

De gedragscode Signum Interfocus Riskmanagement en de werkmaatschappijen (Signum Interfocus Nederland, Signum Interfocus Deutschland en Metis International)

Middels de gedragscode geeft de organisatie aan wat van de medewerkers verwacht wordt. Indien onduidelijk is wat wel en niet mag, dient de medewerker met zijn leidinggevende te overleggen. Indien de medewerker de bepalingen van de gedragscode schendt, kunnen maatregelen tegen hem getroffen worden, startende met een waarschuwing tot in het uiterste geval ontslag op staande voet (al dan niet met het verhalen van de ontstane schade).

1. Werkingsfeer

De gedragscode is van toepassing op alle medewerkers van de organisatie.

2. Algemene uitgangspunten

- 2.1 De medewerkers behoren wettelijke voorschriften en algemeen aanvaarde gedragsregels, zoals deze gedragscode, na te leven.
- 2.2 De gedragscode bevat de belangrijkste aspecten van het integriteitsbeleid van de organisatie. Periodiek wordt getoetst of de gedragscode overeenstemt met de praktijk.
- 2.3 In die gevallen dat de gedragscode niet duidelijk is, of dat een medewerker wenst af te wijken van de gedragscode, moet deze contact opnemen met zijn leidinggevende. De leidinggevende moet bepalen of de afwijking gerechtvaardigd is.
- 2.4 De gedragscode wordt aan elke medewerker bij indiensttreding uitgereikt en is voor elke medewerker te downloaden via het bedrijfsnetwerk.
- 2.5 De gedragscode bevat richtlijnen en geboden hoe door een medewerker gehandeld moet worden. Voor kennisgeving van de administratieve procedures wordt verwezen naar het bedrijfsnetwerk.

3 Procedures

- 3.1 De medewerker vervult geen andere functies dan hem zijn opgedragen in de functiebeschrijving.
- 3.2 De medewerker spant niet samen met andere functionarissen om zodoende de procedures te omzeilen (samenspanning).
- 3.3 De medewerker stelt zich op de hoogte van de bestaande procedures en de wijzigingen daarin. De organisatie verplicht zich tot het regelmatig bijwerken van de procedures en wijzigingen bekend te maken.
- 3.4 Medewerkers moeten op de hoogte zijn van procedures die specifiek voor hun functie gelden.

4 Nevenwerkzaamheden

- 4.1 Indien een medewerker nevenwerkzaamheden wil gaan uitvoeren moet hij vooraf toestemming vragen aan zijn leidinggevende.
- 4.2 Voor het melden van nevenfuncties gaat het om het raken van het belang van de organisatie. Niet van belang is of een vergoeding voor de nevenwerkzaamheden wordt ontvangen.
- 4.3 De organisatie verleent de medewerker toestemming voor de nevenfunctie, als het belang van de organisatie niet geraakt wordt.
- 4.4 Als het belang van de organisatie wel geraakt wordt, wordt onderzocht op welke wijze aan de bezwaren van de organisatie tegemoet gekomen kan worden en de medewerker toch de nevenfunctie kan vervullen. Is dit niet mogelijk, dan krijgt de medewerker geen toestemming voor het vervullen van de nevenfunctie.
- 4.5 De medewerker die toestemming heeft gekregen voor het vervullen van een nevenfunctie meldt iedere wijziging van omstandigheden die van invloed kan zijn op de verleende toestemming aan zijn leidinggevende.
- 4.6 De medewerker moet zijn leidinggevende op de hoogte stellen als hij werkend voor de organisatie geconfronteerd wordt met partijen die hij vanuit zijn nevenfunctie kent (belangenverstrengeling).

5 Financieel belang

- 5.1 De medewerker meldt financiële belangen in ondernemingen waarmee de organisatie zaken doet, aan zijn leidinggevende.
- 5.2 De medewerker die familie- of vriendschapsbetrekkingen of andere persoonlijke betrekkingen heeft met een aanbieder van diensten aan de organisatie, onthoudt zich van deelname aan de besluitvorming over de betreffende opdracht.

