6)
6. Basisregels voor sollicitaties [↑](#footnote-ref-7)
7. Zie hiervoor het operationele product ‘[Geheimhoudingsverklaring](https://www.informatiebeveiligingsdienst.nl/product/geheimhoudingsverklaringen/)’ [↑](#footnote-ref-8)