2023

Gedragscode voor gebruikers van de digitale werkomgeving

Veiligheidsregio Flevoland
Veiligheidsregio Gooi en Vechtstreek

Versiebeheer

Versienr.	Datum	Auteur(s)	Status	Opmerking
0.1	05-04-2022	Jasper Zweers	Concept	Eerste concept
0.2	05-05-2022	Arold Sonke	Concept	Specifieker gemaakt voor VR's
0.3	27-05-2022	Jasper Zweers	Concept	Toevoeging teksten reeds bestaande gedragscodes / reglementen.
0.4	30-05-2022	Arold Sonke	Concept	Integratie teksten en lay-out.
0.5	30-05-2022	Arold Sonke	Concept	Commentaar Yara verwerkt. Versie ter bespreking in projectoverleg 31-05-2022.
0.6	31-05-2022	Arold Sonke	Concept	Aangepast n.a.v. bespreking in projectoverleg (CISO, teamleider I&A en plv. Dir. Bedrijfsvoering).
0.7	16-06-2022	Arold Sonke	Concept	Commentaar verwerkt van FG, Marc v.d. Geer en samenvatting toegevoegd.
0.8	27-06-2022	Arold Sonke	Concept	Commentaar verwerkt van Carlijn van Dolder, samenvatting toegevoegd.
0.9	28-06-2022	Arold Sonke	Concept	Aanpassingen n.a.v. afstemming in het projectoverleg en met de FG.
0.9	28-06-2022	Arold Sonke	Concept	Aanpassingen n.a.v. commentaar Carlijn van Dolder en afstemming in het projectoverleg.
1.0	18-10-2022	Arold Sonke	Concept	Tekstuele aanpassingen n.a.v. projectenoverleg. Versie voorgelegd aan het GMT ter meningsvorming.
1.1	01-11-2022	Arold Sonke	Concept	Commentaar GMT i.s.m. het projectoverleg verwerkt.
1.2	28-11-2022	Jasper Zweers	Concept	Versie na aanbieding Gedragscode als 'voorgenomen besluit' aan de Veiligheidsdirectie.
1.30	24-05-2023	Jasper Zweers	Concept	Tekstuele aanpassingen n.a.v. commentaar dagelijks bestuur.

Autorisatie

Door	Datum	
GMT	25 oktober 2022	Meningsvormend
Veiligheidsdirectie	16 november 2022	Meningsvormend
OR		Advisering / Instemming
Algemeen Bestuur		Besluitvormend

Classificatie en herzieningsdatum

Dit document is voor alle medewerkers die gebruik maken van de digitale werkomgevingbinnen de Veiligheidsregio Gooi en Vechtstreek en de Veiligheidsregio Flevoland.

Het document heeft een geldigheidsduur van 5 jaar vanaf het moment van definitief vaststellen.

Inhoudsopgave

1. Samenvatting

Voor u ligt de gedragscode die van toepassing is voor alle interne en externe medewerkers werkzaam voor de Veiligheidsregio Flevoland en de Veiligheidsregio Gooi & Vechtstreek, die gebruik maken van de digitale werkplek[1] van de Veiligheidsregio Gooi en Vechtstreek en de Veiligheidsregio Flevoland en de door de Veiligheidsregio Gooi en Vechtstreek en de Veiligheidsregio Flevoland verstrekte telefoons, tablets en/of laptops.

De belangrijkste gedragsregels die in dit document verder zijn uitgewerkt, zijn:

