

	VEILIGHEIDSREGIO ROTTERDAM RIJNMOND Integriteits- en Geheimhoudingsverklaring Bedrijven
---	---

Medewerker namens de organisatie:

Bedrijfsnaam :

naam en voorletters :

functie :

werkende voor
VRR organisatieonderdeel :

aard werkrelatie : ☐ Sw-medewerkers werkzaam op arbeidsovereenkomst
☐ uitzendkracht
☒ consultant (w.o. personeel detacheringbureaus)
☐ stagiair
☐ schoonmaak-/catering-/onderhoudsbedrijven
☐ inhuurkracht op projectbasis ingehuurd (technisch personeel e.d.)
☒ overige

Verklaart het volgende:

1. Geheimhouding

zie de toelichting

Ik verklaar geheim te houden alle informatie die onze organisatie gedurende onze werkzame periode ter kennis komt waarvan wij weet of vermoeden dat deze vertrouwelijk is. Persoonsgegevens, financiële gegevens, klantgegevens, aanbestedingsgegevens en contractgegevens beschouwen wij in ieder geval als vertrouwelijk. Wij verstrekken bewust of onbewust deze informatie niet aan anderen, ook niet aan niet belanghebbenden binnen de Veiligheidsregio Rotterdam Rijnmond, tenzij dit noodzakelijk is voor de uitoefening van de taak of wij daartoe wettelijk verplicht zijn. Bij twijfel nemen wij contact op met de opdrachtgever of de security-officer binnen de Veiligheidsregio Rotterdam Rijnmond.

2. Toegang tot gebouwen

zie de toelichting

Wij gebruiken de hulpmiddelen voor toegang tot locaties, apparatuur en ruimten van de Veiligheidsregio Rotterdam Rijnmond uitsluitend voor het doel waarvoor deze aan ons ter beschikking zijn gesteld.

Wij proberen niet om onbevoegd toegang te krijgen tot locaties van de Veiligheidsregio Rotterdam Rijnmond. Voor ons bestemde toegangsmiddelen behouden wij voor onszelf en geven wij 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 ons verstrekte toegangspas, sleutels, tags, toegangscodes, apparatuur of software, stellen wij de daartoe aangewezen personen binnen het organisatieonderdeel waarvoor wij werkzaam ben onmiddellijk daarvan in kennis.

Wij houden ons aan de regels die per locatie van de Veiligheidsregio Rotterdam Rijnmond zijn gesteld ten aanzien van het ontvangen en begeleiden van bezoekers.

3. Omgang informatie

zie de toelichting

Wij laten geen stukken onbeheerd achter, ook niet op een bureau, in een ruimte of werkplek waar wij werken, waarvan wij weet of zouden kunnen weten dat deze vertrouwelijk zijn.

Wij houden mij op onze (thuis)werkplek aan de regels voor de beveiliging van informatie.

Documenten, e-mails en overige zaken die niet voor ons bestemd zijn, zenden wij onmiddellijk door aan het juiste adres of retourneren wij deze aan de afzender. Is het juiste adres noch de afzender bekend, dan vernietigen wij ze.

4. Omgang bedrijfsmiddelen

zie de toelichting

Wij gaan zorgvuldig om met alle ons ter beschikking gestelde bedrijfsmiddelen, zowel op onze werkplek als elders waar wij bedrijfsmiddelen gebruik. Wij houden ons aan de "Regeling ICT- en informatiegebruik VRR 2023" en de huisregels van het organisatieonderdeel. Wij laten geen waardevolle bedrijfsmiddelen onbeheerd achter op onze werkplek of elders waar wij bedrijfsmiddelen gebruiken.

5. Integriteit

Wij gedragen ons integer, wat in ieder geval inhoudt dat wij ons houden aan de interne regels over integriteit¹ en de huisregels van het organisatieonderdeel.

Als wij een misstand constateren, melden wij deze in eerste instantie bij onze opdrachtgever of diens superieur.

6. Omgangsvormen

Wij houden ons aan correcte omgangsvormen en wij houden ons aan het "Protocol ongewenst gedrag", de interne regels over omgangsvormen en de huisregels van het organisatieonderdeel.

Krijgen wij te maken met ongewenste omgangsvormen dan kunnen wij de opdrachtgever raadplegen, dan wel een van de vertrouwenspersonen bij de Veiligheidsregio Rotterdam Rijnmond.

Wordt het probleem niet opgelost dan kunnen wij een klacht indienen bij de klachtencommissie (Landelijke Klachtencommissie Ongewenst Gedrag voor de Decentrale Overheid).

¹ [Gedragscode van de Veiligheidsregio Rotterdam Rijnmond](#)

En verklaart verder

- in kennis te zijn gesteld van de inhoud van dit formulier;
- zich te zullen houden aan alle in dit formulier genoemde (spel)regels;
- bekend te zijn met de verplichting aangifte te doen van elke schending van de geheimhoudingsplicht. Dit onverminderd hetgeen is bepaald in artikel 162 van het Wetboek van Strafvordering.

Ondertekening medewerker namens de organisatie

plaats :

datum :

handtekening : _____

Gezien Veiligheidsregio Rotterdam Rijnmond

plaats :

datum :

naam :

functie :

handtekening : _____

Toelichting

1. Geheimhouding

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 de directieraad, discussies of verschillen van mening.

2. Toegang tot gebouwen, apparatuur en kwetsbare ruimten

Met locatie wordt bedoeld elk gebouw waarin een onderdeel van de Veiligheidsregio Rotterdam Rijnmond 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: computerruimten, netwerkrumten, ruimten met communicatieapparatuur zoals telefooncentrales, archiefruimten, ruimten met toegang tot bedrijfsvoeringgegevens, ruimten waarin zich kluizen bevinden, werkplaatsen waar kostbare apparatuur aanwezig is.

3. Omgang informatie

Zoals onder het kopje “Geheimhouding” al is aangegeven worden in ieder geval 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, usb-sticks en/of andere opslagmiddelen aan derden.

4. Omgang bedrijfsmiddelen

Voorbeelden van bedrijfsmiddelen zijn: computers, (mobiele) telefoons, kantoorbehoeften, laptops, beamers, vervoermiddelen zoals bedrijfsauto of bedrijfsfiets.

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