



Secretariaat: Hulpverleningszone Taxandria
Noord-Brabantlaan 68 – 2300 Turnhout
tel 014 47 09 20
mail info@hvztaxandria.be

Zoneraad

Notulen open zitting

Zitting van 29 maart 2023

Samenstelling:

Aanwezig:

de heer Frank Wilrycx; de heer Walter Luyten; de heer Kristof Hendrickx; de heer Frans de Bont; de heer Bart Craane; de heer Gilles Bultinck; mevrouw Marleen Peeters; de heer Bob Coppens; mevrouw Pascale Van Bael, Secretaris; de heer Luc Faes

Verontschuldigd:

mevrouw Dorien Cuylaerts; de heer Ward Kennes; de heer Marc Van Aperen; de heer Paul Van Miert

29 maart 2023 9:38 -De voorzitter opent de openbare zitting

OPENBARE VERGADERING

Directie Bedrijfsvoering
Dienst Secretariaat

1	2023_ZR_00043	Notulen vorige vergadering - Goedkeuring GOEDGEKEURD
---	---------------	---

Beschrijving

Aanleiding en context

De zoneraad nam in zitting van 25 oktober 2018 kennis van de wijziging in artikel 39 en 124 van de wet van 15 mei 2007, zijnde schrapping van de verplichting van de aanplakking of het online plaatsen van de zonale documenten in de gemeenten en engageerde zich om dit mee te delen binnen het eigen gemeentebestuur.

Plaats, dag, tijdstip en agenda van de vergaderingen van de zoneraad worden ter kennis gebracht van het publiek, door bekendmaking op de website van HVZ Taxandria.

Na elke vergadering van de zoneraad en van het zonecollege wordt van de besluiten binnen de twintig dagen een lijst met een beknopte omschrijving [simultaan] aan de diensten van de Gouverneur, alsook aan de diensten van de Minister gestuurd. Tegelijk met de verzending aan de Gouverneur wordt de lijst van de besluiten bekendgemaakt op de website van HVZ Taxandria en via de ad valvas op de zonale zetel.

Argumentatie

Na goedkeuring van de notulen kan de bekendmaking met besluitvorming van het openbare gedeelte opgemaakt worden, dat gepubliceerd zal worden op de zonale website van HVZ Taxandria.

Regelgeving: bevoegdheid

Wet van 15 mei 2007 betreffende de civiele veiligheid

Regelgeving: openbaarmaking

Dit besluit is niet ter inzage op basis van:

Een federale of niet-federale administratieve overheid wijst de vraag om inzage, uitleg of mededeling in afschrift van een bestuursdocument, die met toepassing van deze wet is gedaan, af, wanneer de openbaarmaking van het bestuursdocument afbreuk doet :

1° aan de persoonlijke levenssfeer, tenzij de betrokken persoon met de inzage, de uitleg of de mededeling in afschrift heeft ingestemd

Besluit

Artikel 1

De zoneraad keurt de notulen van vorige vergadering goed.

Dienst Personeel

2	2023_ZR_00044	Korporaal beroepskader - Aanleg bevorderingsreserve te begeven bij bevordering door verhoging in graad - Goedkeuring GOEDGEKEURD
---	---------------	---

Beschrijving

Aanleiding en context

De zoneraad keurde op 22 januari 2020 de personeelsformatie 2020-2025 goed.

In overeenstemming met het personeelsplan en de noodwendigheid in de zone, wordt er een bevorderingsreserve aangelegd voor de functie van korporaal beroepskader.

De bevordering kan enkel van het elgen personeel naar een toegankelijke en niet bezette betrekking; bevordering beroepskader is enkel toegankelijk voor het beroepskader.

De bevordering is wat betreft de administratieve loopbaan een bevordering door verhoging in graad.

De zoneraad keurde op 27 april 2022 het selectiereglement aanwerving en bevordering van het operationeel personeel hulpverleningszone Taxandria goed en op 25 januari 2023 werden de aanpassingen in het selectiereglement aanwerving en bevordering operationele medewerkers goedgekeurd door de zoneraad. Bijlage 4 specificeert de modaliteiten voor de bevordering korporaal.

Argumentatie

Voor het verzorgen van de continuïteit van de operationele dienst is het aanleggen van een bevorderingsreserve van de functie korporaal beroepskader noodzakelijk.

De timing voor de selectieprocedure is als volgt:

Actie	Datum	Opmerking
Agenderen raad	29 maart 2023	
Publiceren vacature	31 maart 2023	
Uiterste indieningsdatum	30 april 2023	Einddatum indienen vacature
Module 2	Week van 8 en 15 mei 2023	Online
Module 1+ 3	Week van 29 mei en 5 juni 2023	
Kennisname resultaten	28 juni 2023	
Aanstelling in zoneraad	28 juni 2023	Vanaf 01/09/2023

Nota: Datums van de proeven zijn onder voorbehoud van mogelijke wijzigingen.

Juridische grond

Bevoegdheid: Wet van 15 mei 2007 betreffende de civiele veiligheid, Art.26

Koninklijk Besluit van 19 april 2014 tot bepaling van het administratief statuut van het operationeel personeel van de hulpverleningszones.

- Art.52.- Art.53.
- Art 56. 1° bevorderingsvoorwaarden
- Art 57.

Regelgeving: bevoegdheid

Wet van 15 mei 2007 betreffende de civiele veiligheid

Besluit**Artikel 1**

De zoneraad gaat over tot aanleg van een bevorderingsreserve met een geldigheidsduur van twee jaar voor de functie van korporaal in het beroepskader.

3	2023_ZR_00045	Korporaal vrijwilligerskader - Aanleg bevorderingsreserve te begeben bij bevordering door verhoging in graad - Goedkeuring GOEDGEKEURD
---	---------------	---

Beschrijving**Aanleiding en context**

De zoneraad keurde op 27 januari 2021 de personeelsformatie 2020-2025 goed en in zitting van 23 juni 2022 werden de graden binnen het operationeel kader gespecificeerd.

In overeenstemming met het personeelsplan en de noodwendigheid in de zone, wordt er een bevorderingsreserve aangelegd voor de functie van korporaal vrijwilligerskader.

De bevordering kan enkel van het eigen personeel naar een toegankelijke en niet bezette betrekking; bevordering vrijwilligerskader is enkel toegankelijk voor het vrijwilligerskader.

De bevordering is wat betreft de administratieve loopbaan een bevordering door verhoging in graad.

De zoneraad keurde op 27 april 2022 het selectiereglement aanwerving en bevordering van het operationeel personeel hulpverleningszone Taxandria goed en op 25 januari 2023 werden de aanpassingen in het selectiereglement aanwerving en bevordering operationele medewerkers goedgekeurd door de zoneraad. Bijlage 4 specificeert de modaliteiten voor de bevordering korporaal.

Argumentatie

Voor het verzorgen van de continuïteit van de operationele dienst is het aanleggen van een bevorderingsreserve van de functie korporaal vrijwilligerskader noodzakelijk.

De timing voor de selectieprocedure is als volgt:

Actie	Datum	Opmerking
Agenderen raad	29 maart 2023	
Publiceren vacature	31 maart 2023	
Uiterste indieningsdatum	30 april 2023	Einddatum indienen vacature
Module 2	Week van 8 en 15 mei 2023	Online
Module 1+ 3	Week van 29 mei en 5 juni 2023	
Kennisname resultaten	28 juni 2023	
Aanstelling in zoneraad	28 juni 2023	Vanaf 01/09/2023

Nota: Datus van de proeven zijn onder voorbehoud van mogelijke wijzigingen.

Juridische grond

Bevoegdheid: Wet van 15 mei 2007 betreffende de civiele veiligheid, Art.26

Koninklijk Besluit van 19 april 2014 tot bepaling van het administratief statuut van het operationeel personeel van de hulpverleningszones.

- Art.52.- Art.53.
- Art 56. 1° bevorderingsvoorwaarden
- Art 57.