1. Toegangstag, -token, inloggegevens, telefoons, tablet en laptops worden op de persoon uitgereikt en mogen niet gedeeld worden met anderen.
2. Kies een sterk wachtwoord en houdt je wachtwoord strikt geheim.
3. Log alleen in met je eigen accountnaam, wachtwoord en token.
4. Zorg voor een `clean desk' en 'clear screen', ook bij thuiswerken.
    a) Clean Desk = zorg er voor dat je bij het verlaten van je bureau geen persoonsgegevens of vertrouwelijke informatie laat liggen.
    b) Clear Screen = blokkeer de toegang van computer, telefoon, tablet etc. bij het verlaten van de werkplek of bij het niet gebruiken van middelen.
5. Zorg dat niemand kan meekijken als je vertrouwelijke- of persoonsgegevens raadpleegt.
6. Sla geen (zeer) vertrouwelijke en bedrijfskritieke gegevens van de Veiligheidsregio Gooi en Vechtstreek en de Veiligheidsregio Flevoland op, op je laptop, telefoon of tablet of opslagmedia zoals een USB stick of externe harde schijf.
7. Wees zeer terughoudend met het printen. Vernietig of archiveer geprinte gegevens met vertrouwelijke informatie.
8. Verwijder mail afkomstig van onbetrouwbare bron, voor deze te raadplegen.
9. Meldt het verlies van een mobiel apparaat dat je gebruikt voor werkdoeleinden direct bij je leidinggevende en de Helpdesk Veiligheidsregio Gooi en Vechtstreek en de Veiligheidsregio Flevoland.
10. Je mag de door de Veiligheidsregio Gooi en Vechtstreek en de Veiligheidsregio Flevoland aan jou ter beschikking gestelde gegevensbestanden en documenten niet kopiëren of ter beschikking te stellen aan derden, tenzij de informatie openbaar is of dat je daarvoor schriftelijke toestemming hebt gekregen van de eigenaar van deze gegevens.
11. De Veiligheidsregio Gooi en Vechtstreek en de Veiligheidsregio Flevoland digitale werkplek is bedoeld voor zakelijk gebruik, voor het uitoefenen van je werkzaamheden.
12. Wees voorzichtig met het gebruik van sociale media. Voor het gebruik van social en online media geldt het Onlinemediabeleid van Brandweer Gooi en Vechtstreek en Flevoland" van 22 september 2020.
13. Verstuur geen (bijzondere) persoonsgegevens buiten de VR's via gewone e-mail of via een andere toepassing zoals Webmail.

[1] Zie hoofdstuk 3 voor de toelichting wat verstaan wordt onder de digitale werkplek.

14. Meldt een (vermoeden van een) informatiebeveiligingsincident en / of datalek direct bij de CISO of FG.
15. Maak geen gebruik van onbeveiligde wifi netwerken, maar gebruik je (Veiligheidsregio Gooi en Vechtstreek en de Veiligheidsregio Flevoland) telefoon als hotspot.

Deze gedragscode geldt- met ingang van 1 juli 2023 en vervangt het “reglement internetgebruik” van de veiligheidsregio Flevoland en het “privacyreglement e-mail en internet BGV” en het “protocol sociale media BGV” van de Veiligheidsregio Gooi en Vechtstreek.

2. Inleiding

Vrijwel alle medewerkers van de Veiligheidsregio Flevoland en de Veiligheidsregio Gooi & Vechtstreek maken gebruik van de digitale werkomgeving. De digitale werkomgeving omvat zowel de digitale werkplek als de door de Veiligheidsregio Gooi en Vechtstreek en de Veiligheidsregio Flevoland verstrekte telefoon, tablet en laptop. Onder de digitale werkplek wordt verstaan de digitale werkomgeving waarop je met je zakelijk account inlogt.
Het gebruik kent vele voordelen alsook risico’s, daarom worden in deze gedragscode regels en voorwaarden gesteld waaraan het gebruik van de digitale werkomgeving dient te voldoen.

Het instellen van deze gedragscode heeft tot doel eenduidige en expliciete richtlijnen te geven aan alle medewerkers om hen duidelijk te maken wat van hen wordt verwacht in het kader van het veilige en verantwoorde gebruik van digitale werkomgeving. Daarnaast wordt beoogd te voorkomen dat:

- misbruik en overbelasting van de digitale werkomgeving ontstaat.
- onnodige vergissingen, incidenten of schade door het gebruik van de digitale werkomgeving optreedt.
- vertrouwelijke informatie van werknemers, of in het algemeen van de Veiligheidsregio Gooi en Vechtstreek en de Veiligheidsregio Flevoland, ongeoorloofd wordt ontsloten aan derden.
- imagoschade van de Veiligheidsregio Gooi en Vechtstreek en de Veiligheidsregio Flevoland ontstaat.

