

Handreiking

Personeelsbeleid gemeente

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

Colofon

### Naam document

Handreiking Personeelsbeleid gemeente

### Versienummer

2.1.3

### Versiedatum

Mei 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 | 26 augustus 2014 | Eerste versie |
| 1.02 | 19 augustus 2016 | Links naar andere BIG OP producten met meer info toegevoegd, typefouten aangepast. Internet Links aangepast |
| 2.0 | Februari 2019 | BIO update |
| 2.1 | Juli 2019 | Verwijzingen aangepast en kleine aanpassingen in lay-out |
| 2.1.1 | Augustus 2019 | Dode links hersteld |
| 2.1.2 | Februari 2020 | BIO 1.04 aanpassingen uit control 7.1.1 en onderliggende maatregelen verwerkt |
| 2.1.3 | Mei 2020 | Aanpassingen naar aanleiding van de Wet normalisering rechtspositie ambtenaren |

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 beschrijven van alle aan personen (medewerkers, contractanten en inhuur) gerelateerde informatiebeveiligingsaspecten die voor de gemeente relevant zijn in het kader van de BIO.

**Doelgroep**

Dit document is van belang voor de CISO, het management van de gemeente en de afdeling Human Resource (HR) / Personeel en Organisatie (P&O).

**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.

7.2.1 Directieverantwoordelijkheden.

7.2.2 Bewustzijn, opleiding en training ten aanzien van informatiebeveiliging.

7.2.3 Disciplinaire procedure.

7.3.1 Beëindiging of wijziging van verantwoordelijkheden van het dienstverband.

8.1.4 Teruggeven van bedrijfsmiddelen.

9.2.6 Toegangsrechten intrekken of aanpassen.

### 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.

# Managementsamenvatting

Het aspect van menselijk gedrag is een belangrijke factor voor informatieveiligheid. De gemeente kan organisatorische, fysieke en technische beheersmaatregelen treffen, maar willen deze doeltreffend zijn dan moeten medewerkers deze beheersmaatregelen kunnen en willen uitvoeren, zodat de kans dat medewerkers bewust of onbewust maatregelen omzeilen wordt verkleind. Door geen oog te hebben voor de factor mens is de kans groot dat onveiligheid toeneemt en daarmee ook de risico’s voor de gemeente toenemen. Daarom is het belangrijk dat door de hele HR-cyclus hier aandacht voor is.

Voordat de werving en selectie plaatsvindt is het belangrijk om inzichtelijk te hebben wat het belang van de functie is. Het belang van de functie bepaald of er vanuit de informatiebeveiliging bijzondere aandachtspunten zijn waarmee rekeninghouden moet worden. Bij de werving en selectie dient hier rekening mee gehouden te worden en passende instrumenten te worden ingezet, zoals screening. Bij de indiensttreding is het van belang dat de medewerker wordt gewezen op het geldende beleid en wat van de persoon verwacht wordt. De medewerker krijgt immers toegang tot vertrouwelijke informatie(systemen), krijgt bedrijfsmiddelen waarmee hij mag werken en krijgt toegang tot mogelijk bijzondere ruimtes van de gemeente.

Gedurende de loopbaan van de medewerker dient er aandacht te blijven voor dit onderwerp en dient de medewerker continu te werken aan het informatiebeveiligingsbewustzijn. De rol van het management is hierin cruciaal. Het management is verantwoordelijk dat de medewerkers zich voldoende bewust zijn van wat van hen verwacht wordt rondom het thema informatiebeveiliging.

Indien medewerkers zich (on)opzettelijk niet houden aan het (beveiligings)beleid, wat risico’s met zich kan brengen voor de burgers, de gemeente en ketenpartners van de gemeente, is het belangrijk dat hierop wordt geacteerd. Afhankelijk van de ernst en de context kunnen disciplinaire maatregelen opgelegd worden.

Tot slot is het voor de gemeente belangrijk dat wanneer de medewerker uit dienst gaat, de bedrijfsmiddelen en informatie worden ingeleverd en de medewerker zich houdt aan de afspraken, waaronder de nog steeds geldende geheimhoudingsplicht.

Het is belangrijk dat hier beleid en processen voor zijn ingericht. Voorliggend document ondersteunt de gemeente om dit op te zetten, te implementeren en na te leven.

Inhoudsopgave

[Managementsamenvatting 5](#_Toc40343285)

[1. Inleiding 7](#_Toc40343286)

[1.1. Positie ambtenaren 7](#_Toc40343287)

[1.2. Het belang van personele beveiliging 8](#_Toc40343288)

[1.3. Verantwoordelijken voor het Personeelsbeleid 8](#_Toc40343289)

[2. Beveiligingseisen ten aanzien van personeel 9](#_Toc40343290)

[2.1. Screening bij het aannemen van personeel 10](#_Toc40343291)

[2.2. De introductiemap nieuwe medewerkers 13](#_Toc40343292)

[2.3. Arbeidsovereenkomst en reglementen 13](#_Toc40343293)

[2.4. Functies 15](#_Toc40343294)

[2.5. Verantwoordelijkheden 16](#_Toc40343295)

[2.6. Bewustwording, opleiding en training 17](#_Toc40343296)

[2.7. Monitoren 19](#_Toc40343297)

[2.8. Afhandeling beveiligingsincidenten 19](#_Toc40343298)

[2.9. Disciplinaire maatregelen 20](#_Toc40343299)

[2.10. Uitdiensttreding en wijziging van de aanstelling/dienstverband 21](#_Toc40343300)

[Bijlage 1: Voorbeeld checklist bij indiensttreding 23](#_Toc40343301)

[Bijlage 2: Voorbeeld checklist bij uitdiensttreding 25](#_Toc40343302)

[Bijlage 3: Voorbeeld Disciplinaire straffen 27](#_Toc40343303)

[Bijlage 4: Literatuur/bronnen 29](#_Toc40343304)

# Inleiding

Dit product bevat aanwijzingen rondom de beveiligingseisen ten aanzien van personeel binnen de gemeente die in het personeelsbeleid geborgd dienen te worden. De doelstelling is het bewerkstelligen dat werknemers, ingehuurd personeel en externe gebruikers hun verantwoordelijkheden begrijpen, geschikt zijn voor de rol die ze vervullen of gaan vervullen en om het risico van diefstal, fraude of misbruik van faciliteiten te verminderen.

In de BIO worden eisen benoemd met betrekking tot personele beveiligingseisen, deze staan benoemd in hoofdstuk 7. Deze beveiligingseisen dienen in het informatiebeveiligingsbeleid van de gemeente aan bod te komen. Dit document beschrijft alle aan personen (medewerkers, contractanten en inhuur) gerelateerde informatiebeveiligingsaspecten die voor de gemeente relevant zijn in het kader van de BIO en in het informatiebeveiligingsbeleid opgenomen dienen te worden.

## Positie ambtenaren

Met in werking treding van de Wet normalisering rechtspositie ambtenaren (WNRA) begin 2020 is er het een en ander verandert in de rechtspositie van de ambtenaar[[1]](#footnote-1). Ambtenaren krijgen bijvoorbeeld een tweezijdige arbeidsovereenkomst en worden dan niet meer eenzijdig aangesteld. Daarnaast blijft de speciale status van ambtenaren, wat betekent dat speciale regels voor ambtenaren niet verdwijnen, zoals de geheimhoudingsplicht, verbod om giften aan te nemen en de plicht andere functies te melden.[[2]](#footnote-2) De arbeidsvoorwaarden voor gemeenteambtenaren zijn vastgelegd in de collectieve arbeidsvoorwaardenregeling (CAR). De uitwerkingsovereenkomst (UWO) geeft een uitwerking van de hoofdlijnen in de CAR en regelt een aantal secundaire arbeidsvoorwaarden.[[3]](#footnote-3)

Gemeenten maken ook steeds meer de overstap van een gedetailleerde functiebeschrijving met deeltaken en verantwoordelijkheden naar een systeem met een algemene functiebeschrijving van taakgebieden. Dit sluit aan bij de wens van gemeentelijke werkgevers en werknemersorganisaties om sectoraal meer eenduidigheid te brengen in de wijze van functiebeschrijvingen en –waarderingen. De Vereniging van Nederlandse Gemeenten (VNG) heeft in 2011 opdracht gegeven om het systeem HR21 te ontwikkelen.[[4]](#footnote-4)

## Het belang van personele beveiliging

Mensen maken fouten, bewust of onbewust. Daardoor kan de goede afloop van informatieprocessen negatief worden beïnvloed en kan de organisatie (de gemeente) schade oplopen. Om de kans op bewuste fouten te verkleinen dient de betrouwbaarheid van personeel bij aanname te worden getoetst, dienen bepalingen in de arbeidsovereenkomst of in (aanvullende) verklaringen/regelingente worden opgenomen die door de ambtenaren moeten worden ondertekend en dient het vertrek van personeel zorgvuldig te worden begeleid. Om medewerkers te helpen onbewuste fouten zoveel als mogelijk te voorkomen, of de schade die hieruit volgt te beperken, dienen zij getraind te worden in de beveiligingsmaatregelen en dient er een duidelijke procedure aanwezig te zijn zodat beveiligingsincidenten kunnen worden gemeld.

## Verantwoordelijken voor het Personeelsbeleid

Het gedrag van medewerkers is de achilleshiel van het informatiebeveiligingsbeleid. Zonder de bereidheid en discipline van de medewerkers om zich aan het beleid te houden, is elk informatiebeveiligingsbeleid zinloos.