Regelgeving: bevoegdheid

Wet van 15 mei 2007 betreffende de civiele veiligheid

Besluit**Artikel 1**

De zoneraad gaat over tot aanleg van een bevorderingsreserve met een geldigheidsduur van twee jaar voor de functie van korporaal in het vrijwilligerskader.

4	2023_ZR_00046	Reglementen - Rechtspositieregeling administratief personeel Hulpverleningszone Taxandria aanpassing - Goedkeuring GOEDGEKEURD
---	---------------	---

Beschrijving**Aanleiding en context**

De zoneraad keurde op 27/1/2021 het personeelsbehoefteplan 2020-2025 goed.

Voor wat de dienst preventie betreft is volgende hierin opgenomen:

Voor de consultants preventie is er na 4 jaar (mits voldoen aan een aantal voorwaarden) de mogelijkheid om te bevorderen naar het B4-B5 niveau. Eén van de consultanten komt in 2023 hiervoor in aanmerking.

Momenteel is voor bevordering van Bv naar Bx opgenomen in het RPR:

4° Voor een bevordering naar een graad van rang Bx: twee jaar niveauanciënniteit in niveau B of vier jaar niveauanciënniteit in niveau C.

Tijdens de functieweging eind 2017 werd gesteld dat de medewerkers preventie na het behalen van Prev2 opleiding taken uitvoeren die de resultaatsgebieden van de functie consultant overschrijden en dus beter passen binnen de functie hoofdconsultant.

Argumentatie

De bevorderingsvoorwaarden voor de dienst preventie zijn specifiekere dan datgene wat in de huidige RPR is opgenomen.

Daarom voorstel voor aanpassen voor bevordering van consultant preventie naar hoofdconsultant preventie:

- 4 jaar in dienst zijn;
- de opleidingen PREV1 en PREV2 met succes afgerond;
- 2 jaar tussen succesvolle afronding PREV2 en bevordering;
- een minimum van 4 modules van de opleiding PREV3 moeten gevolgd zijn. De te volgen modules worden bepaald door de directeur preventie en zullen gelinkt zijn aan de meest van toepassing zijnde risico's binnen onze hulpverleningszone. De directeur preventie bepaalt de specialistische opdrachten;
- laatste evaluatie moet gunstig zijn, bij ontstentenis: positief;
- slagen in het bevorderingsexamen.

Juridische grond

Wet civiele veiligheid.

Regelgeving: bevoegdheid

Wet van 15 mei 2007 betreffende de civiele veiligheid

Financiële informatie**Financiële informatie**

Bij bevordering van B2 - 4 jaar naar B4 - 5 jaar stijgt de netto jaarloonkost met 1.500 euro niet geïndexeerd.

Besluit

Artikel 1

De zoneraad keurt onder voorbehoud van protocol van akkoord BC van 22 maart 2023 volgende wijziging van het RPR goed :

Voorwaarden bevordering van consultant preventie naar hoofdconsultant preventie:

- 4 jaar in dienst zijn;
- de opleidingen PREV1 en PREV2 met succes afgerond;
- 2 jaar tussen succesvolle afronding PREV2 en bevordering;
- een minimum van 4 modules van de opleiding PREV3 moeten gevolgd zijn. De te volgen modules worden bepaald door de directeur preventie en zullen gelinkt zijn aan de meest van toepassing zijnde risico's binnen onze hulpverleningszone. De directeur preventie bepaalt de specialistische opdrachten.
- laatste evaluatie moet gunstig zijn, bij ontstentenis: positief.
- slagen in het bevorderingsexamen.

5	2023_ZR_00047	Reglementen - Arbeidsreglement van het operationeel en administratief personeel Hulpverleningszone Taxandria- aanpassing bijlagen - Goedkeuring GOEDGEKEURD
---	---------------	--

Beschrijving

Aanleiding en context

De bijlagen van het arbeidsreglement leggen de afspraken vast voor de zone.

Deze bijlagen worden, onder voorbehoud van protocol van akkoord van het BC, aangepast indien van toepassing.

Het arbeidsreglement en bijlagen werden goedgekeurd in de zoneraad van 16 december 2020.

Argumentatie

Tijdens het Bijzonder Comité van 22 maart 2022 worden meerdere bijlagen van het arbeidsreglement voor akkoord voorgelegd.

Regelgeving: bevoegdheid

Wet van 15 mei 2007 betreffende de civiele veiligheid

Besluit

Artikel 1

De zoneraad keurt de wijzigingen in bijlage 4 van het arbeidsreglement : Gedragscode ICT en informatieveiligheid goed met ingang van 1 april 2023 onder voorbehoud protocol van akkoord.

Artikel 2

De zoneraad keurt de wijzigingen in bijlage 6 van het arbeidsreglement: Alcohol en druggebruik goed met ingang van 1 april 2023 onder voorbehoud van protocol van akkoord.

Artikel 3

De zoneraad keurt de wijzigingen in bijlage 12 van het arbeidsreglement: Uurroosters goed met ingang van 1 april 2023 onder voorbehoud van protocol van akkoord.

Artikel 4

De zoneraad keurt de wijzigingen in bijlage 18A van het arbeidsreglement: ziektemelding administratief personeel goed met ingang van 1 april 2023 onder voorbehoud van protocol van akkoord.

Bijlagen

- AR BIJLAGE 4 GEDRAGSCODE ICT EN INFORMATIEVEILIGHEID.pdf
- 2023 BIJLAGE 6 INTEGRAAL ALCOHOL EN DRUGBELEID.pdf
- AR BIJLAGE 12 UURROOSTERS.pdf
- AR BIJLAGE 18A ARBEIDSREGLEMENT ZIEKTEMEIDING ADMIN PERSONEEL.pdf



Gedragcode

ICT en Informatieveiligheid

Inhoudstafel

1 Inleiding	4
1.1 Uitgave en bekrachtiging	4
1.2 Doel	5
1.3 Toepassingsgebied	5
1.4 Verklarende woordenlijst en begrippen	6
2 Algemene regels en voorwaarden	8
2.1 Algemene regels	8
2.2 Ongeoorloofd gebruik en deontologie	9
2.3 Geheimhoudingsplicht	11
2.4 Toegang beheer netwerken, databanken en applicaties	11
2.4.1 Tijdelijk toegangen afsluiten bij afwezigheid	12
2.5 Types persoonsgegevens	12
2.6 Illegale kopieën	12
3 Gebruik Apparatuur	13
3.1 ICT apparatuur	13
3.2 Installatie software en applicaties	13
3.3 Verwerking van gegevens	13
3.4 Netwerk en verbruik	13
3.5 Wifi gebruik	14
3.5.1 Wifi <Gast HVZ Taxandria>	14
3.5.2 Wifi <Taxandria>	14
3.5.3 Algemene gebruiksregels Wifi	14
3.6 Bewaring bestanden	15
3.7 Bewaringstermijnen en archivering	16
3.8 Printpark	16
3.9 Mobiele toestellen	16
3.9.1 Toegelaten toestellen	17
3.9.2 Toegelaten applicaties	17
3.9.3 Abonnementen, licenties, kosten en modaliteiten	17
3.10 Externe opslagmedia, encryptie en beveiligd versturen van gegevens	17
3.10.1 Encryptie gegevens voor extern gebruik en beveiligd versturen gegevens	17
3.10.2 USB disk, CD Roms en externe harde schijven	18
3.10.3 Cloud opslag	18
4 Gebruik e-mail en Internet	19
4.1 E-mail accounts	19
4.2 E-mail gebruik	19