Deze regeling bevat basisafspraken die voor iedereen gelden die, al dan niet op basis van een aanstelling werkzaamheden verricht binnen de Veiligheidsregio Gooi en Vechtstreek en de Veiligheidsregio Flevoland (hierna te noemen: medewerker).

3. Algemeen

3.1 De digitale werkplek betreft het geheel van voorzieningen van de Veiligheidsregio Gooi en Vechtstreek en de Veiligheidsregio Flevoland waarin je gegevens creëert, opslaat, bewerkt, deelt of communiceert.

3.2 Het omvat:

- De Citrix / Microsoft 365 werkomgeving.

- het hele netwerk van de Veiligheidsregio Gooi en Vechtstreek en de Veiligheidsregio Flevoland;
- daarop aangesloten apparatuur zoals computers en printers;
- de aangeboden programmatuur, die vaak in de Cloud wordt aangeboden door leveranciers;
- het intranet en de infrastructuur zoals het bekabelde en draadloze netwerk.

3.3 De digitale werkomgeving betreft zowel je digitale werkplek als de door de Veiligheidsregio Gooi en Vechtstreek en de Veiligheidsregio Flevoland verstrekte telefoon, tablet en/of laptop,

3.4 Deze gedragscode is niet alleen van toepassing op de locaties van de Veiligheidsregio Gooi en Vechtstreek en de Veiligheidsregio Flevoland, maar ook als je op afstand gebruik maakt van de digitale werkplek.

3.5 Het gebruik van de digitale werkplek moet passen binnen je functie.

3.6 De verantwoordelijkheid voor de toewijzing van de digitale werkplek met de juiste functionaliteit aan de medewerkers en het wijzen op hoe de digitale werkomgeving op juiste wijze te gebruiken ligt bij het lijnmanagement. Het team I&A zal het lijnmanagement daarbij ondersteunen en, als daar aanleiding toe bestaat, controleren op juist gebruik en misbruik signaleren.

3.7 Als je via een mobiel apparaat toegang krijgt tot programmatuur en data van de Veiligheidsregio Gooi en Vechtstreek en de Veiligheidsregio Flevoland, dan moet je een gebruikersovereenkomst ondertekenen waarin de voorwaarden voor het gebruik van mobiele apparatuur is vastgelegd.

3.8 Voor het gebruik van door de werkgever beschikbaar gestelde devices met mobiele data geldt aanvullend de ‘Regeling verstrekking en gebruik mobiele telefoons’.

3.9 Het door de Veiligheidsregio Gooi en Vechtstreek en de Veiligheidsregio Flevoland aan jou beschikbaar gestelde apparaat wordt opgenomen in het Mobile Device Management (MDM) van de Veiligheidsregio Gooi en Vechtstreek en de Veiligheidsregio Flevoland. Je dient te accepteren dat MDM een deel van de controle[2] over jouw apparaat overneemt, waaronder het kunnen wissen van de gegevens van je mobiele apparatuur op afstand, beperken van de mogelijkheden tot het installeren van software en het automatisch installeren van updates.

3.10 Het protocol ‘sociale media BGV’, ‘Privacyreglement e-mail en internetgebruik BGV’ en het ‘reglement internetgebruik VRF’ zijn in dit document geïntegreerd en komen met vaststelling van dit document te vervallen.

4. Privégebruik

4.1 De digitale werkplek is bedoeld voor zakelijk gebruik. Beperkt privé gebruik is toegestaan, voorzover dit geen risico met zich meebrengt voor de digitale werkomgeving.

4.2 De door de Veiligheidsregio Gooi en Vechtstreek en de Veiligheidsregio Flevoland aan jou ter beschikking gestelde telefoon, tablet en/of laptop dient niet te worden uitgeleend.

