



## Integriteits- en geheimhoudingsverklaring

### INTEGRITEITS- EN GEHEIMHOUDINGSVERKLARING

BAR-organisatie, gemeente Barendrecht, gemeente Albrandswaard en gemeente Ridderkerk

Naam en voorletters \_\_\_\_\_

Geboortedatum \_\_\_\_\_

Geboorteplaats \_\_\_\_\_

Functie \_\_\_\_\_

Naam afdeling/team \_\_\_\_\_

#### Verklaart het volgende:

##### 1. Geheimhouding

Ik verklaar geheim te houden alle informatie die mij gedurende mijn werkzame periode ter kennis komt waarvan ik weet of vermoed dat deze vertrouwelijk is. Persoonsgegevens, financiële gegevens, klantgegevens, aanbestedingsgegevens en contractgegevens beschouw ik in ieder geval als vertrouwelijk. Ik verstrek deze informatie niet aan anderen, ook niet binnen de BAR-organisatie, tenzij dit noodzakelijk is voor de uitoefening van mijn taak of ik daartoe wettelijk verplicht ben. Bij twijfel neem ik contact op met de opdrachtgever of de CISO van de BAR-organisatie.

##### 2. Toegang tot gebouwen

Ik gebruik de hulpmiddelen voor toegang tot locaties, apparatuur en ruimten van de BAR-organisatie uitsluitend voor het doel waarvoor deze aan mij ter beschikking zijn gesteld. Ik probeer niet om onbevoegd toegang te krijgen tot locaties van de BAR-organisatie. Voor mij bestemde toegangsmiddelen behoud ik voor mijzelf en geef ik niet aan collega's of derden, tenzij daarover afspraken zijn gemaakt met de opdrachtgever en dit past in de bedrijfsvoering.

Bij vermissing, ontvreemding, misbruik of ander onrechtmatig gebruik van de mij verstrekte toegangspas, sleutels, tags, toegangscodes, apparatuur of software stel ik de daartoe aangewezen personen binnen het organisatieonderdeel waar ik werkzaam ben onmiddellijk daarvan in kennis.

Ik houd mij aan de regels die per locatie van de BAR-organisatie zijn gesteld ten aanzien van het ontvangen en begeleiden van bezoekers.

##### 3. Omgang informatie

Ik laat geen stukken onbeheerd achter, ook niet op mijn bureau, in de ruimte of (thuis)werkplek waar ik werk, waarvan ik weet of zou kunnen weten dat deze vertrouwelijk zijn. Ik houd mij op mijn (thuis)werkplek aan de regels voor de beveiliging van informatie. Als ik vermoed dat er een inbreuk wordt gemaakt op de informatieveiligheid dan doe ik daarvan een melding aan mijn leidinggevende/opdrachtgever en de CISO. Documenten, e-mails, en overige zaken die niet voor mij bestemd zijn, zend ik onmiddellijk door aan het juiste adres of ik retourneer deze aan de afzender. Is het juiste adres noch de afzender bekend, dan vernietig ik ze. Ik beperk de inzage en/of het gebruik van vertrouwelijke gegevens tot wat nodig is voor de vervulling van mijn werkzaamheden (Need-to-Know principe).



#### 4. Omgang bedrijfsmiddelen

Ik ga zorgvuldig om met alle mij ter beschikking gestelde bedrijfsmiddelen, zowel op mijn werkplek als elders waar ik bedrijfsmiddelen gebruik. Ik houd mij aan de geldende regels voor internet en e-mail gebruik en de huisregels van het organisatieonderdeel. Ik laat geen waardevolle bedrijfsmiddelen onbeheerd achter op mijn werkplek of elders waar ik bedrijfsmiddelen gebruik.

#### 5. Integriteit

Ik gedraag mij integer, wat in ieder geval inhoudt dat ik mij houd aan de interne regels over integriteit en de huisregels van mijn organisatieonderdeel.

Als ik een misstand constateer, meld ik deze in eerste bij mijn opdrachtgever of diens superieur. Als ik anoniem wil blijven, zal ik gebruik maken van de 'Klokkenluideregeling' en meld ik een geconstateerde misstand bij de vertrouwenspersoon integriteit bij mijn organisatieonderdeel.

Bij twijfel raadpleeg ik de vertrouwenspersoon integriteit.

