



VEILIGHEIDSREGIO ROTTERDAM RIJNMOND

INTEGRITEITS- EN GEHEIMHOUDINGSVERKLARING

naam en voorletters :

functie :

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 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 Veiligheidsregio Rotterdam Rijnmond, 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 security-officer binnen de Veiligheidsregio Rotterdam Rijnmond.

2. Toegang tot gebouwen

zie de toelichting

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

Ik probeer niet om onbevoegd toegang te krijgen tot locaties van de Veiligheidsregio Rotterdam Rijnmond. 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, toegangscode, 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 Veiligheidsregio Rotterdam Rijnmond zijn gesteld ten aanzien van het ontvangen en begeleiden van bezoekers.

3. Omgang informatie

zie de toelichting

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.

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.

4. Omgang bedrijfsmiddelen

zie de toelichting

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 "Regeling internet en e-mailgebruik 2012¹ 2"

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 integriteit³ en de huisregels van mijn organisatieonderdeel.

Als ik een misstand constateer, meld ik deze in eerste instantie bij mijn opdrachtgever of diens superieur. Als ik anoniem wil blijven, maak ik gebruik van de Regeling Meldingen Integriteitschendingen en meld ik een geconstateerde misstand bij een van de vertrouwenspersonen integriteit bij de Veiligheidsregio Rotterdam Rijnmond. Bij twijfel raadpleeg ik de integriteitfunctionaris.

6. Omgangsvormen

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

Krijg ik te maken met ongewenste omgangsvormen dan kan ik mijn opdrachtgever raadplegen, dan wel een van de vertrouwenspersonen bij de Veiligheidsregio Rotterdam Rijnmond.

Wordt het probleem niet opgelost dan kan ik een klacht indienen bij de klachtencommissie

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.

¹ Van de gemeente Rotterdam

² Of geldende regeling van de Veiligheidsregio Rotterdam Rijnmond indien ingevoerd

³ Gedragscode van de Veiligheidsregio Rotterdam Rijnmond

Ondertekening medewerker

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's, 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, floppy's of cd's 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 totaal onbekende afzenders dan wel e-mail met een vreemde bijlage, het downloaden van muziekbestanden of software zonder licentie, etc.