Medewerkers moeten zich bewust zijn van beveiligingsrisico’s van de informatie waarmee ze werken en moeten actief handelen om deze risico’s te verminderen. Om dit gedrag te bewerkstelligen, moet een groot aantal instrumenten in samenhang worden ingezet. Te denken valt aan screening, ambtseden, opname in functiebeschrijvingen en bespreking tijdens functionerings- en beoordelingsgesprekken, interne communicatie en voorlichting en uiteindelijk disciplinaire maatregelen. Al deze instrumenten dienen in samenhang te worden ingezet, geëvalueerd en aangepast.[[5]](#footnote-5)

De afdeling Human Resources (HR) / Personeel en Organisatie (P&O) moet namens het verantwoordelijke management de taak krijgen om beveiliging structureel onderdeel te maken van het arbeidsrechtelijke traject (functionering, beoordeling, eed/belofte, screening, disciplinaire maatregelen). De Chief Information Security Officer (CISO) dient betrokken te worden om de samenhang van het gehele pakket, van beleid tot uitvoering, op het gebied van informatiebeveiliging te bewaken.

# Beveiligingseisen ten aanzien van personeel

Medewerkers moeten zich bewust zijn van beveiligingsrisico’s van de informatie waarmee ze werken en moeten actief handelen om deze risico’s te verminderen. Om dit gedrag te bewerkstelligen, moet een groot aantal instrumenten in samenhang worden ingezet. Deze instrumenten kunnen op verschillende stadia van het dienstverband worden ingezet (vooraf, tijdens en na).

### Voorafgaand aan het dienstverband

Zorg dat medewerkers, ingehuurd personeel en externe gebruikers hun verantwoordelijkheden begrijpen, en geschikt zijn voor de functies waarvoor zij worden overwogen, en om het risico van diefstal, fraude of misbruik van faciliteiten te verminderen. Denk hierbij aan:

* Screening bij het aannemen van personeel;
* Arbeidsovereenkomst en reglementen;
* Functies en verantwoordelijkheden.

### Tijdens het dienstverband

Zorg dat medewerkers, ingehuurd personeel en externe gebruikers zich bewust zijn van bedreigingen en gevaren voor informatiebeveiliging, van hun verantwoordelijkheid en aansprakelijkheid, en dat ze zijn toegerust om het beveiligingsbeleid van de organisatie in hun dagelijkse werkzaamheden te ondersteunen, en het risico van een menselijke fout te verminderen. Denk hierbij aan:

* [Bewustwording, opleiding en training voor informatiebeveiliging](http://fortisnet.nl.fortis.bank/apv_cfo/applicaties/voorschriften/asp/voorschrift.asp?wrk=139);
* Monitoren;
* Melden van beveiligingsincidenten;
* Registratie van uitgegeven bedrijfsmiddelen en verleende toegangsrechten;
* [Disciplinaire maatregelen](http://fortisnet.nl.fortis.bank/apv_cfo/applicaties/voorschriften/asp/voorschrift.asp?wrk=140).

Wanneer een medewerker van functie wisselt, is het belangrijk om hierbij te onderzoeken of dit andere en wellicht hogere beveiligingseisen gaat stellen aan de medewerker. Mogelijk voordat de functie wordt bekleed een zekere vorm van screening worden uitgevoerd (waaronder het overleggen van een VOG als de functie genoemd wordt in het screeningsbeleid) en moet de medewerker aanvullend getraind worden voor bewustwording. Het kan ook zijn dat er conflicterende rollen/taken bij één medewerker terechtkomen.

### Beëindiging of wijziging van dienstverband

Zorg dat medewerkers, ingehuurd personeel en externe gebruikers ordelijk de organisatie verlaten of hun dienstverband wijzigen. Denk hierbij aan:

* Retourneren van bedrijfsmiddelen;
* Verwijderen van toegangsrechten.

## Screening bij het aannemen van personeel

Het doel van screenen[[6]](#footnote-6) van personeel is het verkleinen van integriteits- en beveiligingsrisico’s bij na de start van het dienstverband van de ambtenaren en het in dienst nemen van overig personeel.[[7]](#footnote-7) Door een objectieve vaststelling of bevestiging van het (werk)verleden van de betrokkene worden aanwijzingen verkregen betreffende de moraliteit en de reputatie van de betrokkene.

Alle screeningsactiviteiten die worden uitgevoerd zijn vervat in procedures die eisen en grenzen stellen aan de controles.

Hierbij is vastgelegd wie verantwoordelijk is voor de screening van personeel en hoe, wanneer en waarom de screening wordt uitgevoerd. De screeningsactiviteiten dienen rekening te houden met privacy, persoonlijke gegevens en arbeidsrechtelijke wetgeving.

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 een functiewijziging.

In het operationele product ‘Handleiding screening personeel’ van de Baseline Informatiebeveiliging Overheid (BIO) wordt met de volgende indeling van functies gewerkt:

* Vertrouwensfuncties
Vertrouwensfuncties zijn functies als bedoeld in de Wet veiligheidsonderzoeken (WVO)[[8]](#footnote-8). Dit zijn functies waarin de mogelijkheid bestaat om 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. Als een functie wordt aangewezen als vertrouwensfunctie voert de AIVD een zogenaamd veiligheidsonderzoek uit om vast te stellen of de kandidaat de verplichtingen in deze functie onder alle omstandigheden loyaal vervult. Is er niet of nauwelijks sprake van een risico, dan ontvangt de kandidaat-vertrouwensfunctionaris een schriftelijke verklaring van geen bezwaar.
* Kwetsbare functies
Kwetsbare functies hebben vooral te maken met het aspect integriteit en daarvoor zijn verschillende factoren in kaart gebracht welk in het operationele product ‘Handleiding screening personeel’ opgesomd zijn.[[9]](#footnote-9) Met behulp deze opsomming van risicofactoren kan elke organisatie zelf beoordelen welke factoren voorkomen in welke functies, en daardoor welke functies te kwalificeren zijn als kwetsbare functies voor die specifieke dienst of dat specifieke stads- of gemeentedeel. 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.
* Algemene functies
De algemene functies vormen de restgroep. Dat wil niet zeggen dat integriteit in deze functies geen rol speelt. Ook bij de algemene functies is een goede screening en het informatiebeveiligingsaspect van belang.

Het operationele product ‘Handreiking screening personeel’ geeft een beeld van (grote of meerdere) risico’s die aan sommige functies zijn verbonden. Hiermee kan een organisatie zelf bepalen of zulke functies aanwezig zijn, en hier bij het screenen rekening mee houden.

In alle functies geldt overigens, of er nu al dan niet risicofactoren aanwezig zijn, dat er zowel van ambtenaren, als overheidsdienaren verwacht mag worden dat zij integer handelen, maar ook dat zij de geheimhoudingsplicht in acht nemen. Daarmee wordt gedoeld op een algemene professionele verantwoordelijkheid van de ambtenaar op zijn vakgebied.

Voordat er geworven kan worden voor een functie moeten de integriteit- en de veiligheidsrisico’s van die functie in kaart zijn gebracht, welke vervolgens meegenomen moeten worden in de sollicitatieprocedure. De sollicitatieprocedure biedt een aantal screeningsinstrumenten, zoals:

* Het sollicitatiegesprek
Het sollicitatiegesprek is de manier om de sollicitant in persoon te ontmoeten en middels interactie antwoorden te krijgen op allerhande vragen. Tijdens het gesprek kan onderzocht worden of de sollicitant weet en begrijpt wat er verwacht wordt met betrekking tot integriteit en geheimhouding.
* Identificatie
De identificatie is verplicht in het kader van de Wet op de Identificatieplicht (Wid)[[10]](#footnote-10). Bijvoorbeeld via het Paspoort of Identiteitskaart.[[11]](#footnote-11)
* Diploma’s/ Certificaten / Cijferlijsten / Curriculum Vitae
De sollicitant heeft verschillende manieren om aan te tonen of zijn kennis en kunde in overeenstemming is met de functie eisen. Vraag naar originelen van diploma’s en kwalificaties. Controleer het verhaal op volledigheid en consistentie. Laat eventuele tegenstrijdigheden toelichten. Controleer bij (twijfel) de universiteiten en opleidingsinstellingen of de persoon wel afgestudeerd is, dan wel de genoemde kwalificaties heeft ontvangen.
* Ontslagbrieven, getuigschriften
Ontslagbrieven en getuigschriften geven een direct beeld over het werkverleden van de sollicitant.
* Referenties
Dit zijn schriftelijke stukken die het functioneren van betrokkene beschrijven en die geschreven zijn door de leidinggevenden in vorige functies. Normaliter worden de referenties telefonisch gecontroleerd op authenticiteit.