4.3 Bijlagen	21
4.4 Mails bewaren en archiveren	21
4.5 Digitale agenda	21
4.6 E-mail op mobiele toestellen	22
4.7 Internet gebruik	22
5 Pers, Sociale Media en digitale communicatiekanalen	23
5.1 Pers afspraken	23
5.1.1 Interne afspraken pers	23
5.1.1.1 Persaandacht tijdens een interventie	23
5.1.1.2 Pers neemt achteraf contact op	23
5.1.1.3 Inhoudelijk	24
5.1.1.4 Cruciale info voor de burger	24
5.1.2 Afspraken bij crisis	24
5.1.2.1 Afspraken incidenten gemeentelijke bevoegdheid	24
5.1.2.2 Afspraken crisis binnen Hulpverleningszone Taxandria	25
5.1.2.3 Interne afspraken	25
5.2 Juiste communicatiekanaal kiezen voor verspreiden informatie	25
5.3 Sociale media: context	26
5.4 Op welke sociale media is de HVZ Taxandria aanwezig?	26
5.5 Sociale media & interventies	27
5.6 Drie gouden regels	28
5.7 Juridisch kader	30
6 Mobiel werken en externe toegang	31
7 Informatiebeveiliging	31
7.1 Login- en paswoord beleid	31
7.2 Clean Desk	32
7.3 Antivirus	33
7.4 Malware en Spam	33
7.5 Web filtering	34
7.6 Phishing	34
7.6.1 Verdachte e-mail?	34
7.6.2 Verdacht telefoontje? Ook wel Vishing genoemd.	35
7.6.3 Verdachte sms?	35
7.7 Social Engineering	35
8 Aanmelden van storingen, problemen en/of wensen	36
8.1 Storingen en problemen	36
8.1.1 Dringende Storing	36
8.1.2 Niet-dringende Storing	36
9 Incidenten Meldplicht inbreuk persoonsgegevens en sancties	36
9.1 Contactpersoon meldplicht	36
9.2 Meldingsplicht	36
9.3 Meldingsprocedure	37
9.4 Sancties	40
10 Privacy, toezicht en controle	41
10.1 Geen Privacy waarborg	41
10.2 Toezicht en controle	41
10.2.1 Doeleinden van de controle	41



1 Inleiding

1.1 Uitgave en bekrachtiging

Versie: 2.0

Datum: 07/11/2022

Opmaak: IOK Geel & HVZ Taxandria

Uitgevers:

Luc Pijpers, Deskundige Informatieveiligheid, IOK

HVZ Taxandria Informatieveiligheidsteam (IVT)

Bekrachtiging: Zoneraad HVZ Taxandria
op 29 MAART 2023

Handtekening
Zonecommandant

Informatieveiligheidsteam

Handtekening
Voorzitter zonecollege



1.2 Doel

De hulpverleningszone heeft wettelijke en morele verplichtingen om beveiligingsmaatregelen te nemen met betrekking tot de informatie- en communicatietechnologie (ICT) middelen en de informatie die via deze ICT-middelen verloopt. Het doel van deze gedragscode is een gepast evenwicht te vinden tussen een verantwoord gebruik van de ICT-middelen enerzijds en de bescherming van de belangen - en in het bijzonder van de privacy - van de gebruikers en natuurlijke personen anderzijds.

De medewerker van de hulpverleningszone speelt een wezenlijke rol in de veiligheid van de organisatie in het algemeen. Deze staat bijgevolg in de eerste verdedigingslinie voor wat de risico's bij de verwerking van persoonsgegevens en gevoelige informatie betreft. Daarom is het belangrijk dat elke medewerker zich terdege bewust is van zijn rechten en plichten op dat vlak en van de goede praktijken binnen de organisatie.

De gedragscode beoogt dat de gebruiker weet:

- wat van haar/hem verwacht wordt bij het gebruik van ICT-middelen;
- hoe hij/zij vertrouwelijk omgaat met persoonsgegevens en gevoelige informatie;
- welke controles de werkgever zal doorvoeren;
- welke sancties er eventueel kunnen genomen worden bij misbruik;
- bij wie zij/hij terecht kan voor bijkomende informatie en klachten.

De gedragscode bedoelt ook:

- te waken over de veiligheid en de betrouwbaarheid van de ICT-middelen van de werkgever;
- de dienstverlening van de ICT infrastructuur te verzekeren;
- de ICT kosten te beheersen;
- de goede naam van de hulpverleningszone als verantwoorde ICT gebruikers te beschermen;
- de privacy en veiligheid van de gebruikers en derden (zowel natuurlijke- als rechtspersonen) te bewaken;
- elk ongewenst gedrag te vermijden.

1.3 Toepassingsgebied

De hierna vastgelegde Gedragscode voor medewerkers van de hulpverleningszone is van toepassing op alle ICT-middelen, IT-infrastructuur, elektronische communicatiemiddelen en op alle gegevens die door die systemen worden verzonden of erin worden opgeslagen. De Gedragscode geldt evenzeer voor ICT-middelen, al dan niet eigendom van de hulpverleningszone, die men in relatie met de hulpverleningszone gebruikt.

Deze gedragscode geldt voor alle personeelsleden, uitzendkrachten, ter beschikking gestelde werknemers, stagiairs en voor alle derden die rechtmatig toegang hebben tot de informatie- en communicatie-instrumenten van de hulpverleningszone en deze ICT-middelen gebruiken. Deze gedragscode heeft ook betrekking op technische informatie- en communicatietechnologie die nog in volle ontwikkeling is. De werkgever kan deze gedragscode bijgevolg ten allen tijde aanvullen en/of aanpassen.



Het Informatieveiligheidsteam (IVT), de informatieveiligheidsconsulent (IVC) en de informatieveiligheidsadviseur zien toe op de correcte uitvoering van deze gedragscode binnen de organisatie, en treden op als eerste aanspreekpunt betreffende informatieveiligheid en systeembeveiliging.

Voor vragen of opmerkingen aangaande deze gedragscode of informatieveiligheid kan je hen bereiken:

- via mail DPO / InformatieVeiligheidsTeam (IVT) : privacy@hvztaxandria.be

1.4 Verklarende woordenlijst en begrippen

DPO

Data Protection Officer of Functionaris Gegevensbescherming

IVT

Informatieveiligheidsteam

Werkgroep werkzaam rond de beveiliging van de verwerkingen van informatie en persoonsgegevens.

GDPR

Europese verordening gegevensbescherming van 25 mei 2016 en met ingang vanaf 25 mei 2018. Wordt ook wel afgekort als AVG (Algemene Verordening Gegevensbescherming)

GBW

Gegevensbeschermingswet van 30 juli 2018 – Belgische invulling van de GDPR wetgeving van de zaken die door de EU lidstaten zelf dienen bepaald te worden (vb toestemming door kinderen vanaf leeftijd 13 jaar)

Computervirus (virus)

Een klein computerprogramma dat er op gericht is zichzelf zo veel mogelijk te verspreiden en ondertussen al dan niet schade aan te richten aan de computersystemen waarop het zich bevindt.

Het doel van een virus kan ook het overbelasten van computersystemen zijn.

Wormen

Een worm is een virusprogramma dat zichzelf kopieert. Wormen duiken vooral op plaatsen waar beveiligingslekken zijn, zoals het internet.

Encrypteren

Versleutelen van gegevens door middel van een encryptiesleutel waardoor de leesbaarheid van de gegevens enkel maar mogelijk is indien men beschikt over de encryptiesleutel waarmee de data opnieuw in leesbare vorm kan worden omgezet.



Compressieprogramma of Zip-programma

Een compressieprogramma laat toe om een groot bestand of een reeks bestanden samen te pakken tot één verkleind bestand. Daarbij wordt door een optimale opslagtechniek te gebruiken de bestandsgrootte verminderd (= gecomprimeerd).



Spam

E-mails die in grote getalen worden verstuurd aan of ontvangen van al dan niet gekende mailadressen. Vaak hebben zij commerciële ongewenste boodschappen of verbergen zij de verspreiding van malware.

Malware

Malware is een samenvoeging van het Engelse malicious en software (kwaadwillende software) en een verzamelnaam voor kwaadaardige en/of schadelijke software.

Trojaanse paarden

Dit is een malware dat tijdens de uitvoering iets doet wat je niet meteen verwacht had. Dergelijke programma's nestelen zich op je computer en duiken te pas en te onpas op. Bovendien verschaffen deze onzichtbare toegang tot jouw systeem.