6 Relatiegeschenken

- 6.1 Geschenken en giften die een medewerker uit hoofde van zijn functie ontvangt, worden gemeld en geregistreerd en zijn eigendom van de organisatie.
- 6.2 In afwijking van het vorige lid hoeven geschenken of giften die minder dan 50 euro waard zijn, niet gemeld te worden en mag de ontvanger deze houden. Hierbij geldt dat per onderneming maximaal eenmaal per jaar een geschenk mag worden verstrekt aan een medewerker.
- 6.3 De organisatie stelt via de leidinggevenden en via intranet formulieren aan de medewerkers ter beschikking waarop melding kan worden gedaan van de ontvangen geschenken.
- 6.4 Schenkingen boven 50 euro mogen alleen met toestemming van de leidinggevende worden geaccepteerd.
- 6.5 Indien een schenking niet wordt geaccepteerd wijst de medewerker de schenker op de gedragscode van de organisatie, waarin is opgenomen waarom de schenking niet mag worden geaccepteerd.
- 6.6 Geschenken en giften mogen niet op het huisadres worden ontvangen.
- 6.7 De medewerker neemt van een aanbieder van diensten of goederen geen faciliteiten of diensten aan die zijn onafhankelijke positie ten opzichte van de aanbieder kunnen beïnvloeden (omkoping).
- 6.8 De medewerker verstrekt geen geschenken of giften om zijn eigen positie of die van de organisatie (onrechtmatig) te bevoordelen (steekpenningen).
- 6.9 Geschenken worden niet aangenomen in ruil voor een tegenprestatie.
- 6.10 Aanbiedingen voor privé-diensten of kortingen op privé-goederen worden niet geaccepteerd.

7 Excursies, werkbezoeken, studiereizen, congressen, lunches, diners, recepties

- 7.1 Excursies, werkbezoeken, studiereizen, congressen, lunches, diners *en/of* recepties moeten functioneel zijn en in het belang van de organisatie.
- 7.2 Elke aanbieding moet gemeld worden aan de leidinggevende, ook al wordt deze niet geaccepteerd.
- 7.3 Voor het accepteren van een uitnodiging moet toestemming van een leidinggevende gevraagd worden.
- 7.4 De uitnodiging moet binnen de grenzen van de redelijkheid liggen.

8 Persoonlijk gebruik

- 8.1 De medewerker mag geen kantoorartikelen meenemen voor eigen gebruik.
- 8.2 Het gebruik van e-mail, internet, telefoon, kopieerapparaat e.d. voor privé moet beperkt blijven en mag het dagelijks functioneren van de medewerker niet belemmeren. Wat onder beperkt gebruik moet worden verstaan moet de medewerker afstemmen met zijn leidinggevende. Regels over het gebruik van internet en e-mail zijn gesteld in de daarvoor geldende gedragscode.
- 8.3 De telefoonvoorziening mag in geen enkel geval oneigenlijk worden gebruikt. Onder oneigenlijk gebruik wordt onder andere verstaan:
1. Overmatig privé gebruik, sms-gebruik en privé telefoongesprekken naar buitenlandse bestemmingen;
 2. Servicenummers met een pornografisch *en/of* seksueel karakter;
 3. Servicenummers met een spel *en/of* gok karakter;
 4. Servicenummers met een dating of chat karakter;
 5. Servicenummers met een beledigend of racistisch karakter;
 6. Doorverbinddiensten met als doel door te verbinden met telefoonnummers van één van bovenstaande categorieën.
- Voor de bovenstaande nummers 2-6 geldt dit voor zowel betaalde als niet betaalde diensten, en geldt tevens voor vergelijkbare servicenummers.
- Indien een werknemer een mobiele telefoon ter beschikking is gesteld, gelden onderstaande aanvullende regels:
1. Zonder voorafgaande toestemming, wordt de telefoon niet voor privé-doeleinden gebruikt.
 2. Zonder voorafgaande toestemming is het niet toegestaan om tijdens verblijf in het buitenland de telefoon te gebruiken.
 3. De telefoon mag zonder voorafgaande toestemming niet aan derden ter beschikking worden gesteld.
 4. In het geval van verlies *en/of* diefstal is de werknemer verplicht de werkgever hiervan direct op de hoogte te stellen. In het geval van diefstal is de werknemer tevens verplicht aangifte te doen bij de politie.
- 8.4 Het eigen gebruik van bedrijfsauto's is in beginsel niet toegestaan. Degenen die beschikbaar moeten zijn (oproepdiensten) mogen bedrijfsauto's gebruiken conform de

bedrijfsautoregeling van de organisatie.