* Verklaring Omtrent het Gedrag (VOG)
De organisatie moet een screeningsbeleid hebben waarin uitgewerkt is voor welke functies een VOG verplicht is. Als mensen tewerkgesteld worden op een functie of rol uit het screeningsbeleid dan moeten zijn een VOG overleggen bij aanvang van de werkzaamheden. (verplichte maatregelen uit de BIO). De Verklaring Omtrent het Gedrag (VOG) is een verklaring waaruit blijkt dat het gedrag van de werknemer in het verleden geen bezwaar vormt voor het vervullen van een specifieke taak of functie in de samenleving. De screeningsautoriteit Justis[[12]](#footnote-12) screent (rechts)personen die een VOG aanvragen en geeft de VOG af. Een VOG wordt afgegeven als er geen strafbaar feit is gepleegd dat relevant is voor de betreffende functie. Een VOG heeft geen einddatum, maar een VOG die langer dan een jaar geleden is afgegeven is niet langer geldig. De verklaring zelf zegt niets over de veroordelingen.
* Onderzoek financiële situatie
Onderzoek bij gevoelige functies naar de financiële situatie van een persoon met het oogmerk te bepalen in hoeverre een persoon in geldzorgen zit. De wijze waarop dit onderzoek gedaan wordt kan bestaan uit een directe navraag bij de betrokkene tot en met het raadplegen van financiële informatie bij derden. Bijvoorbeeld via handelsinformatiebureaus.[[13]](#footnote-13) Handelsinformatiebureaus maken onder meer gebruik van openbare bronnen/registers. Openbare registers zijn onder andere de Kamer van Koophandel[[14]](#footnote-14), het Kadaster[[15]](#footnote-15) en het Centraal Insolventieregister[[16]](#footnote-16). Houdt hierbij altijd rekening met de Uitvoeringswet Algemene Verordening Gegevensbescherming (UAVG)[[17]](#footnote-17) en breng de betrokkene van dit onderzoek altijd op de hoogte.

Zodra één van de controlepunten niet bevredigend of onvoldoende beantwoord is, kan men de persoon niet voor de gemeente laten werken. Er zijn dan immers redenen om aan de integriteit te twijfelen.

Een vergelijkbaar screeningsproces dient te worden uitgevoerd voor ingehuurd en tijdelijk personeel of als er via uitbesteding werkzaamheden voor de gemeente worden uitgevoerd. Denk hierbij ook aan stagiaires en afstudeerders. Indien dergelijke medewerkers via een uitzendorganisatie of een detacheringbureau worden ingehuurd, dient het contract met dit bureau duidelijk de verantwoordelijkheden van het bureau te specificeren ten aanzien van de screening en de meldingsprocedures die men volgt indien de screening niet voltooid is of de resultaten aanleiding geven tot twijfel of bezorgdheid.

Aandachtpunten bij screening van personeel zijn:

* Wees in alle gevallen zeker, dat alle informatie met betrekking tot de screening rechtmatig verkregen is.
* Weet ook dat de verkregen informatie een momentopname is. Ook hier geldt dat ‘resultaten’ uit het verleden niets zeggen over de toekomst.

## De introductiemap nieuwe medewerkers

In de introductiemap die als hardcopy, digitaal of via het intranet kan worden aangeboden dient naast de regels met betrekking tot het internetgebruik, instructies toegevoegd te worden hoe met privacygevoelige en vertrouwelijke informatie omgegaan moet worden, het omgaan met toegangspassen, omgaan met papieren gegevens, het gebruik van wachtwoorden[[18]](#footnote-18), het gebruik van mobiele gegevensdragers[[19]](#footnote-19), mobiele apparaten[[20]](#footnote-20) en telewerken[[21]](#footnote-21) en dergelijke. Deze regels worden bij voorkeur door de leidinggevende in het inwerktraject toegelicht. Zie ook bijlage 1 voor een voorbeeld van een checklist bij indiensttreding. Daarnaast moeten nieuwe medewerkers binnen 3 maanden een training i-bewustzijn te hebben gevolgd.

## Arbeidsovereenkomst en reglementen

Door de verantwoordelijkheden op het gebied van informatiebeveiliging in het arbeidscontract van werknemers, de arbeidsovereenkomst met externen en het personeelsreglement[[22]](#footnote-22) vast te leggen, worden enerzijds de verwachtingen duidelijk vastgelegd en anderzijds kan men bij eventuele incidenten terugvallen op deze overeenkomsten.Het maakt hierbij niet uit of men direct voor de gemeente werkt, via een uitzendorganisatie/detacheringbureau, of via uitbesteding. In het vervolg wordt zowel het arbeidscontract als de arbeidsovereenkomst aangeduid als contract.

Neem regels met betrekking tot ‘goed gedrag’ op in het contract dat de werkrelatie regelt. Onder ‘goed gedrag’ wordt onder andere verstaan het eerbiedigen van relevante wet- en regelgeving, maar ook de omgang met de middelen van de gemeente die ter beschikking gesteld zijn, de omgang met basisregistraties[[23]](#footnote-23),[[24]](#footnote-24) en het gebruik van informatiesystemen. Verder valt het signaleren van zwakke plekken in de verdediging onder dit gedrag (het ‘bewijzen’ van zwakke plekken is echter niet toegestaan).

Neem verder in het contract op dat het deze regels ten opzichte van ‘goed gedrag’ ook van kracht zijn buiten het terrein van de werkgever en buiten de kantoortijden, zodra een relatie met de gemeente herkenbaar is. Bijvoorbeeld internet, e-mail en sociaal mediagedrag.

Aandachtspunten met betrekking tot contracten:

* Eisen ten aanzien van informatiebeveiliging moeten in de functiebeschrijving opgenomen zijn. De diverse functies zijn beschreven, inclusief de gevoelige informatie waartoe men toegang heeft.
* Als er gebruik gemaakt wordt van een personeelsreglement maakt dit deel uit van het arbeidscontract. Hierin kunnen extra eisen ten aanzien van informatiebeveiliging zijn opgenomen.

Aandachtspunten met betrekking tot geheimhoudings- en een integriteitsverklaring:

* In contracten met werknemers moet een clausule opgenomen worden waarin geheimhoudingsplicht wordt benoemd en afspraken hierover worden gemaakt. Medewerkers moeten een geheimhoudingsverklaring met boetebeding (sancties)[[25]](#footnote-25) tekenen zolang er nog geen ambtseed is afgelegd.
* In contracten met externe bedrijven (bijvoorbeeld ICT-leveranciers, uitzend- en detacheringbureaus[[26]](#footnote-26)) moet een clausule opgenomen worden waarin geheimhoudingsplicht wordt benoemd en afspraken hierover worden gemaakt. Het gaat hierbij om een geheimhoudings- en een integriteitsverklaring met boetebeding (sancties).
* De geheimhoudings- en een integriteitsverklaring behoren individueel te zijn. Wanneer er sprake is van een collectief contract, dan moet daarin beschreven zijn, dat er aparte individuele geheimhoudingsverklaringen gebruikt worden.
* Maak duidelijk, dat de geheimhouding zowel tijdens de contractperiode als na afloop van het contract geldt.
* De geheimhoudings- en een integriteitsverklaring worden actueel gehouden door de Human Resource (HR) / Personeel en Organisatie (P&O)-adviseur en zijn in lijn met het informatiebeveiligingsbeleid.[[27]](#footnote-27)
* De direct leidinggevende is verantwoordelijk voor de controle op naleving van de afspraken die in de clausule met betrekking tot de geheimhoudingsplicht zijn opgenomen. De leidinggevende dient incidenten te bespreken met de betrokken medewerker en de mogelijke consequenties (disciplinaire maatregelen) kenbaar te maken.

Aandachtspunten met betrekking tot apparatuur en software in personeelsreglement:

* Beschrijf in het personeelsreglement het toegestane en het verboden gedrag van medewerkers met betrekking tot apparatuur en software die door het bedrijf ter beschikking gesteld zijn. Door dit op te nemen in het personeelsreglement, wordt het een onderdeel van het arbeidscontract. Bij medewerkers die niet onderworpen zijn aan het personeelsreglement geldt, dat de omgang met apparatuur en software in het contract opgenomen behoort te zijn.
* Beschrijf in het personeelsreglement het toegestane en het verboden gedrag van medewerkers op het internet, bij het interne en externe e-mailverkeer en bij het gebruik van sociale media, zoals LinkedIn, Facebook, Twitter of bijvoorbeeld Instagram. Door deze aandachtspunten op te nemen in het personeelsreglement, wordt het een onderdeel van het arbeidscontract. Bij medewerkers die niet onderworpen zijn aan het personeelsreglement geldt, dat bovenstaande aandachtspunten onderdeel van het contract behoren te zijn.

## Functies

Voor alle functies binnen de gemeente moet worden vastgesteld of het noodzakelijk is om – naast de reguliere richtlijnen en gedragscodes – een specifieke beschrijving van de bijbehorende taken, rechten en plichten van de medewerker ten aanzien van informatiebeveiliging op te nemen. Deze beschrijving dient ook een overzicht te bevatten van de informatiesystemen, privacygevoelige en vertrouwelijke informatie waartoe men toegang heeft op grond van de functie.[[28]](#footnote-28) Een mogelijk transitiepad kan als volgt worden ingevuld:

* Het opnemen van aanvullende beveiligingstaken in de functieomschrijving kan worden doorgevoerd bij iedere functieherziening, waarbij de functiebeschrijving moet worden aangepast.
* Voor bestaande functies kan worden volstaan met het opstellen van een (nieuwe) gedragscode of een extra artikel voor het personeelsreglement ten aanzien van privacygevoelige en vertrouwelijke informatie en het vastleggen van de toegang die de medewerkers nu op grond van hun functie hebben tot privacygevoelige en vertrouwelijke informatie.

