VEILIGHEIDSREGIO
MIDDEN- EN WEST-BRABANT

BLAD GEMEENSCHAPPELIJKE REGELING

Nr. 1074
16 december
2021

Officiële uitgave van de gemeenschappelijke regeling Veiligheidsregio Midden- en West-Brabant

Gedragscode internet en e-mailgebruik Veiligheidsregio Midden- en West-Brabant

Het Dagelijks Bestuur van de Veiligheidsregio Midden- en West-Brabant,

gelet op:

- artikel 11.2 lid 3 Aanpassingswet Wnra jo artikel 125 ter Ambtenarenwet 2017 (goedwerkgevers- en werknemerschap);
- artikel 11.2 lid 3 Aanpassingswet Wnra jo. artikel 125 quater Ambtenarenwet 2017 (gedragscode);
- de Algemene verordening gegevensbescherming (AVG) (bescherming persoonsgegevens);
- artikel 27, lid 1 onder k en l van de Wet op de ondernemingsraden (instemming ondernemingsraad);

overwegende dat:

- De Veiligheidsregio Midden- en West-Brabant en haar werknemers zich ten opzichte van elkaar dienen te gedragen als een goed werkgever en een goed werknemer;
- de Veiligheidsregio Midden- en West-Brabant aan degenen die bij haar organisatie werkzaam zijn internet en e-mailfaciliteiten ter beschikking stelt om met behulp daarvan hun functie of ambt uit te oefenen
- het gewenst is een gedragscode vast te stellen waarin naast regels voor internet- en e-mailgebruik eveneens regels zijn opgenomen voor het vastleggen en monitoren van dit gebruik;
- dat de Ondernemingsraad heeft ingestemd met het voorgenomen besluit tot het vaststellen van de ‘Gedragscode internet- en e-mailgebruik Veiligheidsregio Midden- en West-Brabant’;

B E S L U I T :

Vast te stellen de volgende ‘Gedragscode internet- en e-mailgebruik Veiligheidsregio Midden- en West-Brabant’:

1. Werkingssfeer
De gedragscode "Internet en e-mailgebruik" is van toepassing op personen in dienst van of werkzaam voor de Veiligheidsregio Midden- en West-Brabant, inclusief bestuurders voor zover die gebruik maken van de centrale internet-en e-mailfaciliteiten van de Veiligheidsregio Midden- en West-Brabant, hierna te noemen gebruikers.

2. Uitgangspunten
Voor het gebruik van internet- en e-mailfaciliteiten gelden de volgende uitgangspunten:

a. Gebruik van internet- en e-mailfaciliteiten impliceert dat de gebruiker zich overeenkomstig de inhoud en de strekking van deze gedragscode zal gedragen;
b. Iedere gebruiker is zelf verantwoordelijk voor zijn/haar internet en e-mailgebruik en kan hierop door zijn leidinggevenden worden aangesproken;
c. Gestreefd wordt naar een goede balans tussen controle op verantwoord internet- en e-mailgebruik en bescherming van de privacy van de gebruiker;
d. De controle op internet- en e-mailgebruik zal overeenkomstig deze gedragscode worden uitgevoerd. Indien er zich situaties voordoen waarin deze regeling niet voorziet, zal conform het arbeidsrechtelijk kader en de AVG en in overleg met de ondernemingsraad gehandeld worden;
e. Persoonsgegevens over internet- en e-mailgebruik worden niet langer bewaard dan noodzakelijk;
f. De werkgever treft voorzieningen over de positie en integriteit van de systeembeheerder en/of afdeling ICT en de controle daarop.
g. Bij het internet- en e-mailgebruik gelden, voor zover van toepassing, ook de 5 gouden regels die zijn opgesteld in het kader van informatieveiligheid.

3. Doel
Deze gedragscode bevat regels ten aanzien van een verantwoord internet- en e-mailgebruik, regels over de wijze waarop controle op internet- en e-mailgebruik kan plaatsvinden en regels over de bescherming van de privacy van de gebruiker.

4. Internet- en e-mailgebruik

1. Het internet- en e-mailsysteem wordt aan de gebruiker voor zakelijk gebruik beschikbaar gesteld. Gebruik is derhalve verbonden aan taken die voortvloeien uit ambt of functie.
2. Persoonlijk gebruik van het internet- en e-mailsysteem is toegestaan, mits dit niet storend is voor de dagelijkse werkzaamheden en/of het computernetwerk en dit geen verboden gebruik in de zin van artikel 5 en 6 oplevert.

5 . Verboden internetgebruik

1. Het is de gebruiker niet toegestaan:
   a. Onverminderd artikel 4, lid 1 op internet sites te bezoeken die pornografisch, racistisch, discriminerend, beledigend of anderszins aanstootgevend materiaal bevatten. Noch is het toegestaan dergelijk materiaal te downloaden;
   b. zich ongeoorloofd toegang tot niet openbare bronnen op internet te verschaffen;
   c. ongeautoriseerde software en applicaties te downloaden en/of te installeren;
   d. op internet onethisch of in strijd met de wet te handelen.