8.5 De medewerker dient de door de organisatie ter beschikking gestelde middelen te behandelen volgens "goed huisvaderschap".

9 (Vertrouwelijke)informatie

9.1 De medewerker ruimt aan het einde van de dag zijn bureau op (*clean desk*) en bewaart gevoelige documenten achter slot en grendel.

9.2 De medewerker verstrekt geen vertrouwelijke informatie aan onbevoegde personen.

9.3 De medewerker mag informatie die hij vanuit zijn taakuitoefening heeft verkregen, niet ten eigen bate aanwenden.

9.4 De medewerker zorgt voor transparante vastlegging van zijn handelingen en neemt de interne afspraken mbt dossierprotocol in acht.

9.5 Er mag niet over vertrouwelijke zaken met de media worden gesproken.

9.6 De medewerker houdt zich aan hetgeen is opgenomen in de geheimhoudingsclausule van zijn arbeidsovereenkomst.

10 Declaraties

10.1 Uitgaven worden uitsluitend vergoed als de hoogte en de functionaliteit ervan kunnen worden aangetoond door de medewerker en de uitgave niet ondoelmatig is.

10.2 Een uitgave is functioneel als de uitgave is gedaan in het belang van de organisatie en de uitgave voortvloeit uit de functie.

10.3 Een uitgave is doelmatig als deze in overeenstemming is met functie van de medewerker en het doel dat met de uitgave moet worden bereikt.

10.4 De medewerker mag geen onkosten declareren die reeds vergoed zijn.

10.5 De medewerker moet de declaratie indienen middels een declaratieformulier, waarachter de betalingsbewijzen zijn gevoegd. De declaratie moet uiterlijk één maand na de uitgave zijn ingediend.

10.6 De medewerker die onkosten wil declareren moet het declaratieprotocol in acht nemen.

11 Facturen

11.1 De medewerker moet vooraf toestemming vragen aan de budgethouder of hij kosten mag laten factureren aan de organisatie.

11.2 De uitgave moet functioneel en doelmatig zijn (zie 10.1, 10.2 en 10.3). Privékosten en boeten moeten worden terugbetaald.

12 Creditcards

12.1 Als een medewerker een creditcard wil gebruiken, dan moet hij hiervoor een aanvraag indienen bij zijn leidinggevende, waarin de noodzaak wordt toegelicht.

12.2 De creditcard wordt voor binnenlands gebruik zo veel mogelijk beperkt.

12.3 Uitgaven met de creditcard moeten schriftelijk worden verantwoord en onderbouwd met betalingsbewijzen.

12.4 De uitgave moet functioneel en doelmatig zijn (zie 10.1, 10.2 en 10.3). Privékosten en boeten moeten worden terugbetaald.

13 Reizen

13.1 De medewerker die een buitenlandse reis wil ondernemen, moet dit van tevoren aanvragen bij zijn leidinggevende. Hierbij moeten de onkosten, het doel van de reis, de afstand, het vervoersmiddel, de omvang van het gezelschap en de duur van de reis uitgewerkt worden.

13.2 Uitnodigingen voor reizen, werkbezoeken en dergelijke, op kosten van derden moeten altijd worden voorgelegd aan de leidinggevende.

13.3 Voor het meereizen van de partner, kinderen of andere mensen die niet werken voor de organisatie, al dan niet op kosten van de uitnodigende organisatie, moet de medewerker toestemming vragen aan zijn leidinggevende.

13.4 De medewerker mag een reis verlengen, zij het dat de aanvullende kosten en tijdsverlof voor zijn rekening komen.

13.5 De medewerker mag de gemaakte onkosten conform het declaratiebeleid declareren.

14 Veiligheidsbeleid

14.1 De medewerker moet zich vergewissen van het veiligheidsbeleid van de organisatie.

14.2 Sleutels en wachtwoorden zijn persoonlijk aan de medewerker overhandigd en toegekend en mogen niet uitgeleend worden.