De leidinggevenden hebben de verantwoordelijkheid om de werkzaamheden van individuele personeelsleden op het vlak van informatiebeveiliging periodiek te beoordelen. Dit kan door informatiebeveiliging als standaard onderwerp op de agenda te zetten tijdens functionerings- en beoordelingsgesprekken.

Bij nieuw of onervaren personeel moet de leidinggevende nagaan of extra toezicht op het naleven van de beveiligingsmaatregelen noodzakelijk is.

### Beveiligingseisen in functiebeschrijving

Neem in de functiebeschrijvingen de beveiligingseisen op. De beschrijving van de rollen en verantwoordelijkheden van gemeentelijke medewerkers, ingehuurde partijen en derden dient in overeenstemming met het informatiebeveiligingsbeleid van de gemeente te zijn. Hierbij gaat het enerzijds om de gewenste integriteit van de functionaris inclusief zijn betrouwbaarheid en zijn omgang met vertrouwelijkheid en anderzijds om de uit te voeren werkzaamheden die betrekking hebben op de veiligheid met betrekking tot de gemeente. Door in functiebeschrijvingen de gewenste kwaliteiten en de werkzaamheden met betrekking tot veiligheid op te nemen, borgt men het niveau van veiligheid.

**Integriteit en vertrouwelijkheid per functie**

Geef per functionaris aan in welke van de drie functiecategorieën[[29]](#footnote-29) deze valt, hierbij wordt indirect de gewenste betrouwbaarheid (integriteit en vertrouwelijkheid) van de functionaris vastgelegd in de functiebeschrijvingen. Met deze indeling wordt in feite het niveau van screening gedefinieerd.

**Beveiligingshandelingen per functie**

Geef speciale aandacht in de functiebeschrijving aan de werkzaamheden, die directe beveiligingshandelingen betreffen. Vooral de rollen en verantwoordelijkheden, zoals deze beschreven zijn in het beleid, behoren in de functiebeschrijvingen terug te komen. Daarnaast behoren ook alle operationele taken in de functiebeschrijvingen terug te keren.

### Uitwerking

De beschrijving van de rollen en verantwoordelijkheden van alle betrokken personen belast met informatiebeveiliging dient aan de volgende eisen te voldoen:

* Er dient vastgelegd te worden dat wordt gehandeld in overeenstemming met het informatiebeveiligingsbeleid van de gemeente.
* Er dient vastgelegd te worden dat medewerkers individueel verantwoordelijk zijn voor hun acties voortvloeiend uit hun rollen en verantwoordelijkheden.
* Er dient vastgelegd te worden dat melding wordt gemaakt van (mogelijke) beveiligingsincidenten of zwakheden via het proces incidentbeheer van de gemeente.
* Bij personen die geen arbeidscontract hebben met de gemeente dienen de rollen en verantwoordelijkheden voor informatiebeveiliging contractueel vastgelegd te worden.
* Er dient vastgelegd te worden wie verantwoordelijk zijn voor de bescherming van de gemeentelijke bedrijfsmiddelen tegen ongeautoriseerde toegang, ontsluiting, wijziging, vernietiging of verstoring.
* Er dient vastgelegd te worden wie voor welk beveiligingsproces en / of beveiligingsactiviteit verantwoordelijk is.
* Er dient vastgelegd te worden dat bij indiensttreding een VOG verplicht is als de functie genoemd staat in het screeningsbeleid.

### Functionerings- en beoordelingsgesprekken

De direct leidinggevende houdt periodiek (bijvoorbeeld jaarlijks) functionerings- en beoordelingsgesprekken met de medewerkers. Een vast onderdeel van deze gesprekken moet het omgaan met privacygevoelige en vertrouwelijke informatie en informatiebeveiliging zijn. Dit moet als onderwerp toegevoegd worden aan het formulier dat wordt gebruikt tijdens deze gesprekken. Bij nieuw en onervaren personeel is het van groot belang hier extra op toe te zien, in ieder geval ter bewustwording.

## Verantwoordelijkheden

Leidinggevenden binnen de gemeenten worden door de Chief Information Security Officer (CISO) ingelicht over: het informatiebeveiligingsbeleid, de hierbij behorende richtlijnen en gedragscodes en specifieke maatregelen of procedures die gelden voor informatiesystemen. Dit gebeurt in speciale werkoverleggen of tijdens Management Teamvergaderingen. Het management is vervolgens verantwoordelijk voor het kenbaar maken en uitdragen van deze informatie aan zowel de interne als externe medewerkers. Zij zijn er ook voor verantwoordelijk dat de gemeentelijke medewerkers, ingehuurde partijen en derden zich houden aan de informatiebeveiligingsvoorschriften en de bijbehorende procedures van de gemeente. Zij gebruiken hiervoor de reguliere werkoverlegmomenten en zetten informatiebeveiliging als vast punt op de agenda.

Het toezien op het tijdig actualiseren en kenbaar maken van beveiligingsmaatregelen, richtlijnen, gedragscodes en procedures is een verantwoordelijkheid van de CISO. In de regel is management verantwoordelijk voor het actualiseren en kenbaar maken. In de praktijk zal de CISO hierin een faciliterende en ondersteunende rol spelen. De proceseigenaar (desbetrefende manager) is dan ook verantwoordelijk voor het documentbeheer. Ook hier kan de CISO een ondersteunende rol spelen om dit te bewerkstelligen. Bij publicatie van deze documenten dient rekening gehouden te worden met de vertrouwelijkheid van bepaalde beveiligingsinformatie.

### Uitwerking

Het management van de gemeente dient ervoor te zorgen dat alle gemeentelijke medewerkers, ingehuurde partijen en derden:

* Op de hoogte zijn van hun beveiligingsrol(len) en verantwoordelijkheden voordat ze toegang krijgen tot vertrouwelijk en geheime geclassificeerde informatie.
* Op de hoogte zijn van de informatiebeveiligingsvoorschriften die gelden binnen de gemeente en noodzakelijk zijn om hun rol(len) uit te kunnen voeren.
* Gemotiveerd zijn om de informatiebeveiligingsvoorschriften na te leven.
* Werken en zich gedragen in overeenstemming met het afgesloten contract, geldende personeelsreglementen, de informatiebeveiligingsvoorschriften en daarmee samenhangende procedures (bijvoorbeeld het melden van beveiligingsincidenten).
* beschikken over de juiste vaardigheden en kwalificaties.

Bovenstaande is te bereiken door bewustwording, opleiding en training op de juiste manier in te zetten.

## Bewustwording, opleiding en training

De veiligheid van informatiesystemen wordt bepaald door de zwakste schakel. Vaak is dat de mens/personeel en dit is dan ook de meest cruciale factor voor het slagen van de informatiebeveiliging. Wanneer het personeel zich niet houdt aan de beveiligingsrichtlijnen en –procedures of nog erger, deze bewust schendt, is elk informatiebeveiligingsbeleid tot mislukken gedoemd.

Alle gemeentelijke medewerkers, ingehuurde partijen en derden dienen een toereikende voorlichting en training te krijgen om:

* Hun bewustzijn ten aanzien van informatiebeveiliging (awareness) te vergroten;
* Hun beveiligingsgedrag te verbeteren;
* Hen te informeren over, voor hun functie, relevante kennis van bestaande beveiligingsrichtlijnen, –procedures en het informatiebeveiligingsbeleid.

Het streven is om de medewerkers zich werkelijk bewust te laten zijn van hun eigen rol en positie in relatie tot veilig gedrag. Ook moet duidelijk zijn wat de consequenties zijn als ze dat niet doen. Deze regels en het sanctiebeleid geven de medewerkers een handvat hoe zij zich moeten gedragen binnen de eigen verantwoordelijkheid. Regels zijn echter geen excuus voor de medewerkers om niet meer zelf na te denken en moeten ook als zodanig gepositioneerd te worden.

De vraag is wat de organisatie kan doen om het juiste gedrag van de medewerkers te bevorderen. Er zijn een aantal mogelijkheden:

* Er kunnen maatregelen worden genomen om te voorkomen, dat er ‘verkeerde’ medewerkers in dienst zijn of dat ‘verkeerd’ gedrag ongemerkt of ongestraft kan plaatsvinden (zie paragraaf 2.1 ‘Screening bij het aannemen van personeel’);
* Er zijn maatregelen mogelijk waarmee het beveiligingsbewustzijn wordt vergroot (zie paragraaf 2.6 ‘Bewustwording, opleiding en training’);
* Ernstige of herhaaldelijke schendingen van de informatiebeveiliging kunnen worden aangemerkt als plichtverzuim met alle gevolgen van dien (zie paragraaf 2.9 ‘Disciplinaire maatregelen’);
* Sommige gedragsregels kunnen door technische maatregelen worden afgedwongen (zie hieronder voor een uitgebreidere beschrijving).

Naast het formuleren van de regels moeten deze ook actief onder de aandacht worden gebracht. Uitsluitend als medewerkers op de hoogte zijn van de regels, kunt u hen daar op aanspreken.

Diverse gemeentelijke afdelingen kunnen bijdragen aan bewustwording. Bewustwording kent zijn grenzen en is niet gericht op medewerkers die willens en wetens de regels overtreden. Het gaat om het voorkomen van onjuist handelen door onwetendheid, slordigheid et cetera. De managers moeten deze bewustwording actief ondersteunen.