2. Bestellen via internet verloopt uitsluitend via de daartoe geautoriseerde budgethouder. Opgave van een creditcardnummer van een creditcard van de Veiligheidsregio Midden- en West-Brabant en / of machtiging voor automatische afschrijving van een bankrekening van de Veiligheidsregio Midden- en West-Brabant is niet toegestaan.

6. Verboden e-mailgebruik

Het is de gebruiker niet toegestaan het e-mailsysteem te gebruiken voor het verzenden van:

a. berichten met een pornografische, racistische, discriminerende, beledigende, of anderszins aanstootgevende inhoud;
b. berichten met een (seksueel) intimiderende inhoud;
c. berichten die (kunnen) aanzetten tot haat en/of geweld;

7. Voorwaarden voor controle

1. De controle op internet- en e-mailgebruik vindt uitsluitend plaats in het kader van:
   a. Voorkomen van negatieve publiciteit;
   b. Bescherming van bedrijfsgeheimen;
   c. Tegengaan van verboden internet en e-mailgebruik (zie artikel 5 en 6);
   d. Systeem en netwerkbeveiliging;
   e. Kosten en capaciteitsbeheersing.

2. Loggegevens kunnen voor analysedoeleinden worden gebruikt, mits deze zijn geanonimiseerd. Inzage in niet-geanonimiseerde loggegevens mag alleen plaatsvinden wanneer hier een gegronde reden voor is, zoals overtreden van de regels c.q. misbruik of een cyberaanval.
3. Indien een gebruiker of een groep gebruikers wordt verdacht van het overtreden van de regels c.q. misbruik, kan gedurende een vastgestelde (korte) periode gerichte controle plaatsvinden. Controle beperkt zich in beginsel tot verkeersgegevens van het internet- en e-mailverkeer. Slechts bij zwaarwegende redenen vindt controle op de inhoud plaats.
4. E-mailberichten van leden van de Ondernemingsraad onderling, van bedrijfsartsen en functionarissen met een vertrouwensfunctie worden niet gecontroleerd.
   Andere berichten van en naar leden van de Ondernemingsraad, berichten van en naar het ambtelijk secretariaat Ondernemingsraad en de leden van de door de Ondernemingsraad ingestelde commissies worden bij vermeende strijdigheid met de artikelen 5 en 6 slechts gecontroleerd op basis van procedureafspraken tussen de bestuurder en de voorzitter van de Ondernemingsraad.
5. De Veiligheidsregio Midden- en West-Brabant kan op voorhand bepalen dat bepaalde websites en/of diensten niet toegankelijk zijn en technisch moeten worden afgeschermd.

8. Controle

1. De controle ter voorkoming van negatieve publiciteit, ter voorkoming van het uitlekken van bedrijfsgeheimen, ter voorkoming van internet- en e- mailgebruik omschreven onder artikelen 5 en 6 en de controle in het kader van systeem- en netwerkbeveiliging vindt plaats op basis van contentfiltering.
2. De controle in het kader van kosten- en capaciteitsbeheersing vindt plaats op basis van geanonimiseerde loggegevens.

9. Procedure bij vermoeden

1. Bij een vermoeden van verboden gebruik zoals aangegeven in artikel 5 en 6 wordt dit door de leidinggevende zo spoedig mogelijk met de betrokken gebruiker besproken. De gebruiker krijgt daarbij de gelegenheid om het vermoeden te weerleggen en het internet- en e-mailgebruik te verantwoorden. De gebruiker wordt door zijn leidinggevende gewezen op de mogelijke consequenties van (voortzetting van) verboden internet- en e-mailgebruik. De leidinggevend maakt verslag op van de bespreking.
2. Bij een vermoeden van verboden gebruik zoals aangegeven in artikel 5 en 6 heeft de leidinggevende, nadat hij het vermoeden met de gebruiker heeft besproken het recht een schriftelijk verzoek te doen bij de het afdelingshoofd Informatisering, met een kopie naar de gebruiker, voor het samenstellen van een rapportage over de betreffende gebruiker. Na toestemming van de FG en de CISO schakelt het afdelingshoofd Informatisering een systeembeheerder in om het proces te begeleiden. Het onderzoek wordt uitgevoerd door een onafhankelijk extern bureau. De Functionaris Gegevensbescherming houdt toezicht op het proces. De aanvraag en het onderzoek dient door betrokkenen strikt vertrouwelijk te worden behandeld.

10. Overtredingen

Overtreding van de "Gedragscode internet en e-mailgebruik Veiligheidsregio Midden- en West-Brabant " kan worden aangemerkt als plichtsverzuim.