14.3 Verlies van sleutels moet direct aan de leidinggevende gemeld worden.

15 Arbeidsongeschiktheid

15.1 Een zieke medewerker heeft een aantal verplichtingen. Zo dient hij het verzuim op dezelfde dag voor aanvang van zijn dienst, of zo spoedig als mogelijk, te melden bij de leidinggevende.

Vervolgens dient hij zich te houden aan de regels die omschreven zijn in het kader van Wet Werk en Inkomen naar Arbeidsvermogen (WIA).

16. Disfunctioneren

16.1 Indien een medewerker niet functioneert conform de gestelde functie-eisen en/of vastgestelde competenties, of gedrag vertoont waardoor de functie niet op een acceptabele wijze wordt uitgeoefend en begeleiding niet heeft geleid tot verbetering, heeft dit consequenties voor de medewerker.

Daarbij bestaat de mogelijkheid van het plaatsen in een andere functie, het plaatsen in een andere functiegroep of het beëindigen van de arbeidsovereenkomst.

Bij plaatsing in een lagere functiegroep als gevolg van eigen toedoen, wegens onbekwaamheid of op eigen verzoek de medewerker met ingang van de daarop volgende periode in de bijbehorende lagere salarisschaal wordt ingedeeld. Het salaris wordt hierbij in negatieve zin aangepast.

17 Sancties

17.1 Het schenden van de gedragscode zal leiden tot het treffen van disciplinaire maatregelen. Dit kan variëren van een waarschuwing tot en met ontslag. De aard van de op te leggen sancties hangt af van de bijzonderheden van het geval. In geval van disciplinaire bestraffing zal de werkgever de daarvoor geldende procedures volgen.

17.2 Ter zake van het gebruik van het internet en e-mail geldt de gedragscode internet.

18 Slotbepaling

18.1 Deze regeling treedt in werking op 1 januari 2009.

Hummelo,

Getekend voor gezien en akkoord,

Medewerker

Gedragscode voor het gebruik van e-mail en internet voor Signum Interfocus Riskmanagement en werkmaatschappijen (Signum Interfocus Nederland, Signum Interfocus Deutschland en Metis International)

1. Doel van de afspraken

1.1 Deze regeling geeft de wijze aan waarop in de organisatie wordt omgegaan met e-mail en internetgebruik. Deze omvat gedragsregels ten aanzien van verantwoord e-mail en internetgebruik en regels over de wijze waarop controle op e-mail en internetgebruik plaatsvindt.

1.2 De controle op persoonsgegevens over e-mail en internetgebruik vindt plaats met als doel:

Dat in een integere organisatie management en medewerkers zorgvuldig met de bedrijfsmiddelen, met elkaar en met de belangen van externen dienen om te gaan
De continuïteit van de technische infrastructuur te waarborgen
Verstoring van bedrijfsprocessen en andere (financiële) schade tegen te gaan en om toezicht te houden op de naleving van de gedrags- en gebruiksregels door de gebruiker

2 Algemene uitgangspunten

2.1 De controle op e-mail en internetgebruik zal overeenkomstig deze afspraak uitgevoerd worden. Indien er zich situaties voordoen waarin deze regeling niet voorziet, zal conform het arbeidsrechtelijk kader en de Wet bescherming persoonsgegevens (WBP) gehandeld worden.

2.2 Gestreefd wordt naar een goede balans tussen controle op verantwoord e-mail en internetgebruik en bescherming van de privacy van werknemers op de werkplek.

2.3 Persoonsgegevens over e-mail en internetgebruik worden niet langer bewaard dan noodzakelijk, met een maximum bewaartermijn van 6 maanden.