Valkuilcode

Idem als Trojaanse paarden maar dergelijke code wordt niet via internet verspreid maar met kwade intenties op netwerken geïnstalleerd.

Phishing

Phishing is fraude waarbij een oplichter gevoelige informatie (gebruikersnaam, wachtwoord, kredietkaartnummer, ...) probeert te verkrijgen om later te misbruiken.

Phishing via e-mail of een contactformulier

Fraudeurs misbruiken het logo en de identiteit van bedrijven en overheid om er misleidende e-mails mee te maken. Je krijgt de vraag om je gegevens te controleren, in te vullen op een valse site of ze via reply door te sturen.

Phishing via telefoon (Vishing)

- Iemand belt je (mogelijk via een verborgen nummer) en vraagt persoonlijke gegevens.
- Vaak vanuit het buitenland, soms verborgen achter een Belgisch nummer.
- Sms'je met vraag om terug te bellen (meestal dure betaallijnen).



2 Algemene regels en voorwaarden

2.1 Algemene regels

Enkel de personen aan wie de hulpverleningszone toelating heeft gegeven om gebruik te maken van ICT-middelen zoals e-mail, internet en intranet, telefonie-infrastructuur, computers, printers, scanners en/of andere informatie- en communicatie-instrumenten, mogen deze middelen ook daadwerkelijk gebruiken. Het dataregister bepaalt welk personeelslid uit hoofde van zijn functie toegang tot deze instrumenten krijgt.

ICT-middelen zijn niet onbeperkt bruikbaar. Zo zijn de bandbreedte van het netwerk en de opslagcapaciteit niet eindeloos. Alle aan het netwerk gekoppelde gebruikers dienen op verantwoorde wijze met deze middelen om te gaan. De gebruiker mag derhalve geen opzettelijke handelingen verrichten waardoor computerapparatuur slijt, noch op zodanige wijze op deze apparatuur beslag leggen dat anderen daarvan worden buitengesloten. Deze handelingen omvatten, maar beperken zich niet, tot het verzenden van omvangrijke mailings of kettingbrieven, te lang verblijven op het internet, spelen van spelletjes, deelnemen aan online privé- praatgroepen, uploaden en downloaden van grote bestanden, streaming van audio- en/of video of het op andere wijze belasten van het internet voor niet-zakelijk gebruik.

De ICT-dienst is verantwoordelijk voor de installatie, het beheer en het onderhoud van de ICT-middelen en de bijhorende diensten. Problemen daarmee of vragen en opmerkingen daarover worden aan de ICT-dienst doorgegeven.

De verschillende ICT-toepassingen in gebruik in de hulpverleningszone worden beheerd door hun respectievelijke verantwoordelijken, zoals opgelijst is in het data register. Problemen, vragen of opmerkingen over het gebruik van deze toepassingen dienen aan de verantwoordelijke gericht te worden.

De gebruiker heeft, voor zover van toepassing, een aantal **algemene verantwoordelijkheden en plichten** ten aanzien van ICT-middelen op het vlak van:

- in goede toestand bewaren van de ICT-middelen die ter beschikking gesteld werden;
- niet onbeheerd achterlaten van de ter beschikking gestelde ICT-middelen en het nemen van voldoende veiligheidsmaatregelen om diefstal ervan te verhinderen. Bij diefstal moet de ICT-dienst van de hulpverleningszone zo snel mogelijk gecontacteerd worden. De medewerker moet ook zo snel mogelijk de wachtwoorden wijzigen;
- nemen van voldoende veiligheidsmaatregelen die de mogelijkheid tot het inbreken op de systemen van de hulpverleningszone en diefstal van informatie zo klein mogelijk maakt:

zoals o.a. (de lijst is niet uitputtend):

- nooit meedelen van een gebruikersnaam en wachtwoord aan derden (zoals bv. collega's, stagiairs, consultants, externen, via e-mail, op onbekende websites en locaties ...) aangezien iedere gebruiker verantwoordelijk en aansprakelijk is voor alles wat onder zijn/haar loginnaam en wachtwoord gebeurt;
- het afsluiten van de werkplek bij het verlaten voor een bepaalde periode wanneer men de laatste aanwezigheid op de werkplek is;



- het activeren van de schermbeveiliging (windows-teken + L) of uitloggen;
- het beveiligen van alle ICT-middelen die op het netwerk verbonden worden (zoals o.a. laptops, smartphones, tablets, USB-sticks ...) en alle vertrouwelijke en bedrijfsgevoelige informatie die op deze ICT-middelen bewaard worden (door bv. een opstartwachtwoord, een pincode, een schermbeveiliging, een firewall, data-encryptie ... te voorzien);
- inloggen vanop externe locaties op het zonenetwerk via door de ICT Dienst beveiligde protocollen (bv. VPN ...) en systemen;
- het juist registreren en maximaal opslaan van bestanden op beveiligde en centrale locaties om te verzekeren dat de continuïteit van de dienstverlening ten allen tijde gegarandeerd blijft;
- enkel installeren en/of gebruiken van programmatuur op het ICT-middel waarvoor de nodige licenties of gebruiksafspraken aanwezig zijn;
- de veiligheid te verzekeren van de eigen gegevens die bewaard worden op de systemen;
- het installeren van hardware of software enkel door of met goedkeuring van de ICT-dienst;
- het melden van incidenten, eventuele lacunes in de beveiliging van het computersysteem of van methodes die de beveiliging van de gegevens in het gedrang brengen, bij de ICT-dienst; derden mogen hiervan niet op de hoogte worden gebracht; het uitbuiten van deze zwakheden wordt beschouwd als (poging tot) inbraak;
- op regelmatige tijdstippen lezen van zijn/haar werk e-mailadressen en het opruimen en eventueel archiveren van zijn/haar inbox;
- het voorzichtig omgaan met het doorgeven van persoonsgegevens zoals het e-mailadres, GSM-nummers, adressen, gerechtelijke gegevens, e.a. zonder dat hiervoor een officiële opdracht vanuit de hulpverleningszone voor werd gegeven;
- het voorzichtig omgaan met bestanden (o.a. bijlagen) van onbekende oorsprong en deze nooit openen wanneer men niet zeker is van de inhoud of de geadresseerde;
- het voorzichtig omgaan met het inloggen op het zonenetwerk van op andere, externe, (publieke) locaties (zoals bv. inloggen via cybercafés, inloggen via onbeveiligde open/publieke draadloze netwerken ...);
- het niet versturen van virussen of virusmeldingen (hoaxen) vanop het zonenetwerk;
- het respecteren van de algemene geldende beleefdheidsregels (nettiquette);
- Het gebruik van het internet en e-mail moet ten dienste staan van de hulpverleningszone en haar doeleinden. Uitzonderlijk privégebruik, bv. tijdens de pauze, kan in beperkte mate op voorwaarde dat de werkprestaties er niet onder lijden en het gebruik geen inbreuk vormt op onze gedragscode. Gebruik voor winstbejag, persoonlijke commerciële doeleinden of voor louter persoonlijk amusement zijn niet toegelaten.

2.2 Ongeoorloofd gebruik en deontologie

De ICT-middelen eigendom van de Hulpverleningszone mogen uitsluitend voor legale zakelijke doeleinden gebruikt worden met respect voor de deontologische code.

Behoudens specifieke richtlijnen van de hulpverleningszone, maken de personeelsleden geen gebruik voor privédoeleinden van ICT-middelen en materieel of software die de organisatie



ter beschikking stelt. In het bijzonder voor wat de communicatiemiddelen betreft, zijn zij zich ervan bewust dat ICT technische controle mechanismen in werking kunnen worden gesteld ter bescherming van ICT middelen en om misbruik ervan te voorkomen, ook al is de inhoud van privé-boodschappen gedekt door de bescherming van de persoonlijke levenssfeer en het briefgeheim.