4.3 Installeer alleen app’s uit de officiële app stores van Apple of Microsoft.

4.4 Jaag de organisatie niet op kosten door excessief telefoon- en/of internetgebruik.

4.5 Buiten Europa mag je niet via je databundel internetten.

[2] In de voorwaarden die je accepteert zal nader gespecificeerd worden welke controle kan worden overgenomen. Dit zal beperkt blijven tot hetgeen noodzakelijk is.

5. Beveiliging

5.1 Je toegangstoken en inloggegevens zijn strikt persoonlijk en niet overdraagbaar.

5.2 Je mag je geen toegang verschaffen tot de digitale werkplek met de toegangstoken of inloggegevens van een andere gebruiker.

5.3 Wijzig een toegewezen wachtwoord direct na beschikbaar stellen van een account.

5.4 Je dient je wachtwoord strikt geheim te houden.

5.5 Let erop dat wachtwoorden niet automatisch worden opgeslagen in een browser, maar in een wachtwoordmanager zoals Microsoft authenticator Dit is met name een risico als je inlogt op een apparaat dat niet verstrekt is door de Veiligheidsregio Gooi en Vechtstreek en de Veiligheidsregio Flevoland.

5.6 Je mag bedrijfsmiddelen zoals een toegangstag, toegangstoken, telefoon, tablet en/of laptop nooit onbeheerd of in een niet afgesloten ruimte achterlaten of uitlenen aan anderen.

5.7 Sla geen vertrouwelijke en bedrijfskritieke gegevens van de Veiligheidsregio Gooi en Vechtstreek en de Veiligheidsregio Flevoland op je eigen computer of mobiele apparatuur op.

5.8 Meldt bij constatering of vermoeden van misbruik, verlies of diefstal van een bedrijfsmiddel en/of je inloggegevens dit zonder uitstel aan je leidinggevende en de Helpdeks Veiligheidsregio Gooi en Vechtstreek en de Veiligheidsregio Flevoland.

5.9 Ga zorgvuldig om met vertrouwelijke en persoonsgegevens. Noodzakelijke persoonsgegevens worden verwerkt in applicaties die de Veiligheidsregio Gooi en Vechtstreek en de Veiligheidsregio Flevoland voor specifieke doelen beschikbaar stelt. Wanneer er toch bijzondere persoonsgegevens verzonden moeten worden doe dat dan op beveiligde wijze. Zie daarvoor ook hoofdstuk 10, “Veilig e-mailen” en “Veilig verzenden”.

5.10 Meldt een (potentieel) informatiebeveiligingsincident zonder uitstel aan de CISO. De CISO schakelt bij een potentieel datalek met de Functionaris Gegevensbescherming.

5.11 Bij vermoeden van een datalek neem je direct contact op met de Functionaris gegevensbescherming van de Veiligheidsregio Gooi en Vechtstreek en de Veiligheidsregio Flevoland. Melden van een datalek is een wettelijke verplichting. Raadpleeg de werkinstructie “Datalek melden” van Veiligheidsregio Gooi en Vechtstreek en de Veiligheidsregio Flevoland.

5.12 Zorg voor een `clean desk’; dat wil zeggen dat je bij het verlaten van je werkplek geen persoonsgegevens of vertrouwelijke informatie laat liggen.
Dat wil zeggen dat papieren documenten en verwijderbare media afgeschermd worden bewaard.

5.13 Zorg bij het verlaten van je werkplek voor een `clear screen’. Voorkom toegang door anderen door de computer, telefoon, tablet, etc. te blokkeren bij verlaten van de werkplek of bij het niet gebruiken van middelen en voorzieningen.

5.14 Probeer je geen toegang te verschaffen tot niet-openbare bronnen op het netwerk van de veiligheidsregio of het internet, waartoe je niet bevoegd bent.

5.15 Wijzigingen en/of toevoegingen aan de digitale werkomgeving mogen alleen worden aangebracht na goedgekeurde opdracht van de teamleider I&A.