2.4 De werkgever treft voorzieningen over de positie en integriteit van de systeembeheerder en de controle daarop.

3 E-mailgebruik

3.1 Het versturen van e-mailberichten moet voldoen aan de volgende voorwaarden:

- Verstuur E-mail gericht en beperk u tot de werkelijk belanghebbenden.
- Controleer uw mail regelmatig, verwerk deze direct en archiveer bestanden regelmatig.
- Maak gebruik van ter zake doende Onderwerp regels.
- Wees voorzichtig met het reageren op E-mail die gericht zijn aan een grote groep gebruikers.
- Voor het versturen en ontvangen van persoonlijke e-mailberichten verstrekt de

onderneming een apart e-mailadres.

- Werknemers mogen incidenteel en kortstondig het e-mailsysteem gebruiken voor het ontvangen en versturen van persoonlijke e-mailberichten mits dit niet storend is voor de dagelijkse werkzaamheden en het computernetwerk.
- Een correcte vermelding van afzender;
- Het meesturen van een disclaimer;

3.2 Het is niet toegestaan om:

- Berichten anoniem of onder een fictieve naam te versturen
- Berichten of bestanden met bijlage(n) met dreigende, beledigende, seksueel getinte, racistische dan wel discriminerende en ketting mail te verzenden, op te slaan of door te sturen
- Iemand via digitale en/of elektronische weg lastig te vallen.
- Niet zakelijke bijlagen te versturen > 1024Kb.
- E-mail te gebruiken voor persoonlijke advertenties

4. Internetgebruik

4.1 Werknemers hebben het recht om het internet te gebruiken de leidinggevende kan dit recht ook altijd weer intrekken.

4.2 De werkgever kent de gebruiker een gebruikersnaam en wachtwoord toe, deze zijn persoonsgebonden en mogen niet aan anderen worden doorgegeven.

4.3 De volgende gedragsregels zijn van toepassing:

- Voor het ondertekenen van schriftelijke correspondentie, het vertegenwoordigen van de organisatie en het verzenden van post (zoals correct taalgebruik) zijn ook van toepassing op e-mail en andere toepassingen (zoals nieuwsgroepen, telefoneren via internet).
 - Met betrekking tot vertrouwelijke gegevens en bedrijfsgevoelige informatie. Deze gegevens mogen niet zonder toestemming van de directie naar buiten de organisatie worden verstuurd. Het berichtenverkeer hoort dan versleuteld te verlopen.
 - Voor het ondertekenen van stukken. Indien gebruik wordt gemaakt van elektronische correspondentiemiddelen, dan mogen deze op geen enkele wijze worden voorzien van gedigitaliseerde handtekeningen. Alleen bij afdoende beveiligingsmaatregelen en met instemming van de directie kan worden afgeweken van deze regel.
 - Het ongeoorloofd toegang verschaffen tot niet openbare bronnen op het internet is niet toegestaan.
 - Het downloaden van software en applicaties is niet toegestaan, tenzij vooraf schriftelijke toestemming is verleend door de systeembeheerder. Deze toestemming wordt alleen verleend, als wordt voldaan aan de geldende rechten en eventuele licenties worden betaald. Gedownloade software en applicaties moeten op virussen zijn gescand voor gebruik.
 - Het is niet toegestaan inkomende privé-berichten te genereren door deel te nemen aan niet-zakelijke nieuwsgroepen, abonnementen op e-zines, nieuwsbrieven en dergelijke.
 - Het is niet toegestaan om voor persoonlijke doeleinden internet te gebruiken. Bij persoonlijk gebruik van internet moet onder andere worden gedacht aan het spelen of downloaden van spelletjes, muziekbestanden, winkelen, gokken of deelnemen aan kansspelen en het bezoeken van chat-/babbelboxen of vergelijkbare activiteiten.
 - Het bezoeken, bekijken en/of downloaden van sites die pornografisch, racistisch, discriminerend, beledigend of aanstootgevend materiaal bevatten is niet toegestaan;
 - Opzettelijk informatie zonder toestemming te veranderen of te vernietigen, waartoe men via internet toegang heeft verkregen is niet toegestaan.
- 4.4 Het is ook anderszins niet toegestaan op internet in strijd met de wet of onethisch te handelen. Onbedoelde inbreuken op beveiliging, vanuit de organisatie of vanuit de buitenwereld, dient u aan de leidinggevende afdeling te melden.