### Technische maatregelen

Er zijn tal van technische mogelijkheden om gewenst gedrag af te dwingen. Dit soort maatregelen heeft voor- en nadelen. De voordelen zijn dat de integriteit van de informatie beter wordt beschermd en dat de technische beheersbaarheid wordt vergroot. Dit laatste punt kan een bijdrage leveren aan de mogelijkheden van de ICT-afdeling om de continuïteit te waarborgen. Een nadeel is dat de suggestie kan worden gewekt, dat alles wat kan, ook mag. Een ander nadeel kan zijn, dat het vaak moeilijk is om de maatregelen zo in te regelen, dat het ook ongevaarlijke activiteiten belemmerd. Een voorbeeld daarvan is het downloaden van nuttige (en ongevaarlijke) software.

Neem na alle afwegingen zo veel mogelijk technische maatregelen om het gedrag van medewerkers te sturen. Deze maatregelen worden uitsluitend ingevoerd na instemming van de ondernemingsraad (OR).

### Uitwerking

De activiteiten voor het verhogen van het bewustzijn rondom informatiebeveiliging dienen aan de onderstaande eisen te voldoen.

* Medewerkers dienen een passende introductie te krijgen over informatiebeveiliging en de manier waarop de gemeente hieraan invulling geeft. In introductieprogramma’s[[30]](#footnote-30) van nieuw personeel wordt informatiebeveiliging als vast onderdeel meegenomen en dient ten minste de volgende onderwerpen te bevatten:
	+ Toelichting op de voorschriften/gedragsregels (omgaan met papier, wachtwoorden, mobiele gegevensdragers, mobiele apparaten, telewerken en gebruik internet);
	+ Toelichting op beveiligingsprocessen (bijvoorbeeld rapporteren beveiligingsincidenten);
	+ Toelichting hoe correct gebruik te maken van informatieverwerkende voorzieningen;
	+ Toelichting op het disciplinaire beleid van de gemeente (zie ook het onderdeel disciplinaire maatregelen in deze paragraaf).
* Regelmatig worden activiteiten uitgevoerd die het beveiligingsbewustzijn bevorderen en op peil houden. In de jaarplannen en werkoverleggen wordt daar aandacht aan besteed.[[31]](#footnote-31).
* Informeer werknemers over het informatiebeveiligingsbeleid en de beveiligingsreglementen. Iedereen die voor de gemeente werkt, behoort geïnformeerd te zijn over het bestaan en over de inhoud van deze documenten, alsook zijn rol in de handhaving van de beveiliging van de gemeente.
* Informeer en/of train de werknemers in het omgaan met de beveiligingsprocedures en het correcte gebruik van de ICT-voorzieningen. Het betreft hier de omgang met wachtwoorden, de inlogprocedures, het gebruik van de software, het herkennen en rapporteren van (potentiële) beveiligingsincidenten en dergelijke.
* Er dienen beveiligingsopleidingen beschikbaar te zijn die aansluiten op de rol, kennis en verantwoordelijkheid van de medewerker.
* Bij opleidingen in het gebruik van informatiesystemen dient expliciet aandacht te worden besteed aan de beveiligingsmaatregelen die specifiek bij het informatiesysteem horen. Indien deze opleidingen door derden (bijvoorbeeld ICT-leveranciers) worden gegeven, dan moeten informatiebeveiliging en de eigen procedures onderdeel zijn van het opleidingsprogramma. De functioneel beheerder ziet toe op naleving van deze afspraak bij opleidingen.
* Bij nieuwe versies van programmatuur of apparatuur dient de functioneel beheerder te beoordelen of aanvullende training op het gebied van informatiebeveiliging aan de medewerkers noodzakelijk is. Dit dient een onderdeel te zijn van de acceptatieprocedure.

## Monitoren

Controle op naleving van de regels door de medewerkers, denk hierbij aan het gedrag van medewerkers in informatiesystemen met gevoelige informatie, moet worden gewaarborgd. Bijvoorbeeld door structurele logging, monitoring en auditing[[32]](#footnote-32) van inloggegevens. Deze maatregelen dienen besproken te worden met de OR, in verband met de mogelijke juridische consequenties, en uitsluitend ingevoerd te worden na instemming van de OR. De resultaten kunnen besproken worden bij de functionerings- en beoordelingsgesprekken met de medewerkers.

Om ten einde beveiligingsincidenten te kunnen beheersen zijn registraties en rapportages nodig. Monitoren omvat het registreren, kwalificeren, rapporteren, escaleren en evalueren van beveiligingsincidenten.

### Uitwerking

De activiteiten met betrekking tot de controle op naleving van de regels dienen aan de onderstaande eisen te voldoen.

* Beveiligingsincidenten worden geregistreerd, gerapporteerd, geëscaleerd en geëvalueerd. Registreer bij alle cruciale processen die gebeurtenissen die relevant zijn voor het kunnen reconstrueren van eventuele incidenten. Denk daarbij vooral aan de logische en fysieke toegang.
* Vanuit deze registraties worden tevens rapportages samengesteld die een overzicht geven over de beveiligingstoestand. Op basis daarvan kan men lering trekken uit eerdere incidenten.
* Zorg voor standaardisatie en centralisatie van deze registraties, signaleringen en rapportages. Het kan hierbij immers om zeer grote aantallen systemen gaan. Zonder standaardisatie en centralisatie zullen deze registraties sterk in kwaliteit uiteenlopen en door het grote aantal van deze registraties zou een onbeheersbare situatie kunnen ontstaan.

## Afhandeling beveiligingsincidenten

Om lering te kunnen trekken uit beveiligingsincidenten, is het van het grootste belang dat deze ook gemeld worden aan de Servicedesk, de directe leidinggevende en/of de CISO.[[33]](#footnote-33)

Door een beveiligingsincident te melden en vervolgens te analyseren, is te beoordelen of procedures aangepast moeten worden, of scholing verbeterd moet worden. Of misschien dat er technische oplossingen bedacht kunnen worden om dergelijke situaties te voorkomen.

### Uitwerking

De activiteiten voor bij de afhandeling van beveiligingsincidenten dienen aan de onderstaande eisen te voldoen.

* Zorg ervoor dat de persoonlijke betrokkenheid van de daders bij incidenten en de disciplinaire maatregelen vertrouwelijk behandeld worden. Sta niet toe dat de betrokken personen met naam en toenaam bekend worden.
* Maak overzichten van de aard, omvang en kosten van incidenten. Stel vast welke incidenten aanvullende maatregelen vereisen. Door overzichten te maken en door kosten te kwantificeren wordt inzichtelijk waar maatregelen het beste renderen.
* Leer van incidenten en zorg voor een veilige meldcultuur.

## Disciplinaire maatregelen

Er dient een formeel disciplinair proces te zijn in het geval van (bewust) doorbreken van beveiligingsmaatregelen of het overtreden van het informatiebeveiligingsbeleid of beveiligingsvoorschriften door een interne of externe medewerker. Op basis van de ernst van de beveiligingsovertreding wordt bepaald welke disciplinaire maatregel wordt gehanteerd. Deze maatregelen kunnen variëren van een waarschuwing tot onmiddellijk ontslag en eventuele juridische stappen.

**Formaliseer disciplinaire maatregelen**

Hanteer vaste formele procedures voor de afhandeling van incidenten, voor eventuele disciplinaire maatregelen en voor de contacten met justitie. Sta niet toe dat er op dit punt ruimte voor willekeur is. Immers onduidelijkheid op dit punt geeft ruimte voor meer. Zie hiervoor de disciplinaire straffen en schorsing zoals vastgelegd in de CAR-UWO, de arbeidsvoorwaardenregeling voor de sector gemeenten.[[34]](#footnote-34) Zie bijlage 3 voor voorbeelden van disciplinaire maatregelen.

### Uitwerking

Het disciplinaire proces voor het bestraffen van overtredingen gerelateerd aan informatiebeveiliging dient aan de onderstaande eisen te voldoen:

* Voordat het disciplinaire proces wordt gestart dient zekerheid verschaft te worden dat er een beveiligingsovertreding heeft plaatsgevonden.
* Er dienen voldoende waarborgen ingebouwd te zijn die zorgen voor een rechtvaardige behandeling van medewerkers die verdacht zijn van een overtreding.
* Wanneer vast staat dat een medewerker een overtreding heeft begaan dienen de te nemen maatregelen proportioneel en adequaat te zijn voor de begane overtreding.
* Bij zeer ernstige overtredingen dienen er procedures te bestaan om een medewerker direct uit zijn functie te zetten, al zijn rechten en privileges in te trekken en hem onder begeleiding direct uit een gemeentelijk gebouw te verwijderen.

## Uitdiensttreding en wijziging van de aanstelling/dienstverband

De verantwoordelijkheden voor het beëindigen of wijzigen van een dienstverband / arbeidsovereenkomst dienen belegd te zijn.

Bij uitdiensttreding of functiewijziging van een medewerker zal door de leidinggevende moeten worden nagegaan of de rechten van toegang tot gebouw[[35]](#footnote-35), apparatuur en informatie op de juiste wijze zijn ingetrokken of gewijzigd.

De vertrekkende medewerker zal bij uitdiensttreding moeten worden gewezen op eventuele resterende verplichtingen op het gebied van informatiebeveiliging, zoals een blijvende verplichting tot geheimhouding. Een checklist ‘personeel uit dienst’ helpt bij het controleren van deze punten. Zie bijlage 2 voor een voorbeeld checklist bij uitdiensttreding.

### Uitwerking

Het proces rondom de beëindiging of wijziging van een arbeidscontract dient aan de onderstaande eisen te voldoen.