6. Thuiswerken

6.1 Voor alle medewerkers geldt dat thuiswerken is toegestaan in overleg met je direct leidinggevende. Als het belang van de medewerker of de Veiligheidsregio Gooi en Vechtstreek en de Veiligheidsregio Flevoland dit rechtvaardigt kan de teamleider beslissen om het recht op thuiswerken te ontzeggen.

6.2 Zorg ook thuis voor een `clean desk'; zorg ervoor dat je bij het verlaten van je thuiswerkplek persoonsgegevens of vertrouwelijke informatie niet toegankelijk is voor huisgenoten en derden.

6.3 Ook op je werkplek thuis zorg je voor een `clear screen'. Voorkom toegang door huisgenoten en bezoek door de computer, telefoon, tablet, etc. te blokkeren bij verlaten van je werkplek.

6.4 Toegang van huisgenoten en derden tot de digitale werkplek en de aan de medewerker verstrekte telefoon, tablet en/of laptop is niet toegestaan.

6.5 Wees met name voorzichtig bij het thuis raadplegen van persoonsgegevens. Raadpleeg deze gegevens uitsluitend wanneer geen huisgenoten of derden kunnen meekijken.

6.6 Zorg ervoor dat bij het bespreken van vertrouwelijk gegevens, niet door anderen 'meegeluisterd' kan worden.

7. Kopiëren, printen en delen van gegevens

7.1 Je mag alleen openbare gegevens van de Veiligheidsregio Gooi en Vechtstreek en de Veiligheidsregio Flevoland delen met derden. Alle interne gegevens van de Veiligheidsregio Gooi en Vechtstreek en de Veiligheidsregio Flevoland zijn vertrouwelijk en alleen bestemd voor medewerkers van de Veiligheidsregio Gooi en Vechtstreek en de Veiligheidsregio Flevoland.

7.2 Deel geen vertrouwelijke en zeker geen persoonsgegevens met derden en maak geen kopieën van deze gegevens voor opslag op andere media dan de digitale werkomgeving van de Veiligheidsregio Gooi en Vechtstreek en de Veiligheidsregio Flevoland.

7.3 Wees zeer terughoudend met het printen van gegevens. Zorg dat na gebruik de geprinte gegevens passend vernietigd of gearchiveerd worden.

7.4 Mocht je print outs zien rondslingeren met persoonsgegevens, meldt dit als informatiebeveiligingsincident bij de CISO of FG.

8. Gebruik van internet, e-mail en sociale media

8.1 Jij bent persoonlijk verantwoordelijk voor het delen van content via internet, e-mail en sociale media.

8.2 Je mag e-mail en internet op de digitale werkomgeving alleen gebruiken binnen de normale gedragsregels van beleefdheid en fatsoen. Ander gebruik, ofwel misbruik, is niet toegestaan. Onder misbruik wordt onder meer verstaan (niet limitatief):

- Dreigende, beledigende, seksueel getinte dan wel discriminerende berichten en ketting e-mailberichten versturen;
- Bewust sites bezoeken die, racistisch, discriminerend, beledigend of aanstootgevend materiaal bevatten;

- Auteursrechtelijk beschermd materiaal, waaronder programmatuur, teksten, beeldmateriaal en muziek, kopiëren of downloaden zonder toestemming van de auteursrechthebbende;
- E-mailberichten op enigerlei wijze vervalsen of het op enig andere wijze misbruik maken van e-mail of internetvoorzieningen;
- E-mailberichten anoniem of onder een fictieve naam verzenden;
- Iemand elektronisch lastig te vallen;
- Berichten verzenden waarvan men redelijkerwijs kan begrijpen dat zij onethisch, onwettig, dan wel schadelijk voor het systeem kunnen zijn.