De ICT-middelen van de hulpverleningszone mogen NIET gebruikt worden:

- om informatie te verspreiden of op te slaan die:
 - het imago, de morele of economische belangen van de hulpverleningszone kunnen schaden;
 - beledigend, lasterlijk, aanstootgevend of discriminerend is;
 - schade kan toebrengen aan derden;
 - strijdig is met de openbare orde of goede zeden.
- om informatie die als vertrouwelijk betiteld wordt of die wegens de aard ervan redelijkerwijze als vertrouwelijk moet worden beschouwd, door te geven aan personen die niet gerechtigd zijn om deze informatie te ontvangen, te verspreiden of te publiceren;
- om vertrouwelijke informatie onbeschermd te bewaren zowel elektronisch als op papier;
- om bedrijfsdata, voor andere doeleinden dan werk gerelateerde toepassingen, geheel of gedeeltelijk te kopiëren naar locaties buiten het netwerk van de hulpverleningszone zonder voorafgaandelijke schriftelijke toestemming van de hulpverleningszone; bij werk gerelateerde toepassingen moet alle data teruggegeven worden aan de hulpverleningszone bij het beëindigen van de opdracht of bij het beëindigen van de medewerking van het personeelslid aan de opdracht waaraan de data gerelateerd is;
- om persoonlijk toegekende ICT-middelen, gebruiksrechten en licenties van de hulpverleningszone door te geven aan derden;
- om onwettige handelingen te stellen door bijvoorbeeld:
 - informatie te verspreiden of op te slaan in strijd met de geldende wetgeving (zoals bv. de wetgeving op de bescherming van de persoonlijke levenssfeer bij de verwerking van persoonsgegevens, het auteursrecht of in het domein van de elektronische communicatie);
 - programmatuur te installeren of te gebruiken waarvoor de bevoegde autoriteit geen toestemming heeft verleend of waarvoor er geen afdoende licentie is;
 - de wetgeving over het auteursrecht en andere intellectuele rechten te schenden (zoals bv. programmatuur te kopiëren tenzij dit door de licentie van de leverancier of door de wet is toegestaan);
 - een valse identiteit aan te nemen op het netwerk tenzij dit beroepsmatig noodzakelijk is (ICT, beveiligingsdeskundigen).
- om buiten de gevallen van de normale bedrijfscommunicatie, massaal ongewenste of ongevraagde elektronische post (zoals o.a. spamming, phishing ...) of kettingbrieven (zoals o.a. hoaxen ...) te verspreiden;
- om via ongeoorloofde manieren (zoals o.a. phishing, sniffing ...) gebruikersgegevens en wachtwoorden van derden te verkrijgen;



- om acties te ondernemen die de beveiliging van systemen of informatie in het gedrang kunnen brengen zoals bijvoorbeeld:
 - interne en externe systeem- en netwerkbeveiliging (zoals bv. de beveiliging van een computer, netwerk, gebruikersnummer ...) te omzeilen, zodat o.a. in die systemen kan worden binnengedrongen om de bedrijfszekerheid te ondermijnen of schade toe te brengen;
 - schadelijke programmatuur (zoals o.a. Trojaanse paarden, virussen, wormen ...) op de systemen van hulpverleningszone te ontwerpen, met opzet te installeren en/of andere gebruikers aan te zetten deze programmatuur te gebruiken;
 - willens en wetens ongeëigende en ongeoorloofde toegang te forceren tot systemen waartoe men niet gerechtigd is;
 - het netwerk af te luisteren.
- om bestanden met persoonsgegevens op onbeveiligde publieke Cloud opslagplaatsen te bewaren of via onbeveiligde internet diensten te versturen;
- om andere gebruikers opzettelijk te storen bij het uitoefenen van hun activiteiten of pogingen te ondernemen om eender welke dienst, netwerk of computer te verstoren (zoals o.a. een netwerk of computer overbelasten, pogingen om een systeem te doen falen ...);
- om systeeminformatie, systeemconfiguratie, toepassingsprogramma's of bestanden te wijzigen, te verwijderen of door te geven aan derden, indien men daarvoor uit hoofde van zijn functie niet toe is gerechtigd;
- om ICT-apparatuur dat geen eigendom is van de hulpverleningszone en dat niet voldoet aan de beveiligingsregels opgenomen in dit document, aan te koppelen zonder toestemming van de systeem- of netwerkbeheerder.

2.3 Geheimhoudingsplicht

De bepalingen omtrent geheimhoudingsplicht voor het administratief personeel en het operationeel personeel van de hulpverleningszone zijn terug te vinden in de resp. arbeidsreglementen zoals goedgekeurd door de zoneraad.

[Hier refereren we naar het artikel 2.3 van het Arbeidsreglement.](#)

2.4 Toegang beheer netwerken, databanken en applicaties

Toegangsrechten moeten worden verleend volgens de 'need-to-have' en 'need-to-know'-principes. Hierbij krijgt een gebruiker standaard enkel de toegangsrechten die noodzakelijk zijn voor de functionele rol van de gebruiker binnen de organisatie. Het managementteam bepaalt via het data register per functionele rol welke toegangen noodzakelijk zijn. Indien een gebruiker een afwijkende toegang nodig heeft dient deze formeel te worden goedgekeurd door het managementteam.

In regel beheert de ICT-dienst de gebruikersaccounts, tenzij het gaat om een systeem waarvoor een specifieke beheerder werd aangesteld. De gebruikersaccounts zijn persoonlijk en worden niet doorgegeven. Elke gebruiker is verantwoordelijk voor zijn/haar account en maakt geen gebruik van de accounts van anderen.



De verwerkingsverantwoordelijke (of data-eigenaar) moet er op toe zien dat de toegangsrechten correct zijn en beperkt zijn tot wat noodzakelijk is voor de uitoefening van de job van de betrokken medewerker. Op regelmatige basis moet er een evaluatie gedaan worden door de verwerkingsverantwoordelijke van de personen en de toegangsrechten tot de informatie waarvoor de verwerkingsverantwoordelijke verantwoordelijk is.

Wanneer een gebruiker merkt dat men toegang heeft tot informatie waarvoor men niet gemachtigd zou moeten zijn, moet de gebruiker dit onmiddellijk melden bij de verantwoordelijke van de systemen, applicatie of de gegevens en/of de ICT-dienst zodat de toegangen beperkt kunnen worden.

Een medewerker die een korte- of lange tijd afwezig is, moet zijn 'out-of-office' opzetten. Voor de correcte instelling zie onder [4.2 E-mail gebruik](#). Als een medewerker zelf zijn out-of-office niet heeft opgezet kan de ICT-dienst de out-of-office opzetten. E-mails van afwezige werknemers worden omwille van privacy-redenen NIET automatisch doorgezonden. Om de continuïteit van de dienstverlening te garanderen kan het zijn dat de de leidinggevende toegang krijgt tot de mailbox van de (langdurig) afwezige medewerker, tezamen met een vertrouwenspersoon of een door de werknemer aangeduide vertrouweling. Enkel die e-mails mogen gelezen worden die relevant blijken voor de continuïteit van de dienst.

Wanneer een medewerker de organisatie verlaat, wordt de kwestie van de mailbox geregeld VOOR het vertrek. De werknemer moet de mogelijkheid krijgen om zijn/haar mailbox op te kuisen, al dan niet in het bijzijn van de leidinggevende. Indien het door omstandigheden niet mogelijk is om het opkuisen van de mailbox te regelen voor vertrek, kan de leidinggevende deze tezamen met een vertrouwenspersoon of vertrouweling aangeduid door de werknemer opkuisen, en de e-mails recupereren die nodig zijn om de continuïteit van de dienstverlening te garanderen.

Onmiddellijk na het verlaten van de organisatie wordt:

- de toegang tot de mailbox afgesloten (wachtwoord gewijzigd);
- de 'out-of-office' ingesteld door de ICT-dienst, met de vermelding dat de persoon de organisatie heeft verlaten, dat de e-mails niet worden gelezen en dat de e-mail opnieuw moet worden verzonden naar zijn/haar vervanger (contactgegevens opnemen);
- de mailbox van een werknemer die de organisatie verlaat wordt definitief verwijderd na 1 (max. 6) maand (-en), tenzij anders overeengekomen met de werknemer.