* HR- / P&O-adviseur zijn in verband met de objectiviteit verantwoordelijk voor het voeren van een exitgesprek waarin minimaal de volgende onderwerpen worden besproken:
	+ De werkzaamheden die de vertrekkende werknemer nog mag uitvoeren.
	+ Welke informatie en kennis de vertrekkende werknemer dient over te dragen aan de gemeente.
	+ De vertrekkende werknemer dient te worden gewezen op de contractuele geheimhoudingsplicht voor vertrouwelijk en geheim geclassificeerde informatie.
	+ Afspraken over de in te leveren bedrijfsmiddelen die eigendom zijn van de gemeente door de vertrekkende medewerker bij het einde van het dienstverband.
* Het wisselen van functie dient afgehandeld te worden als het beëindigen van de functie en het ‘in dienst’ treden voor de nieuwe functie.
* HR / P&O is verantwoordelijk voor de registratie van de exitgesprekken, ook als het exitgesprek door de leidinggevende is uitgevoerd.

**Retourneren van bedrijfsmiddelen**

Alle gemeentelijk medewerkers, ingehuurde partijen en derden dienen alle bedrijfsmiddelen die eigendom zijn van de gemeente te retourneren na beëindiging van het arbeidscontract of de overeenkomst.

### Uitwerking

Deze procedures dienen aandacht te besteden aan:

* Indien de gemeentelijke medewerkers, ingehuurde partijen of derden gebruik maken van eigen middelen tijdens de werkzaamheden voor de gemeente dient onderzocht te worden of alle relevante informatie volledig is overgedragen. Tevens dient deze informatie volledig en op een passende manier te worden verwijderd van deze gegevensdrager.[[36]](#footnote-36)
* Indien gemeentelijke medewerkers, ingehuurde partijen of derden kennis hebben die van belang is voor lopende processen dient deze informatie tijdig te worden gedocumenteerd en overgedragen aan de gemeente.
* De procedures rondom het beëindigen van het contract dient een procedure te bevatten die de teruggaaf van bedrijfsmiddelen beschrijft. Zie bijlage 2 voor een voorbeeld checklist bij uitdiensttreding.

Verwijderen van toegangsrechten

Het beschermen van gemeentelijke informatie en bedrijfsmiddelen tegen gemeentelijke medewerkers, ingehuurde partijen of derden waarvan het contract is beëindigd of gewijzigd.

### Uitwerking

Deze procedures dienen aandacht te besteden aan:

* Toegangsrechten van gemeentelijke medewerkers, ingehuurde partijen of derden die toegang tot informatie of bedrijfsmiddelen van de gemeente hebben, dienen te worden aangepast op het moment dat het contract met de desbetreffende persoon is beëindigd of gewijzigd.
* Bij een wijziging in de werkzaamheden dienen alle toegangsrechten te worden verwijderd die niet noodzakelijk zijn voor de uitvoering van de nieuwe werkzaamheden. Toegangsrechten die dienen te worden verwijderd of aangepast, omvatten fysieke en logische toegang, sleutels, identificatiekaarten en informatieverwerkende voorzieningen. Abonnementen dienen te worden gewijzigd en in alle administraties dient aangegeven te worden dat de betreffende persoon niet langer werkzaam is voor de gemeente.
* Indien een gemeentelijke medewerker, ingehuurde partij of derden waarvan het contract is beëindigd of gewijzigd in het bezit is van geheime codes (bijvoorbeeld wachtwoorden of toegangscodes) die gedeeld worden met andere medewerkers dienen deze geheime codes te worden veranderd.
* Toegangsrechten tot informatiebedrijfsmiddelen en informatieverwerkende voorzieningen dienen op basis van een risicoafweging te worden beperkt of verwijderd voordat het contract wordt beëindigd of gewijzigd.
* In bepaalde omstandigheden zijn de toegangsrechten toegewezen aan meerdere personen dan alleen de vertrekkende gemeentelijke medewerker, ingehuurde partij of derden, zoals functionele accounts. De vertrekkende medewerker dient te worden verwijderd als lid van deze groepen en er dienen afspraken te worden gemaakt dat alle andere betrokken medewerkers van de gemeente, ingehuurde partijen en derden geen informatie meer delen met de vertrekkende medewerker.

Bijlage 1:  Voorbeeld checklist bij indiensttreding

**1. Persoons- en adresgegevens**

|  |  |
| --- | --- |
| Naam: |  |
| Voornamen voluit: |  |
| Roepnaam: |  |
| Datum in dienst: |  |
| Geboorte datum: |  |
| 1e werkdag: |  |
| Functie: |  |
| Afdeling: |  |
| Leidinggevende: |  |

**2. Aanmelden / ontvangen documenten**

|  |  |  |
| --- | --- | --- |
| **Actie** | **Ja / Nee / n.v.t.** | **Retour** |
| Personeelsdossier aangemaakt |  |  |
| Arbeidsovereenkomst in tweevoud opgesteld |  |  |
| Arbeidsovereenkomst ondertekend door directie |  |  |
| Loonbelastingverklaring |  |  |
| In dienst melden personeelsinformatiesysteem |  |  |
| Aangemeld bij Belastingdienst[[37]](#footnote-37) |  |  |
| Aangemeld bij Arbodienst |  |  |
| Aangemeld bij Pensioenfonds |  |  |
| Aangemeld bij de uitvoeringsinstelling voor werknemersverzekeringen |  |  |
| Aanmeldingsformulier ziektekosten |  |  |
| Aanmeldingsformulier levensloopregeling |  |  |
| Kopie geldig identiteitsbewijs |  |  |
| Kopie diploma’s ontvangen |  |  |
| Verklaring Omtrent het Gedrag ontvangen |  |  |
| Overig: |  |  |
|  |  |  |

**3. Te nemen acties (voor de 1e werkdag)**

|  |  |  |  |
| --- | --- | --- | --- |
| **Actie** | **Ja / Nee / n.v.t.** |  | **Actiehouder** |
| Informeren van receptie[[38]](#footnote-38) |  |  |  |
| Informeren leidinggevende[[39]](#footnote-39) |  |  |  |
| Werkplek |  |  |  |
| Sleutels |  |  |  |
| Toegangspassen |  |  |  |
| Parkeerpas/Parkeerplaats |  |  |  |
| Documentatie |  | Titel |  |  |
| (Hand)boeken |  | Titel |  |  |
| Mobiele telefoon |  | Merk/type |  |  |
| SIM-kaart |  | Provider |  |  |
| Computerapparatuur (laptop) |  | Merk/type |  |  |
| Apparatuur |  | Merk/type |  |  |
| Software |  | Merk/versie |  |  |
| Mobiele gegevensdragers |  | Merk/type |  |  |
| Aangemeld bij informatiesystemen[[40]](#footnote-40) |  |  |  |
| <informatiesysteem> |  |  |  |
| E-mailaccount aangevraagd |  |  |  |
| Introductieprogramma opstellen |  |  |  |
| Introductiemap samengesteld |  |  |  |
| Overig: |  |  |  |
|  |  |  |  |

**4. Checklist 1e werkdag**

|  |  |  |
| --- | --- | --- |
| **Actie** | **Ja / Nee** | **Actiehouder** |
| Arbeidsovereenkomst ondertekend in ontvangst genomen |  |  |
| Introductiemap inclusief Personeelshandboek / CAO boekje / personeelsreglement / huis- en gedragsregels overhandigd  |  |  |
| Rondleiding |  |  |
| Voorstellen collega’s |  |  |
| Ziekmeldingsprocedure toelichten |  |  |
| Verlofprocedure toelichten |  |  |
| Werk benodigdheden/ apparatuur verstrekken |  |  |
| Uitnodigen deelname training i-bewustzijn |  |  |
| Overig: |  |  |
|  |  |  |

**5. Inwerken**

|  |  |  |
| --- | --- | --- |
|  | **Ja / Nee** | **Actiehouder** |
| **Benoem een mentor.***Het is een enorm houvast voor de nieuweling. De ideale kandidaat is een collega met meer ervaring die hetzelfde werk doet.* |  |  |
| **Zorg voor een lijst met personen die belangrijke informatie kunnen geven over de functie.***Ook de namen van de functionarissen die veel contact hebben met de nieuweling horen hierop thuis. Met deze mensen moet de nieuweling zeker kennis maken.* |  |  |
| **Besef dat voor de nieuweling veel, zo niet alles nieuw is. Ook de voor u meest vanzelfsprekende zaken.***Stel de werknemer op zijn gemak, toon de eerste praktische dingen en benadruk dat er altijd iemand is om vragen te beantwoorden.* |  |  |
| **Zorg voor een feestelijke stemming op de eerste werkdag.***Denk aan een bloemetje op het bureau, of een lunch met de hele afdeling om informeel kennis te maken.* |  |  |
| **Probeer in het programma een vragenuur op te nemen***Dit voorkomt dat er onduidelijkheden blijven bestaan en het bespaart uiteindelijk tijd.* |  |  |
| **Sluit de introductie af met een eindgesprek***De nieuweling kan vanaf dat moment volledig op zijn taak en verantwoordelijkheid worden aangesproken. Bovendien geeft een evaluatie ook uzelf nuttige informatie.* |  |  |