8.3 Neem alleen noodzakelijke geadresseerde(n) in het Aan/To, CC en Bcc veld op.

8.4 Wanneer de beveiliging of de continuïteit van de elektronische berichtenvoorziening dit vereist, is de beheerder gerechtigd voor gebruikers bestemde berichten te kopiëren, verplaatsen, vernietigen of bijlagen te verwijderen. Dit geschiedt met inachtneming van de rechten van gebruikers die in artikel 11 van deze gedragscode zijn opgenomen.

8.5 De gedragscode voor ambtenaren werkzaam bij de veiligheidsregio is voor iedere ambtenaar geldend. Twee elementen in het bijzonder vragen aandacht in het kader van het gebruik van sociale media. Deze elementen zijn het vertrouwelijk omgaan met gevoelige informatie en transparant en integer werken. Waar deze waarden als gedragscode vorm krijgen in het dagelijks leven en werk is het gebruik van sociale media hier ook onder te vatten. Integer zijn geldt voor zowel de offline als de online wereld.

8.6 Als werkgever respecteren we de vrijheid van meningsuiting en het gebruik van sociale media. Van belang vinden we wel om op te merken dat bij gebruik van sociale media iedereen kan lezen welke informatie geplaatst wordt. Informatie die voor een beperkte groep anderen bestemd was kan met enkele klikken breed verspreid worden met gewenste en ongewenste impact voor individu en organisatie.

8.7 Draag er zorg voor dat vertrouwelijke informatie die je vanuit je functie of als werknemer van de veiligheidsregio hebt verkregen niet door gebruik van sociale media bij derden terecht komen.

8.8 Let op wanneer je persoonlijke en zakelijk of werk gerelateerde onderwerpen door elkaar mixt. Wees transparant en positioneer je. Maak kenbaar of je als privé persoon spreekt of vanuit je functie of namens de organisatie.

8.9 Respecteer de privacy van anderen evenals het auteursrecht, publiciteitsrecht en andere rechten.

8.10 Verspreid geen beeld- en geluidsmateriaal vanaf de plaats incident.

8.11 Bezoek geen internetsites die pornografisch, racistisch, discriminerend of aanstootgevend materiaal bevatten dat op de een of andere manier in strijd is met de grondslagen van de veiligheidsregio om deze te bekijken, te downloaden of te verspreiden.

8.12 Download en/of gebruik geen illegale software, muziekbestanden, films en/of spelletjes.

8.13 Bezoek geen website om te gokken, deel te nemen aan kansspelen en/of chat-/babbelboxen.

8.14 Download geen bestanden om deze voor verkoop of andere commerciële doeleinden te gebruiken en/of te dupliceren.

8.15 Voor het gebruik van social en online media geldt verder het Onlinemediabeleid van Brandweer Gooi en Vechtstreek en Flevoland" van 22 september 2020.

9. Veilig e-mailen

9.1 **Veilig verzenden**

9.1.2 Iedere medewerker van de Veiligheidsregio Gooi en Vechtstreek en de Veiligheidsregio Flevoland heeft een persoonlijk mailaccount. Het is *niet* de bedoeling om een andere persoon toegang te geven tot dit persoonlijk mailaccount, tenzij de werksituatie dit vereist (zoals bij leidinggevenden).

9.1.3 Het is *niet* toegestaan om bijzondere persoonsgegevens en burgerservicenummers buiten de VR's te versturen via gewone e-mail of via een andere toepassing zoals Webmail.
Bijzondere persoonsgegevens zijn bijvoorbeeld gegevens over gezondheid, ras of etnische afkomst, politieke opvattingen, religieuze of levensbeschouwelijke overtuigingen, lidmaatschap vakbond, seksueel gedrag of seksuele geaardheid, genetische gegevens zoals DNA of biometrische gegevens zoals een vingerscan of irisscan.

9.1.4 Moeten (bijzondere) persoonsgegevens verstuurd worden, versleutel dan deze gegevens.

9.1.5 Het verzenden van persoonsgegevens per e-mail dient tot een minimum beperkt te blijven.

9.1.6 Een bericht met bijzondere persoonsgegevens dien je zodanig te verzenden dat in het onderwerp van het bericht niet direct te herleiden is welke persoon het betreft.
Vermeld bijv. geen persoonsgegevens in het onderwerp van het bericht.