11. Rechten van de gebruiker

1. De Veiligheidsregio Midden- en West-Brabant informeert de gebruikers, omtrent de doeleinden, de aard van de gegevens, de omstandigheden waaronder zij verkregen zijn en de inhoud van deze regeling.
2. De gebruiker kan zich tot de Veiligheidsregio Midden- en West-Brabant wenden met het verzoek om een volledig overzicht van zijn verwerkte persoonsgegevens. Het verzoek wordt binnen 4 weken schriftelijk beantwoord.
3. De gebruiker kan de Veiligheidsregio Midden- en West-Brabant 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 schriftelijk beantwoord.
4. De gebruiker kan bij de Veiligheidsregio Midden- en West-Brabant verzet aantekenen tegen de verwerking van zijn gegevens in verband met bijzondere persoonlijke omstandigheden. Binnen 4 weken na ontvangst wordt dit verzoek beoordeeld. Indien het verzoek gerechtvaardigd wordt geacht, wordt de verwerking terstond beëindigd

Aldus vastgesteld te Tilburg, 24 november 2021

de voorzitter,
Th.L.N. Weterings

de secretaris.
J. Trijselaar

Bijlage 1 Toelichting:

Algemeen

Medewerkers maken veelvuldig gebruik van internet om hun taken uit te voeren. Verschillende internetsites worden bezocht om informatie te verkrijgen met betrekking tot werkzaamheden die moeten worden uitgevoerd. Ook wordt er veel gecommuniceerd over uit te voeren werkzaamheden via e-mailtoepassingen.

Zowel werkgever als werknemer dienen zich ten opzichte van elkaar te gedragen als goede werkgever en goed werknemer (artikel 125 ter Ambtenarenwet 2017). De werkgever dient daartoe onder andere zorg te dragen voor de totstandkoming van een gedragscode voor goed ambtelijk handelen (artikel 125 quater Ambtenarenwet 2017);

De gedragscode internet- en e-mailgebruik Veiligheidsregio Midden- en West-Brabant is op het gebied van het internet- en e-mailgebruik bedoeld als een uitwerking van de begrippen goed werkgever- en goed werknemerschap.

De gedragscode geeft gedragsregels voor het gebruik van de internet- en e-mailfaciliteiten waarvan de werknemer gebruik kan maken, voor het controleren van dit gebruik door de werkgever en voor de bescherming van de persoonsgegevens.

Artikelsgewijs

Artikel 1, 2 en 3
Deze artikelen waarin de werkingssfeer, de uitgangspunten en het doel van de gedragscode worden vermeld spreken voor zichzelf.

Artikel 4, 5 en 6
In deze artikelen worden de grenzen voor het internet- en e-mailgebruik aangegeven. De internet- en e-mailfaciliteiten zijn bedoeld voor het zakelijke gebruik.
Artikel 4 geeft echter aan dat persoonlijk gebruik onder voorwaarden is toegestaan.
Persoonlijk gebruik mag niet storend zijn voor de dagelijkse werkzaamheden, met andere woorden privé-gebruik dient niet van je werktijd af te gaan en mag het tijdig uitvoeren van je taken niet belemmeren.
Persoonlijke gebruik mag ook niet leiden tot een verstoring in het netwerk van de veiligheidsregio.
Tenslotte mag er geen sprake zijn van verboden gebruik zoals beschreven in de artikel 5 (internetgebruik) en artikel 6 (e-mailgebruik). De veiligheidsregio mag en wil als overheidslichaam niet met zaken die in deze artikelen worden benoemd geassocieerd worden
Artikel 5, lid 1 bepaalt dat het verboden is om internetsites te bezoeken die pornografisch, racistisch, discriminerend, beledigend of anderszins aanstootgevend materiaal bevatten. Uiteraard geldt dit niet voor zover dit logischerwijze verbonden is aan taken die voortvloeien uit je ambt of functie (zie artikel 4, lid 1). Er kan daarbij bijvoorbeeld worden gedacht aan toezichthouden brandveiligheid bij toezicht op een prostitutie-inrichting of aan het maken van een omgevingsanalyse in het kader van crisisbeheersing. Het bezoek van bedoelde sites moet dan uiteraard wel deugdelijk kunnen worden gemotiveerd en verantwoord in het kader van werkzaamheden voor de veiligheidsregio.
Artikel 5, lid 2 verbied het gebruik van creditcard en machtiging automatische afschrijving bij bestelllingen via internet. Indien dit tot onoverkomelijke praktische problemen leidt dient de afdeling Financiën te worden ingeschakeld, die voor een oplossing kunnen zorgen.
Artikel 6 verbiedt het gebruik van e-mail voor het zenden van berichten met een pornografische, racistische, discriminerende, beledigende of anderszins aanstootgevende inhoud. Ook het verzenden van berichten met een (seksueel) intimiderende inhoud of berichten die aanzetten tot haat en/of geweld is verboden. Iedere werknemer dient te beseffen dat de mogelijkheid bestaat dat hij later kan worden aangesproken op de verzonden berichten. Mocht dit zich voordoen dan krijgt de werknemer uiteraard alle gelegenheid om zijn zienswijze over de inhoud van het bericht te geven c.q. te motiveren waarom een bericht is verstuurd voordat er eventuele verdere stappen worden genomen (zie ook artikel 8, lid 4).