5. Controle

5.1 Controle op e-mail en internetgebruik vindt slechts plaats in het kader van in artikel 1.2 genoemde doelen. Deze doeleinden stellen beperkingen aan de omvang en wijze van controle:

- de registratie wordt door de (interne en/of externe) leverancier van de diensten alleen verstrekt aan de directie

5.2 Controle vindt op de volgende wijze plaats:

Controle vindt in beginsel plaats op het niveau van getotaliseerde gegevens die niet herleidbaar zijn tot individuele personen. Indien een werknemer of een groep werknemers ervan wordt verdacht de regels te overtreden, kan gedurende een vastgestelde (korte) periode gerichte controle plaatsvinden.

Controle beperkt zich in principe tot verkeersgegevens van het gebruik van e-mail en internet. Alleen bij zwaarwegende redenen vindt er controle op de inhoud plaats.

'Verboden' e-mail en internetgebruik wordt zo veel mogelijk softwarematig onmogelijk gemaakt. Overige controle vindt slechts steekproefsgewijs plaats.

In het kader van begeleiding en/of individuele beoordelingen vindt er steekproefsgewijs controle plaats van zakelijke e-mailberichten zoals overeengekomen met de individuele werknemer.

Voor het tegengaan van virussen en andere schadelijke programma's, in het kader van systeem- en netwerkbeveiliging, wordt het e-mail en internetgebruik op geautomatiseerde wijze gecontroleerd.

Controle op het uitlekken van bedrijfsgeheimen vindt plaats op basis van steekproefsgewijze contentfiltering. Een verdacht bericht wordt apart gezet voor nader onderzoek.

Controle in het kader van het voorkomen van negatieve publiciteit vindt plaats op basis van contentfiltering. Verdachte berichten worden geautomatiseerd teruggestuurd naar de afzender en 'verboden' sites geblokkeerd.

Controle in het kader van het tegengaan van seksuele intimidatie vindt op geautomatiseerde wijze plaats. Verdachte berichten worden geautomatiseerd teruggestuurd naar de afzender.

Controle in het kader van het tegengaan van 'verboden gebruik' vindt in beginsel geanonimiseerd en slechts steekproefsgewijs plaats.

5.2 Werknemers ten aanzien van wie geconstateerd is dat zij zich niet aan deze regeling houden, worden zo spoedig mogelijk door de leidinggevende op hun gedrag aangesproken.

6. Rechten van de betrokkenen

6.1 De werkgever informeert de werknemers voorafgaand aan de invoering van de regeling over controle op e-mail en internetgebruik, omtrent de doeleinden, de aard van de gegevens, de omstandigheden waaronder zij verkregen zijn en de inhoud van deze regeling. (zie artikel 33, WBP)

6.2 De werknemer kan zich tot de werkgever wenden met het verzoek om een volledig overzicht van zijn verwerkte persoonsgegevens. Het verzoek wordt binnen 4 weken beantwoord. (zie artikel 35, WBP)

6.3 De werknemer kan de werkgever verzoeken zijn persoonsgegevens te verbeteren, aan te vullen, te verwijderen of af te schermen indien deze feitelijk onjuist zijn, voor het doel onvolledig of niet ter zake dienend, dan wel in strijd met een wettelijk voorschrift worden verwerkt. Het verzoek wordt binnen 4 weken beantwoord. (zie artikel 36, WBP)

6.4 De werknemer kan bij de werkgever verzet aantekenen tegen de verwerking van zijn persoonsgegevens in verband met bijzondere persoonlijke omstandigheden. De werkgever oordeelt binnen 4 weken na ontvangst van het verzet of dit gerechtvaardigd is. Indien de werkgever het verzet gerechtvaardigd acht, beëindigt hij terstond de verwerking. (zie artikel 40, WBP)

7. Slotbepaling

7.1 De werkgever kan deze regeling wijzigen.

Deze wijzigingen worden schriftelijk vastgelegd en voorafgaand aan de invoering aan de werknemers bekend gemaakt.

7.2 Deze regeling wordt jaarlijks geëvalueerd door de werkgever en de werknemers.

7.3 Deze regeling treedt in werking op 1 januari 2009.

Hummelo,

Getekend voor gezien en akkoord,

Medewerker