9.1.7 Een onbedoeld verzonden bericht dien je zo snel mogelijk in te trekken.
Wanneer intrekken niet meer mogelijk is, dien je de ontvanger op de hoogte te stellen dat hij een bericht heeft ontvangen dat niet voor hem bedoeld was met het verzoek het bericht te verwijderen.

9.1.8 Als de ontvangst van een bericht essentieel is, dien je aan de hand van een leesbevestiging te controleren of de ontvanger het bericht heeft ontvangen en gelezen.
Als je binnen redelijke termijn geen leesbevestiging ontvangt, is het van belang de ontvanger op andere wijze te contacteren om het bericht onder de aandacht te brengen.

9.2 **Veilig ontvangen en beantwoorden van e-mail**

9.2.1 Als je een e-mail ontvangt, beoordeel je altijd of deze voor jou bedoeld is. Bij twijfel neemt je contact op met de verzender.
Als een e-mail niet voor jou bestemd is, dan informeer je de verzender daar per omgaande over en verwijder je de e-mail definitief (zowel uit het Postvak IN als uit de map Verwijderde items).
Je stuurt een e-mail met bijzondere persoonsgegevens *niet* door naar de juiste ontvanger.

9.3 **Afwezigheid**

9.3.1 Als je afwezig bent en je e-mail niet kan lezen, dien je een *out of office*-reply in te stellen, waarmee de verzender wordt geïnformeerd dat je niet aanwezig bent en wie tijdens je afwezigheid jouw vervanger is.

9.3.2 Het is *niet* toegestaan bij afwezigheid berichten geautomatiseerd door te sturen aan een mailadres buiten de Veiligheidsregio Gooi en Vechtstreek en de Veiligheidsregio Flevoland.

9.3.3 Het is *niet* toegestaan om bij afwezigheid een ander (bijv. een collega of vervanger) toegang te geven tot je persoonlijke mailaccount.

9.3.4 Als je niet zelf in staat bent om de hierboven bedoelde *out of office*-reply in te stellen en je e-mail te raadplegen, dan kan je je leidinggevende toestemming geven om je account te resetten, zodat je leidinggevende de *out of office*-reply kan instellen.

10. Monitoring en Controle

10.1 Op de naleving van deze gedragscode zal worden toegezien door of namens de CISO.

10.2 Bij het toezicht wordt wetgeving, zoals de AVG, in acht genomen. Tevens is de privacyverklaring van de Veiligheidsregio Gooi en Vechtstreek en de Veiligheidsregio Flevoland hierop van toepassing.

10.3 De controle op het gebruik van e-mail en internet vindt plaats met als doel:

- het tegengaan van misbruik of oneigenlijk gebruik van de digitale werkomgeving.
- capaciteitsbeheersing
- informatie- en netwerkbeveiliging.

10.4 Elektronische vastleggen van persoonsgegevens geschiedt (automatisch) door de veiligheidsregio ingezette software.

10.5 De vastlegging beperkt zich tot de gegevens die noodzakelijk zijn:

- Voor het verkrijgen van inzicht in de mate van gebruik van de elektronische communicatiemiddelen wordt niet de inhoud van de communicatie, maar alleen stroom- en soortgegevens vastgelegd.
- Voor het voorkomen van onrechtmatig gebruik, dan wel misbruik van elektronische communicatiemiddelen wordt het gebruik van de elektronische communicatiemiddelen op individueel en inhoudelijk niveau gevolgd. Dit geschiedt slechts bij een redelijk vermoeden van onrechtmatig gebruik, dan wel misbruik van de elektronische communicatiemiddelen.