#### 6. Omgangsvormen

Ik houd mij aan correcte omgangsvormen en ik houd mij aan de interne regels over ongewenst gedrag, omgangsvormen en de huisregels van mijn organisatieonderdeel.

Krijg ik te maken met ongewenste omgangsvormen dan kan ik mijn opdrachtgever raadplegen, dan wel de vertrouwenspersoon ongewenste omgangsvormen bij mijn organisatieonderdeel of de gemeentelijke vertrouwenspersoon. Wordt het probleem niet opgelost dan kan ik een klacht indienen bij de klachtencommissie van mijn dienst of de gemeentebrede klachtencommissie.

Ik verklaar verder in kennis te zijn gesteld van de inhoud van dit formulier en:

- mij te zullen houden aan alle in dit formulier genoemde (spel)regels;
- bekend te zijn met de verplichting melding te doen van elke schending van de geheimhoudingsplicht. Dit onverminderd hetgeen is bepaald in [artikel 162](#) van het [Wetboek van Strafvordering](#) (geldend op 17 november 2015);
- kennis te hebben genomen van de bepalingen in het [Wetboek van Strafrecht](#) inzake geheimhouding (geldend op 20 april 2016), te weten de artikelen [2](#) tot en met [8](#), [23](#), [272](#) en [273](#) (snellinkjes te vinden op internet);
- Ik heb kennis genomen van de informatie in het personeelshandboek BAR- Organisatie, welke te vinden is via het intranet (BAR-Plaza) > Weten & Regelen

dat ik de betekenis en het belang van die bepalingen heb begrepen.

#### Nadere uitleg:

#### Ondertekening medewerker

Plaats \_\_\_\_\_

Datum \_\_\_\_\_

Handtekening \_\_\_\_\_



## Toelichting

### 1. Geheimhouding

*In ieder geval worden als vertrouwelijk beschouwd: Persoonsgegevens, financiële gegevens, klantgegevens, aanbestedingsgegevens en contractgegevens. Daarnaast is vertrouwelijke informatie op schrift is te herkennen doordat er 'vertrouwelijk' op staat. Ook stempels of aantekeningen als 'geheim' en dergelijke kwalificeren een document als vertrouwelijk.*

*Ook niet-schriftelijke informatie kan een vertrouwelijk karakter hebben, zoals interne uitspraken van het college, management, discussies of verschillen van mening.*

### 2. Toegang tot gebouwen, apparatuur en kwetsbare ruimten

*Met locatie wordt bedoeld elk gebouw waarin een onderdeel van de gemeente is gevestigd, of een plaats waar medewerkers werkzaam zijn, dus ook bedrijfsterreinen, kunstwerken, vervoermiddelen, etc.*

*Toegangsmiddelen zijn bijvoorbeeld toegangspassen, sleutels, tags, toegangscode, passwords, apparatuur en software.*

*Voorbeelden van extra kwetsbare ruimten zijn: computer- en netwerkruimten, ruimten met communicatieapparatuur zoals telefooncentrales, archiefruimten, ruimten met toegang tot bedrijfsvoeringsgegevens ruimten waarin zich kluizen bevinden, werkplaatsen waar kostbare apparatuur aanwezig is.*

### 3. Omgang informatie

*In ieder geval worden als vertrouwelijk beschouwd: persoonsgegevens, financiële gegevens, klantgegevens, aanbestedingsgegevens en contractgegevens. Voorbeelden van mogelijke beveiligingsmaatregelen zijn: clean desk, afsluiten kasten, aanzetten schermbeveiliging tijdens afwezigheid, regelmatig wijzigen van wachtwoorden, niet uitlenen van apparatuur of gegevensdragers aan derden.*

### 4. Omgang bedrijfsmiddelen

*Voorbeelden van bedrijfsmiddelen zijn: computers, (mobiele) telefoons, kantoorbehoeften, laptops, beamers, vervoermiddelen zoals dienstauto of dienstfiets.*

*Voorbeelden van ongewenst gebruik van inter-/intranet en e-mail zijn het surfen naar dubieuze websites, het openen van e-mail van totaal onbekende afzenders dan wel e-mail met een vreemde bijlage, het downloaden van muziekbestanden of software zonder licentie, etc.*