2.4.1 Tijdelijk toegangen afsluiten bij afwezigheid

Wanneer een gebruiker langdurig afwezig is, dienen de leidinggevendenden te bepalen welke toegangen (zowel logische als fysieke) tijdelijk dienen afgesloten te worden. Bij de logische toegangen denken wij aan o.a. netwerk login, Abi-logins, e-mail en agenda, remote login, specifieke applicaties, enz. Bij de fysieke toegangen denken wij aan o.a. gebouwen en ruimten (badge en/of sleutels), voertuigen, enz.

Het is dan ook belangrijk dat de dienst personeelszaken aan de ICT beheerders doorgeeft wanneer een gebruiker mogelijk langer dan 6 maanden gaat afwezig zijn. Zij kunnen dan met



de leidinggevend en overleggen welke toegangen tijdelijk dienen afgesloten te worden. Ook bij een medewerker die geheel of gedeeltelijk geschorst wordt van bepaalde taken ten gevolge van een sanctionering, dienen de leidinggevend en de toegangen te evalueren en mogelijk tijdelijk te laten afsluiten.

2.5 Types persoonsgegevens

Alle medewerkers die persoonsgegevens gebruiken/verwerken moeten op de hoogte zijn van dit onderscheid en moeten hiermee duidelijk rekening houden:

- **publieke gegevens;**
- **persoonsgegevens:** informatie over een geïdentificeerd of identificeerbaar natuurlijk persoon. Bv. naam, adres, geboortedatum, pasfoto, e-mailadres ... ;
- **gevoelige persoonsgegevens:** bv. medische gegevens, lid van politieke partij, geloofsovertuiging, etnische gegevens, gevangenisstraf uitgezeten, vingerafdruk ... ;
 - het is in principe verboden om dergelijke gegevens te verwerken tenzij er een wettelijk kader bestaat die de verwerking toelaat;
- gecodeerde al dan niet gevoelige persoonsgegevens.

2.6 Illegale kopieën

Het computernetwerk mag niet worden gebruikt om de intellectuele eigendomsrechten van eender welke partij te schenden. Deze rechten omvatten de reproductierechten, het merkenrecht, het publiciteitsrecht en het privaat recht. De medewerkers mogen niet proberen om de mechanismes te omzeilen die geïmplementeerd werden om deze intellectuele eigendomsrechten te beschermen. Elke aanval op de informatiesystemen en de netwerken is strikt verboden.



3 Gebruik Apparatuur

3.1 ICT apparatuur

Alle gebruikers benutten uitsluitend het door de werkgever ter beschikking gestelde materiaal. Alle nieuwe of bijkomende apparatuur/hardware/software wordt uitsluitend geïnstalleerd door IT-dienst of met hun uitdrukkelijke toestemming. Het is de gebruikers ten strengste verboden om zelf apparatuur van welke aard dan ook fysiek te koppelen op het netwerk tenzij de uitdrukkelijke toestemming. Het personeelslid kan steeds om verantwoording worden gevraagd omtrent het eigenlijke, buitensporig en niet deontologisch verantwoord gebruik van de middelen. [Zie 9.4 Sancties](#).

3.2 Installatie software en applicaties

Voor al wie gebruik maakt van een PC die eigendom is of ter beschikking wordt gesteld door de werkgever gelden de volgende beperkingen:

- de installatie van software en applicaties kan alleen gebeuren door de ICT-dienst of met hun uitdrukkelijke toestemming;
- de beveiligingssoftware op deze computer (antivirus, firewall, enz.) mag niet gewijzigd of uitgeschakeld worden tenzij uitgevoerd door of onder begeleiding van ICT-dienst en dit van tijdelijke aard.

3.3 Verwerking van gegevens

De Gedragscode geldt voor verwerking van alle informatie ongeacht de vorm waarin deze wordt:

- kenbaar gemaakt (op papier, elektronisch, mondeling, ...);
- opgeslagen (tekst, administratieve systemen, gegevensbanken, websites, netwerk schijven, draagbare media ...);
- verspreid (applicaties, e-mail, directory, website, telefoon ...).

Het verwerken van persoonsgegevens dient op een veilige manier te gebeuren met het oog op het verzekeren van:

- **vertrouwelijkheid:** de mate waarin de toegang tot gegevens of functionaliteit beperkt is tot degenen die daartoe bevoegd zijn;
- **integriteit:** de mate waarin gegevens of functionaliteit juist en volledig ingevuld zijn;
- **beschikbaarheid:** de mate waarin gegevens of functionaliteit op de juiste momenten beschikbaar zijn voor gebruikers.

De verwerking van gegevens wordt beperkt tot de gegevens die toereikend, relevant en niet overmatig zijn voor het bereiken van de doelstellingen van opdrachten uitgevoerd door de personeelsleden. Zelfs indien het technisch mogelijk zou zijn, is het niet toegestaan de gegevens van andere gebruikers zonder hun toestemming te raadplegen, deze te wijzigen of te vernietigen.

Ontoereikende veiligheidsmaatregelen dienen gemeld te worden aan ICT.



3.4 Netwerk en verbruik

Het is verboden informatie op het netwerk te consulteren waarvoor geen toegang is toegekend, of om toegang te proberen krijgen tot informatie zonder samenspraak met het managementteam/directiecomité.

Al wie van buiten het netwerk toegang zoekt tot de server(s), zal dit uitsluitend doen mits uitdrukkelijke toelating van de werkgever. De modaliteiten worden beschreven in hoofdstuk 6 Mobiel werken en externe toegang. Iedere gebruiker beschikt op het netwerk over persoonlijke schijfruimte waarin bestanden kunnen bewaard worden. Afhankelijk van de rechten, die bepaald worden door het managementteam/directiecomité, heeft de gebruiker ook schrijfrechten op bepaalde gemeenschappelijke schijven.

Indien een gebruiker langdurig afwezig is en er onmiddellijk actie vereist is met bestanden/informatie die niet op de gemeenschappelijke schijven kunnen teruggevonden worden, kan de zonecommandant opdracht geven aan de technisch beheerder om deze bestanden/informatie op te zoeken in de persoonlijke schijfruimte van de gebruiker.

3.5 Wifi gebruik

Binnen de hulpverleningszone bestaan er 2 Wifi netwerken, nl <Gast HVZ Taxandria> en <Taxandria>

Voor beide draadloze netwerken gelden de algemene gebruiksregels Wifi.

3.5.1 Wifi <Gast HVZ Taxandria>

- bij het verbinden met dit open Wifi netwerk dient men de gebruiksregels van de hulpverleningszone te accepteren;
- betreft een open Wifi met versleuteling van het netwerkverkeer;
- maakt verbinding met het publieke internet;
- een externe bezoeker dient de algemene gebruiksregels Wifi te lezen en aanvaarden;
- door in te loggen op het Wifi netwerk van de hulpverleningszone gaat u akkoord met deze gebruiksvoorwaarden en bevestigt u dat u deze onverkort zult respecteren;

3.5.2 Wifi <Taxandria>

- toegangscode enkel gekend door ICT van de hulpverleningszone;
- toegang configuratie van dit Wifi netwerk wordt enkel door ICT uitgevoerd;
- Wifi <Taxandria> enkel voor professioneel gebruik conform deze gedragscode;
- toegangscode kraken en/of doorgeven zijn verboden, ook indien onvrijwillig de toegangscode werd bekomen;
- ICT beheert de toegangscode en kan deze ten allen tijde aanpassen.

3.5.3 Algemene gebruiksregels Wifi

Het gebruik van het internet is voor eigen risico. De hulpverleningszone is niet aansprakelijk voor enige schade naar aanleiding van het gebruik van de internet- of draadloze netwerkverbinding.