**6. Ondertekening**

|  |
| --- |
| **Arbeidsovereenkomst en formulieren zijn ondertekend ontvangen en werknemer is geïnformeerd over bovenstaande punten:** |
| Naam |  | Handtekening: |  |
| Datum |  |  |  |

|  |
| --- |
| **Alle overige punten (ontvangst, apparatuur, rondleiding zijn verzorgd.)** |
| Naam |  | Handtekening: |  |
| Datum |  |  |  |

Bijlage 2: Voorbeeld checklist bij uitdiensttreding

**1. Persoonsgegevens**

|  |  |
| --- | --- |
| Naam: |  |
| Personeelsnummer: |  |
| Datum in dienst: |  |
| Functie: |  |
| In functie sinds: |  |
| Afdeling: |  |
| Leidinggevende: |  |

**2. Algemeen**

|  |  |  |  |
| --- | --- | --- | --- |
| **Actie** | **Ja / Nee / n.v.t.** | **Actiehouder/ Verantwoordelijke** | **Afgehandeld****op datum** |
| Verzoek tot eervol ontslag ontvangen  |  |  |  |
| Bevestiging opzegging verzonden |  |  |  |
| Start nieuwe werving |  |  |  |
| Uitgenodigd voor een exit gesprek |  |  |  |
| Getuigschrift opgesteld |  |  |  |
| Afscheidgeschenk geregeld |  |  |  |
|  |  |  |  |

**3. Afmelden/opzeggen**

|  |  |  |  |
| --- | --- | --- | --- |
| **Actie** | **Ja / Nee / n.v.t.** | **Actiehouder/ Verantwoordelijke** | **Afgehandeld op datum** |
| Afmelden ziektekosten |  |  |  |
| Afmelden bij het pensioenfonds |  |  |  |
| Afmelden bij de Arbodienst |  |  |  |
| Afmelden bij levensloopregeling |  |  |  |
| Afmelden bij de bedrijfs-/personeelsvereniging |  |  |  |
| Uitdienst melden personeelsinformatiesysteem |  |  |  |
|  |  |  |  |
|  |  |  |  |

**4. Intrekken rechten**

|  |  |  |  |
| --- | --- | --- | --- |
| **Actie** | **Ja / Nee / n.v.t.** | **Actiehouder/ Verantwoordelijke** | **Afgehandeld op datum** |
| Intrekken rechten voor alle systemen[[41]](#footnote-41) |  |  |  |
| <informatiesysteem> |  |  |  |
| Blokkeren van toegang tot e-mail[[42]](#footnote-42) |  |  |  |
| Blokkeren van mogelijkheid tot inloggen35 |  |  |  |
|  |  |  |  |

**5. Eindafrekening**

|  |  |  |  |
| --- | --- | --- | --- |
| **Actie** | **Ja / Nee / n.v.t.** | **Actiehouder/ Verantwoordelijke** | **Afgehandeld op datum** |
| Afrekenen van het vakantiegeld |  |  |  |
| Afrekenen van de eindejaarsuitkering |  |  |  |
| Afrekenen verlofdagen |  |  |  |
| Afrekenen van de tegemoetkoming ziektekostenvergoeding |  |  |  |
| Afrekenen studieschuld/ kosten |  |  |  |
| Afrekenen openstaande leningen |  |  |  |
|  |  |  |  |
|  |  |  |  |

**6. Uitgegeven middelen**

|  |  |  |  |
| --- | --- | --- | --- |
| **Actie** | **Ja / Nee / n.v.t.** |  | **Ingeleverd op datum** |
| Sleutels retour |  |  |  |
| Toegangspassen retour |  |  |  |
| Documentatie retour |  | Titel |  |  |
| (Hand)boeken retour |  | Titel |  |  |
| Mobiele telefoon retour |  | Merk/type |  |  |
| SIM-kaart retour |  | Provider |  |  |
| Computerapparatuur (laptop) retour |  | Merk/type |  |  |
| Apparatuur |  | Merk/type |  |  |
| Software retour |  | Merk/versie |  |  |
| Mobiele gegevensdragers retour |  | Merk/type |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

**7. Overig**

|  |  |  |  |
| --- | --- | --- | --- |
| **Actie** | **Ja / Nee / n.v.t.** | **Actiehouder/ Verantwoordelijke** | **Afgehandeld op datum** |
| Getuigschrift afgeven |  |  |  |
| Exit gesprek voeren |  |  |  |
| Afscheid organiseren |  |  |  |
|  |  |  |  |
|  |  |  |  |

**8. Ondertekening**

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Datum:** | **Naam:** | **Handtekening:** |
| Medewerker: |  |  |  |
| Leidinggevende: |  |  |  |

Bijlage 3: Voorbeeld Disciplinaire straffen

De werkgever kan een tiental disciplinaire straffen opleggen, variërend van een schriftelijke berisping tot ongevraagd ontslag. Er dient sprake te zijn van evenredigheid tussen de opgelegde straf en de ernst van het plichtsverzuim. Criteria voor wat wel of niet als evenredig valt aan te merken, zijn niet te geven.

Onderstaande opsomming van disciplinaire straffen is limitatief. Het is ook mogelijk om een combinatie van straffen op te leggen.[[43]](#footnote-43)

Schriftelijke berisping

Een schriftelijke berisping is de lichtste disciplinaire straf. Het is een officiële schriftelijke waarschuwing – al dan niet na eerdere waarschuwingen – waarbij eventuele consequenties in geval van herhaling van het plichtsverzuim kunnen worden genoemd.

### Arbeid verrichten buiten de voor hem geldende werktijd

De medewerker kan worden verplicht arbeid te verrichten buiten zijn normale werktijden. De werkgever kan besluiten deze uren slechts gedeeltelijk of helemaal niet te vergoeden. De straf mag maximaal zes uur duren. Per dag mag niet meer dan drie uur van de straf worden uitgevoerd. De arbeid kan niet worden verricht op een zondag of een voor de medewerker geldende kerkelijke feestdag.

### Vermindering van vakantie

De vakantie kan verminderd worden met ten hoogste een derde deel van het aantal vakantie-uren waarop de medewerker in een jaar aanspraak heeft

### Geldboete

De werkgever kan een geldboete opleggen. Deze boete mag ten hoogste 1% van het jaarsalaris bedragen.

### Inhouding salaris

De werkgever kan salaris inhouden ter hoogte van maximaal een half maandsalaris.

### Geen periodiek

De gebruikelijke periodieken kunnen voor ten hoogste vier jaren niet worden toegekend. Algemene salarisverhogingen worden wel doorgevoerd. Eventuele salarisverhogingen als gevolg van een functieherwaardering worden ook doorgevoerd.

### Vermindering van salaris

De werkgever kan besluiten het salaris van de medewerker te korten. De korting bedraagt ten hoogste het bedrag van de twee laatste periodieken. Ook kan deze straf ten hoogste gedurende twee jaar worden opgelegd. Wanneer het salaris een vast bedrag is, kan de vermindering tot 5% van dat bedrag gaan.

### Plaatsing in een andere betrekking

De medewerker kan in een andere functie worden geplaatst. Dit kan tijdelijk zijn of voor altijd. Als de nieuwe functie een andere bezoldiging kent, is het mogelijk om de bezoldiging al dan niet te verminderen.

### Schorsing als disciplinaire straf

De medewerker kan voor een bepaalde tijd worden geschorst. Daarbij kan de bezoldiging geheel of gedeeltelijk worden ingehouden. Al naar gelang de ernst van de gedraging van de medewerker, stelt de werkgever de inhouding op de bezoldiging vast.

### Ontslag als disciplinaire straf

De zwaarste straf is ongevraagd ontslag. Afhankelijk van de ernst van de misdraging van de medewerker kan deze direct of na (een) andere disciplinaire maatregel(en) worden opgelegd. Wanneer de straf niet direct wordt opgelegd, kan de medewerker in de aanloop naar het ontslag worden geschorst. Dit betreft dan een schorsing als ordemaatregel en niet een schorsing als disciplinaire straf. UWV beoordeelt of recht bestaat op een WW-uitkering. Bij ontslag als disciplinaire maatregel bestaat geen recht op een bovenwettelijke werkloosheidsuitkering op grond van hoofdstuk 10a CAR-UWO.

### Voorwaardelijke straf

De werkgever kan besluiten de straf voorwaardelijk op te leggen. Dit betekent dat de straf niet ten uitvoer zal worden gelegd als de medewerker zich gedurende een bepaalde termijn niet meer schuldig maakt aan het vergrijp of andere vormen van plichtverzuim. Gedurende die termijn kunnen bijzondere voorwaarden voor het functioneren worden opgelegd. De voorwaarden dienen redelijk te zijn; er dient rekening te worden gehouden met de belangen van de organisatie en die van de medewerker. Ook de termijn waarbinnen de voorwaarde kan worden vervuld, dient redelijk te zijn. Wanneer aan een voorwaarde is voldaan, wordt de straf ten uitvoer gelegd. Een dergelijk uitvoeringsbesluit is een besluit in de zin van de Algemene wet bestuursrecht.

Bijlage 4: Literatuur/bronnen

Voor deze publicatie is gebruik gemaakt van onderstaande bronnen:

**Titel: Beleidsdocumenten in kader van informatiebeveiliging**

Voor het samenstellen van dit beleidsdocument is gebruik gemaakt van verschillende documenten die op het internet te vinden zijn. Bronnen hierbij zijn ‘Bureau Integriteitszorg De Achterhoek’, ‘Bureau Integriteitsbevordering Openbare Sector’ en ‘Coöperatie Integrale Huisartsenzorg Nijmegen’.