Artikel 7, 8, 9 en 10
In de artikel 7, 8 , 9 en 10 worden regels gesteld voor de controle door de werkgever en de mogelijke gevolgen voor de werknemer.
In artikel 7 zie je met welk doel controles kunnen worden uitgevoerd en welke voorwaarden gelden voor de uitvoering van controles. Pas indien er echt sprake is van een vermoeden van het overtreden van de regels c.q. misbruik kan een gerichte controle plaatsvinden. Deze zal in principe alleen betrekking hebben op het inzage van logggevens, maar bij zwaarwegende redenen kan ook controle op de inhoud

plaatsvinden. Denk daarbij bijvoorbeeld aan een vermoeden van betrokkenheid bij kinderporno of andere strafbare zaken.
In artikel 8 is verder uitgewerkt welke controles kunnen worden uitgevoerd voor de verschillende doelen benoemd in artikel 7, lid 1.
In artikel 9 is de procedure geschetst indien er een vermoeden van overtreding van de gedragscode bestaat. Allereerst zal een leidinggevende de gebruiker aanspreken en het principe van hoor en wederhoor toepassen en daarbij aangeven wat de consequenties kunnen zijn (van toepassing voor geconstateerd verboden gebruik als voor het voortzetten van verboden gebruik). Leidinggevende maakt een verslag op van het gesprek. Dit verslag wordt als vertrouwelijk opgenomen in het personeelsdossier. Mede afhankelijk van het gesprek tussen leidinggevende en gebruiker kan leidinggevende besluiten om een schriftelijk verzoek te doen bij het afdelingshoofd informatisering om een rapportage op te stellen over het internet- en e-mailgebruik van betrokkene. Het onderzoek wordt uitgevoerd door een onafhankelijk extern bureau. De systeembeheerder voorziet de onderzoeker van informatie en de Functionaris Gegevensbescherming houdt toezicht op het proces.
In artikel 10 is, om buiten alle twijfel te stellen dat dit mogelijk is, opgenomen dat een overtreding van de gedragscode kan (uiteraard afhankelijk van de omstandigheden van het concrete geval) worden aangemerkt als plichtsverzuim.

Artikel 11
In artikel 11 zijn op basis van de Algemene verordening gegevensbescherming (AVG) rechten van de werknemers opgenomen ter bescherming van de persoonsgegevens.

Bijlage 2 5 gouden regels informatieveiligheid

1. *Informatie deel je, maar niet met iedereen*
   - o Let op wat je deelt en voorkom meelezen / meeluisteren
   - o Laat vertrouwelijke informatie niet onbeheerd achter
   - o Laat geen printjes liggen bij de printer
   - o Gooi vertrouwelijke informatie die je niet meer nodig hebt in de beveiligde archiefbak
   - o Vergrendel je digitale werkplek bij afwezigheid

2. *Ga bewust om met mobiele apparatuur*
   - o Laat smartphones, tablets, laptops, USB-stick niet onbeheerd achter
   - o Gebruik (wachtwoord-)beveiliging
   - o Let op welke gegevens je deelt als je een app gebruikt
   - o Wees voorzichtig met het gebruik van openbare wifi

3. *Ga zorgvuldig om met internet, e-mail en social media*
   - o Verstrek geen informatie ongecontroleerd aan derden: weet met wie je handelt
   - o Klik niet op verdachte links of vreemde bijlagen
   - o Reageer niet op phising-, spam-, j unk- en kettingmails
   - o Wees je er van bewust wat je online zet
   - o Gedraag je sociaal en deel je trots

4. *Wachtwoorden zijn persoonlijk*
   - o Houd wachtwoord geheim
   - o Schrijf je wachtwoord niet op
   - o Deel wachtwoorden niet met anderen
   - o Geef wachtwoorden nooit ‘online’ door
   - o Zorg dat je wachtwoord niet gestolen of geraden kan worden

5. *Besteed aandacht aan fysieke beveiliging*
   - o Laat toegangsdeuren niet onnodig open
   - o Spreek onbekende personen aan
   - o Een toegangspas is persoonlijk en leen je niet uit
   - o Laat voertuigen niet onnodig open
   - o Let op bij het bewaren en vervoeren van informatie buiten de VRMWB en BMWB