Gebruikers die zich niet conform de gedragscode gedragen, worden van het netwerk verwijderd.



De hulpverleningszone is niet verantwoordelijk als gevolg van het gebruik van het draadloos netwerk voor de veiligheid van persoonlijke apparatuur (BYOD - Bring Your Own Device). De hulpverleningszone heeft het recht om het draadloos netwerk op ieder moment te deactiveren om onderhoud te verrichten. Ook volgende aandachtspunten gelden bij het gebruik van de Wifi:

- de hulpverleningszone biedt geen ondersteuning bij het opzetten van een verbinding op apparaten van derden;
- de hulpverleningszone kan nooit verantwoordelijk gesteld worden voor eventuele uitval van het internet of verlies van data of derving van inkomsten door technische of andere storingen;
- de hulpverleningszone is niet verantwoordelijk voor eventuele schade aan of vermissing van hardware of software van de gebruiker of veranderingen van de instellingen door het gebruik van het Wifi netwerk;
- de gebruiker is zelf verantwoordelijk voor de beveiliging van zijn of haar apparatuur;
- het is niet toegestaan om het Wifi netwerk te gebruiken om spam, virussen en illegale software te verspreiden en/of te gebruiken voor zaken en/of activiteiten die op basis van Belgisch recht niet zijn toegestaan;
- de gebruiker is verplicht zich te houden aan de letter van de wet aangaande copyright. Hij/zij mag niets over het Wifi netwerk van de hulpverleningszone naar het internet uploaden waarvan hij/zij niet zeker is dat hij/zij het copyright bezit;
- de hulpverleningszone is niet verantwoordelijk voor de informatie die door de gebruiker geplaatst werd op een server of internet. Daar is de gebruiker geheel verantwoordelijk voor. De inhoud en verstrekking van de informatie mogen in geen geval pornografisch, discriminerend of anderszins aanstootgevend zijn;
- de normale werkzaamheden en gang van zaken in de hulpverleningszone mogen niet verstoord worden door gebruik van Wifi;
- personeel en bezoekers van de hulpverleningszone mogen geen last hebben van het gebruik van mobiele apparatuur door de gebruiker (gebruik hoofdtelefoons, wees voorzichtig met kabels etc.);
- de hulpverleningszone is niet verantwoordelijk voor enige claims die voortvloeien uit activiteiten van de gebruiker;
- het gebruik van het Wifi netwerk is op basis van een fair user policy. Dit betekent dat er geen limiet is gesteld aan de hoeveelheid data die mag worden verstuurd en ontvangen. Echter, in het belang van alle gebruikers is het niet toegestaan grote bestanden (films, grote afbeeldingen) te down- of uploaden;
- de hulpverleningszone kan ingrijpen als significant meer dataverkeer wordt gebruikt dan gemiddeld en behoudt zich het recht voor om in dat geval, of om een andere reden, de verbinding met het Wifi netwerk en de gebruiker te blokkeren;
- in het belang van alle gebruikers behoudt de hulpverleningszone zich het recht voor om de bandbreedte te beperken, filters toe te passen en zogeheten 'peer-to-peer'-verbindingen te blokkeren. Ook wanneer specifieke websites een grote belasting vormen voor het netwerk, kunnen deze worden geblokkeerd. Deze maatregelen dienen het belang van alle gebruikers;
- het gebruik van uw laptop, smartphone en tablet PC is voor eigen risico. De hulpverleningszone is niet aansprakelijk voor diefstal of beschadiging;



- door in te loggen op het Wifi netwerk van de hulpverleningszone gaat hij/zij akkoord met deze gebruiksvoorwaarden en bevestigt deze onverkort te zullen respecteren.

3.6 Bewaring bestanden

Uitsluitend bestanden die verband houden met de professionele werkzaamheden mogen bewaard worden op de servers en de shared drives. De persoonlijke documenten moeten bewaard worden in de MyDrive: deze is voor privé-gebruik en is niet toegankelijk noch ondersteund door de ICT-dienst.

Voor wat betreft de manipulatie van bestanden die van buiten de hulpverleningszone afkomstig zijn, is het van noodzaak deze bestanden eerst op hun veiligheid te scannen d.m.v. een antivirussoftware.

Het bewaren van werk gerelateerde bestanden gebeurt op netwerkschijven en shared drives.

Het bewaren van persoonsgegevens in bestanden vraagt enige voorzichtigheid. Elke gegevensbank van persoonsgegevens met een permanent karakter dient te worden opgenomen in het **Register van Verwerkingsactiviteiten** (verplichting GDPR) en mogelijk in het data register. Bekijk steeds de mogelijkheid om reeds bestaande databanken te gebruiken. ***De ontwerper van een databestand met persoonsgegevens is verantwoordelijk voor het aanmelden van de gegevensbron aan het InformatieVeiligheidsteam (zie 1.3 Toepassingsgebied).*** Maken we bijvoorbeeld een telefoonlijst met persoonlijke GSM-nummers voor de planning en organisatie van de interne werking van een brandweerpost, dan dienen we deze te melden en zal deze worden opgenomen in het register.

3.7 Bewaringstermijnen en archivering

Voor de bewaartermijnen van gegevens verwijzen we naar de archiefselectielijsten bij het Rijksarchief in België te vinden achter volgende link:

<http://www.arch.be/index.php?l=nl&m=online-aanbod&r=archieffselectielijsten>

Er bestaat een specifieke [selectielijst](#) voor hulpverleningszones (brandweer).

Daarnaast zijn er specifieke archiveringsregels bepaald in andere wetgeving:

- camerawet – bewakingsbeelden
 - 1 maand of drie maanden voor de plaatsen met een bijzonder veiligheidsrisico.
- Wet elektronische communicatie – bewaring opgenomen geluidsopnames noodoproepen
 - vastgelegd in artikel 125, § 1, 3° en artikel 128
 - bij 112 wordt 1 jaar gehanteerd ([zie 112.be – FAQ](#))

3.8 Printpark

De hulpverleningszone beschikt over performante kopieermachines of netwerkprinters die de personeelsleden ook toelaten om te scannen en kleur afdrukken te maken. Het gebruik



ervan is louter voor professionele doeleinden. Het is aangewezen om bij het afdrukken op centrale printers van documenten met persoonsgegevens zoveel mogelijk gebruik te maken van **beveiligd afdrukken**.

Bij het beveiligd printen wordt het effectief uitdrukken van documenten beveiligd door ingave van een persoonlijke code op het toestel en vermijdt dat gevoelige documenten zomaar zichtbaar op de printer liggen.

Het gebruik van interventie printers is enkel toegelaten voor oproepinformatie en als back-up bij problemen met de kleurenprinter.

3.9 Mobiele toestellen

De term 'mobiele toestellen' slaat op tablets, laptops, smartphones en elk ander toestel dat buiten eigen beveiligde werkplek van hulpverleningszone kan worden gebruikt. Het gebruik van mobiele toestellen, eigendom van de hulpverleningszone, is hoofdzakelijk voor professionele doeleinden. Het privégebruik ervan kan echter op zeer beperkte schaal getolereerd worden op voorwaarde dat dit de goede werking van de ICT-infrastructuur, de dienst, de correcte uitvoering van de taken en opdrachten, niet in het gedrang brengt. Het privégebruik van GSM of smartphone eigendom van de hulpverleningszone wordt wel toegestaan. [Hiervoor verwijzen we naar bijlage 8 van het Arbeidsreglement.](#)

Het gebruik van privé toestellen tijdens de werkuren kan in beperkte mate worden toegestaan, wetende dat het gebruik ondersteunend is aan de professionele taken of dat de werkprestaties en de dienstverlening er niet onder lijden en het gebruik geen inbreuk vormt op deze gedragscode.