Links: <http://www.integriteitoverheid.nl/>, <http://integereachterhoek.nl/> en bijlage\_13\_Personeelsbeleid\_in\_kader\_van\_informatiebeveiliging.pdf op de volgende site: <https://www.huisartsenpostnijmegen.nl/content/praktijkhandboek-lsp>

**Titel: Nationale Richtlijn Pre-employment Screening**

Wie: Vereniging Beveiligingsprofessionals Nederland

Link: <https://www.security-kaders.nl/wp-content/uploads/2018/12/Nationale-Richtlijn-pre-in-post-employment-screening-3.0.pdf>

**Titel: in- en uitdienst checklists**

Voor het samenstellen van de checklist in- en uitdienst is gebruik gemaakt van verschillende formulieren die op het internet te vinden zijn. Bronnen hierbij zijn: <http://www.hr5.nl/>, <http://www.tuxx.nl/>



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 / incident@IBDGemeenten.nl

Kijk voor meer informatie op:

www.informatiebeveiligingsdienst.nl

1. Zie ook: <https://www.wnra.nl/wat-is-er-veranderd> [↑](#footnote-ref-1)
2. Meer informatie: <https://www.rijksoverheid.nl/onderwerpen/overheidspersoneel/werknemer-bij-de-overheid/nieuwe-rechtspositie-ambtenaren> [↑](#footnote-ref-2)
3. Zie ook <http://www.rijksoverheid.nl/onderwerpen/overheidspersoneel/vraag-en-antwoord/wat-zijn-de-arbeidsvoorwaarden-bij-de-overheid.html> [↑](#footnote-ref-3)
4. Zie hiervoor <https://vng.nl/onderwerpenindex/arbeidsvoorwaarden-en-personeelsbeleid/po-beleid/hr-21%20> en <http://www.hr21.nl/> [↑](#footnote-ref-4)
5. Zie voor de opzet en voorbeelduitwerking het operationele product ‘Communicatieplan’ [↑](#footnote-ref-5)
6. Zie hiervoor ook het operationele product ‘Handleiding screening personeel’ [↑](#footnote-ref-6)
7. Zie de ‘Handreiking integriteit politieke ambtsdragers’ van de VNG voor meer informatie met betrekking tot integriteit. De handreiking bevat een bijlage met een model gedragscode. <http://www.vng.nl/files/vng/nieuws_attachments/2013/20131007-integriteit-pol-ambtsdr.pdf> [↑](#footnote-ref-7)
8. <http://wetten.overheid.nl/BWBR0008277/> [↑](#footnote-ref-8)
9. Denk hierbij aan vertrouwelijke informatie, omgaan met geld, machts- en monopoliepositie, toekennen rechten/bevoegdheden (aan personeel of burgers), beoordelen en adviseren (met grote gevolgen), aanschaffen goederen/diensten/aanbestedingen, handhaven, solistisch handelen en werken in de directe invloedsfeer van burgers/bedrijven [↑](#footnote-ref-9)
10. Zie voor extra informatie <http://wetten.overheid.nl/BWBR0006297/> en <https://www.rijksoverheid.nl/onderwerpen/identificatieplicht> [↑](#footnote-ref-10)
11. Bij indiensttreding zijn de volgende soorten identiteitsbewijs geldig: Paspoort (Nederlands of Buitenlands) of Nederlandse Identiteitskaart. Let op: Het rijbewijs is dus geen geldig identiteitsbewijs bij indiensttreding, omdat de nationaliteit moet kunnen worden vastgesteld. [↑](#footnote-ref-11)
12. <https://www.justis.nl/> [↑](#footnote-ref-12)
13. Zie voor meer informatie <http://nl.wikipedia.org/wiki/Handelsinformatiebureau> [↑](#footnote-ref-13)
14. <https://www.kvk.nl/> [↑](#footnote-ref-14)
15. <https://www.kadaster.nl> [↑](#footnote-ref-15)
16. In dit register staan gegevens van faillissementen, surséances van betaling en schuldsaneringen van natuurlijke personen. De gegevens zijn vanaf januari 2005 gergegistreerd. Er zijn alleen gegevens vanaf die datum te raadplegen. Het register kunt u vinden op de website <https://insolventies.rechtspraak.nl> [↑](#footnote-ref-16)
17. Zie voor meer informatie: <https://wetten.overheid.nl/BWBR0040940/2019-01-01> [↑](#footnote-ref-17)
18. Zie hiervoor ook het operationele product ‘Wachtwoordbeleid’ [↑](#footnote-ref-18)
19. Zie hiervoor ook het operationele product ‘Mobiele gegevensdragers’. [↑](#footnote-ref-19)
20. Zie hiervoor ook het operationele product ‘Aanwijzing Mobile device management’. [↑](#footnote-ref-20)
21. Zie hiervoor ook het operationele product ‘Telewerkbeleid’ [↑](#footnote-ref-21)
22. Het personeelsreglement wordt ook wel personeelshandboek, personeelsregeling of arbeidsvoorwaardenreglement genoemd en is een aanvulling op de cao en/of arbeidsovereenkomst, waarin de arbeidsvoorwaarden (nader) zijn uitgewerkt. Het bevat belangrijke procedures, regelingen en overige voorwaarden ten behoeve van u en uw werknemers. Voorbeelden hiervan zijn: verzuimreglement, verlof et cetera. Het personeelsreglement maakt onderdeel uit van de arbeidsovereenkomst. De werknemer is daarom gehouden om de voorschriften en regels in het reglement na te leven, want deze heeft immers zijn/haar handtekening gezet onder de arbeidsovereenkomst. [↑](#footnote-ref-22)
23. <https://www.digitaleoverheid.nl/overzicht-van-alle-onderwerpen/basisregistraties-en-afsprakenstelsels/inhoud-basisregistraties/> [↑](#footnote-ref-23)
24. De voorwaarden met betrekking tot de basisregistatries zijn vastgelegd in de aansluitvoorwaarden op basisregistraties. Het niet voldoen aan de aansluitvoorwaarden kan leiden tot afsluiting van de basisregistratie zoals de Basisregistratie Personen (BRP), waardoor primaire bedrijfsvoering in gevaar komt. [↑](#footnote-ref-24)
25. Zie hiervoor ook het operationele product ‘Handreiking Geheimhoudingsverklaringen’ [↑](#footnote-ref-25)
26. Aan de uitzendbureaus is de verplichting opgelegd om de uitzendkrachten een geheimhoudings- en een integriteitsverklaring te laten ondertekenen. Check of dit ook daadwerkelijk is gebeurd en en vraag altijd om een kopie van de verklaring. [↑](#footnote-ref-26)
27. Zie hiervoor ook het operationele product ‘Voorbeeld Informatiebeveiligingsbeleid van de gemeente’. [↑](#footnote-ref-27)
28. Zie hiervoor ook het operationele product ‘Telewerkbeleid’. [↑](#footnote-ref-28)
29. Het gaat hierbij om vertrouwensfuncties, kwetsbare functies of algemene functies. Zie het operationele product ‘Handleiding screening personeel’ voor een uitgebreide omschrijving van deze functiecategorieën. [↑](#footnote-ref-29)
30. Zie hiervoor ook het onderdeel ‘introductiemap nieuwe medewerkers’ in paragraaf 2.1. [↑](#footnote-ref-30)
31. Zie hiervoor ook het operationele product ‘Handreiking Communicateplan’. [↑](#footnote-ref-31)
32. Zie hiervoor ook het operationele product ‘Aanwijzing Logging’. [↑](#footnote-ref-32)
33. Zie hiervoor ook het operationele product ‘Incident Management en responsebeleid’. [↑](#footnote-ref-33)
34. <http://www.car-uwo.nl/onderwerpenindex/disciplinaire-straffen-en-schorsing> [↑](#footnote-ref-34)
35. Zie hiervoor ook het operationele product ‘Toegangsbeleid’ [↑](#footnote-ref-35)
36. Zie hiervoor ook de operationele producten ‘Dataclassificatie’ en ‘Mobiele gegevensdragers’. [↑](#footnote-ref-36)
37. <http://www.belastingdienst.nl/bibliotheek/handboeken/html/boeken/HL/stappenplan-stap_2_gegevens_werknemer_administreren.html> [↑](#footnote-ref-37)
38. De receptie dient de nieuwe medewerker te ontvangen. [↑](#footnote-ref-38)
39. De leidinggevende dient aanwezig te zijn op 1e werkdag. [↑](#footnote-ref-39)
40. Denk hierbij aan accounts, rechten en software. [↑](#footnote-ref-40)
41. Voor ieder informatiesysteem/netwerkshare waar de medewerker rechten heeft dienen de rechten ingetrokken/geblokkeerd te worden. Na 3 maanden uit dienst dient het account in zijn geheel verwijderd te worden. Er dient per informatiesysteem/netwerkshare een afzonderlijke regel in dit overzicht opgenomen te zijn. [↑](#footnote-ref-41)
42. Na 3 maanden uit dienst dient het account in zijn geheel verwijderd te worden. [↑](#footnote-ref-42)
43. Bron: <http://www.car-uwo.nl/onderwerpenindex/disciplinaire-straffen-en-schorsing/disciplinaire-straf#Vermindering_van_vakantie>. [↑](#footnote-ref-43)