10.6 Bij de controle op het verantwoord gebruik van e-mail internet wordt gestreefd naar een goede balans tussen de controle en de bescherming van jouw privacy op de werkplek. De omvang en manier van controleren is daarom beperkt:

- Controle in het kader van het tegengaan van “verboden gebruik” vindt in beginsel geanonimiseerd en slechts steekproefsgewijs plaats.
- Controle in het kader van capaciteitsbeheersing wordt beperkt tot verkeersgegevens (tijd, hoeveelheid, omvang e.d.).
- Voor het tegengaan van virussen en andere schadelijke programma’s in het kader van informatie- en netwerkbeveiliging, wordt het e-mail en internetgebruik op geautomatiseerde wijze gecontroleerd.

Persoonsgegevens gerelateerd aan e-mail en internetgebruik worden niet langer bewaard dan noodzakelijk.

10.7 Controle in het kader van het beveiligen van het systeem en het netwerk voor het tegengaan van virussen en andere schadelijke programma’s vindt in beginsel op geautomatiseerde wijze plaats.

10.8 Controle ter voorkoming van onrechtmatig gebruik dan wel misbruik van de elektronische communicatiemiddelen wordt zo beperkt mogelijk gehouden, in die zin dat deze in redelijke verhouding staat tot het doel waarvoor deze wordt aangewend. Bovendien vindt de controle in beginsel geanonimiseerd en slechts steekproefsgewijs plaats.

10.9 Controle vindt in beginsel plaats op het niveau van getotaliseerde gegevens die niet herleidbaar zijn tot individuele personen. Indien een medewerker of een groep medewerkers wordt verdacht van het overtreden van regels, kan gedurende een vastgestelde (korte) periode gerichte controle plaatsvinden. De medewerker wordt hierover vooraf geïnformeerd, tenzij er zwaarwegende redenen zijn om dit niet te doen.

10.10 Alleen bij zwaarwegende redenen vindt er controle op inhoud plaats. Dit gebeurt niet eerder dan na een daartoe strekkend besluit van de Veiligheidsdirectie.

10.11 Persoonsgegevens gerelateerd aan e-mail- en internetgebruik worden bij gerechtvaardigd vermoeden of constatering van oneigenlijk gebruik langer bewaard totdat de noodzaak daartoe is vervallen.

10.12 Beheerders verschaffen zich slechts toegang tot accounts of computerfaciliteiten van werknemers als de werknemer daarvoor zijn toestemming heeft gegeven. Toegang zonder deze toestemming is slechts toegestaan alleen als de inzage noodzakelijk is en de controle niet op een andere manier kan. De werknemer zal in dat geval achteraf worden geïnformeerd.

10.13 Als geconstateerd is dat je je niet aan deze gedragscode houdt, dan wordt je zo spoedig mogelijk door de verantwoordelijke, dan wel een door de verantwoordelijke aangewezen leidinggevende op je gedrag aangesproken.

10.14 Overtreding van de regels opgenomen is deze gedragscode wordt aangemerkt als plichtsverzuim en kan resulteren in disciplinaire maatregelen als bedoeld in artikel 8:13 en 16:1:2 CAR-UWO/arbeidsvoorwaardenregeling BGV / VRF. Tevens kan overtreding van deze gedragscode leiden tot het (tijdelijk) niet langer beschikbaar stellen van de e-mail- en internetvoorzieningen; zulks ter beoordeling van het MT.

10.15 Overtreding van de gedragscode kan voor medewerkers die (betaalde of niet-betaalde) werkzaamheden voor de veiligheidsregio verrichten, anders dan in ambtelijk dienstverband, resulteren in maatregelen waardoor deze medewerkers, al dan niet tijdelijk, geen beschikking meer hebben over (een deel van) de elektronische communicatiemiddelen.

11. Slotbepaling

Deze gedragscode geldt met ingang van 1 juli 2023 en vervangt het “reglement internetgebruik” van de veiligheidsregio Flevoland en het “privacyreglement e-mail en internet BGV” en het “protocol sociale media BGV” van de Veiligheidsregio Gooi en Vechtstreek.

Wijzigingen in deze gedragscode worden schriftelijk vastgelegd en, indien relevant voor de gebruiker, voorafgaand aan de invoering aan de gebruiker bekend gemaakt.