3.9.1 Toegelaten toestellen

De hulpverleningszone stelt bepaalde personeelsleden, ter ondersteuning van hun taken en opdrachten, een mobiel toestel ter beschikking. Indien het gebruik van private toestellen (BYOD) wordt toegestaan, is het de gebruiker verplicht de nodige beveiligingsmaatregelen te voorzien welke door de werkgevers worden opgelegd en minimaal bestaat deze uit:

- toegangsbeveiliging minimaal d.m.v. een code;
- Antivirus en Anti-Malware software
- Up-To-Date software;

3.9.2 Toegelaten applicaties

De hulpverleningszone werkt niet met 'White list' waarin alle toegelaten toepassingen in een lijst zijn opgenomen, maar laat alle toepassingen toe die niet in strijd zijn met onze gedragscode. Echter kunnen zij wel een 'Black list' opstellen van niet toegelaten applicaties. De installatie van applicaties op toestellen eigendom van de hulpverleningszone gebeurt na goedkeuring van ICT. De hulpverleningszone heeft het recht om te allen tijde bepaalde applicaties te verwijderen of de configuratie aan te passen wanneer dit de werking van het apparaat negatief beïnvloedt of het gebruik van de applicatie indruist op deze gedragscode.

3.9.3 Abonnementen, licenties, kosten en modaliteiten

Er mogen geen abonnementen of licentieovereenkomst aangegaan worden of materiaal gedownload waarvoor registratiekosten verschuldigd zijn, zonder dat de hulpverleningszone daarvoor vooraf uitdrukkelijk en schriftelijk toestemming heeft verleend.



Het is de personeelsleden niet toegestaan om:

- telefoonlijsten, mailinglijsten ... van de hulpverleningszone te gebruiken voor privé doeleinden of deze te delen met derden;
- via de mobiele toestellen deel te nemen aan spel- of amusementsprogramma's;
- dreigende, beledigende, seksueel getinte dan wel discriminerende berichten (via sms, e-mail, Twitter, Facebook ...) te versturen;
- 0900-nummers, dan wel nummers die op gelijke wijze opereren (zogenaaamde betaalnummers) te contacteren, tenzij dit m.b.t. de taken en opdrachten van het betrokken personeelslid, noodzakelijk is;
- berichten (sms ...) te versturen naar zogenaamde betaalnummers.

3.10 Externe opslagmedia, encryptie en beveiligd versturen van gegevens

3.10.1 Encryptie gegevens voor extern gebruik en beveiligd versturen gegevens

Alle informatie die via het internet verstuurd wordt of op draagbare media wordt bewaard, kan in principe gelezen, gewijzigd of hergebruikt worden, tenzij specifieke maatregelen getroffen worden. Gebruikers dienen er zich dus van bewust te zijn dat de meest gangbare protocollen op het intranet/internet geen ingebouwde technieken bevatten die de vertrouwelijkheid van de berichten waarborgen. Bovendien garanderen publieke tools zoals Dropbox, We-transfer, e.a. niet dat ze vertrouwelijk omgaan met de gegevens.

Gebruikers die persoonsgegevens of vertrouwelijke en/of gevoelige gegevens veilig wensen te verspreiden doen dit bij voorkeur door het delen van het bestand met de gepaste rechten, binnen onze werkomgeving. Bij gebruik van e-mail binnen onze organisatie dient het delen van de informatie te gebeuren via een link met de gepaste rechten.

Wanneer er elektronische post, geheugensticks, digitale transportsystemen, e.a. gebruikt worden die onze organisatie kunnen verlaten dienen bijkomende maatregelen genomen te worden ter bescherming van de gegevens zoals bv. data-encryptie (= versleuteling).

3.10.2 USB disk, CD Roms en externe harde schijven

In het netwerk zal de toegang tot mobiele opslagmedia (bv. geheugenstick, cd-rom ...) beperkt zijn. De rechten worden bepaald door de het managementteam/directiecomité. Gebruikers mogen in geen geval opslagmedia zoals geheugensticks, CD Roms of externe harde schijven gebruiken die niet van de hulpverleningszone zelf afkomstig zijn en deze op het netwerk brengen zonder dat het materiaal eerst gescand werd met een door de hulpverleningszone goedgekeurde antivirussoftware.

Speciale aandacht wordt gevraagd voor draagbare media die vertrouwelijke informatie bevatten. Deze media moeten steeds veilig opgeborgen worden. Bij vernietiging en eventueel hergebruik ervan, moet erop gelet worden dat ze geen vertrouwelijke informatie meer bevatten. Het is dan ook aangewezen om het opslagmedia leeg te maken na elk afgehandeld gebruik zodat mogelijk dataverlies tot een minimum beperkt kan worden. Bij twijfel kan altijd advies ingewonnen worden bij de ICT-dienst.



3.10.3 Cloud opslag

Cloud opslag zoals Dropbox, We-transfer, e.a. voor identificeerbare persoonsgegevens is niet toegelaten wanneer het gaat om niet beveiligde informatie. Enkel wanneer de gegevens geëncrypteerd worden met een private encryptiesleutel die je in eigen beheer hebt, kan Cloud opslag voor tijdelijke doeleinden gebruikt worden. [Zie 3.10.1 voor meer informatie over encryptie.](#)



4 Gebruik e-mail en Internet

4.1 E-mail accounts

Een personeelslid in vast dienstverband van de hulpverleningszone beschikt over een persoonlijk e-mailadres met de extensie '...@hvztaxandria.be' om in het kader van de uitoefening van zijn functie e-mails te ontvangen en te versturen. Het persoonlijke e-mailadres wordt als volgt samengesteld: 'voornaam.naam@hvztaxandria.be'. Indien een persoonsnaam uit meerdere woorden bestaat zullen de naamdelen zonder tussenkarakters geschreven worden bv. vandenbroeck.

Zij zijn dan ook verplicht deze mailadressen te gebruiken bij het uitvoeren van hun functie, dit om het officieel karakter van de communicatie aan te tonen en opdat de informatieveiligheid van de mailomgeving kan gegarandeerd worden door de hulpverleningszone.

Een **persoonlijke mailbox** is een mailbox die toegekend is aan één persoon. De persoon is volledig verantwoordelijk voor het correct gebruik van de eigen persoonlijke mailbox.

Een **gedeelde of shared mailbox** is een mailbox die toegekend is aan een groep (dienst/team). Meerdere personen hebben toegang tot deze mailbox, om de continuïteit van de dienstverlening te garanderen, ook tijdens vakantieperiodes en onverwachte afwezigheden van een contactpersoon.

4.2 E-mail gebruik

De gebruikers zijn ten allen tijde verantwoordelijk voor een beroepsmatig, ethisch en geoorloofd gebruik van e-mail. Het is niet toegestaan e-mailberichten te verzenden die in strijd zijn met de ethische en morele principes die ingaan tegen de fundamentele waarden beschreven in de deontologische code.

Het gebruik van e-mail voor persoonlijke doeleinden is niet verboden maar moet sporadisch blijven. Dit gebruik voor privéaangelegenheden mag echter geen inbreuk op deze beleidslijn inhouden, noch op enige andere wettelijke of reglementaire bepaling.

Het personeelslid zal vermijden e-mails naar grote groepen medewerkers te versturen tenzij het personeelslid hiervoor gemandateerd is. Het aanmaken van distributielijsten dient aangevraagd te worden bij de ICT-dienst. De aanvrager wordt beheerder van die lijst en staat verder in voor het correct gebruik en de opvolging van de leden.

Het is verboden om ontvangen e-mails systematisch door te sturen naar externe bestemmingen (e-mail adres), omdat dan ook professionele en gevoelige informatie automatisch verstuurd wordt naar deze externe bestemmingen. In overgangsregeling bij de uitrol van de zonale mailadressen werd voor de bestaande vrijwilligers de mogelijkheid geboden om de mail te laten forwarden naar een privé-mailadres. Hiertoe dient een aanvraag te gebeuren aan de ICT-dienst met het gedateerd en ondertekend document "Formulier doorsturen HVZ e-mail", waarin de voorwaarden worden opgesomd om dit toe te staan.



Bij langdurige afwezigheid van het personeelslid (meerdere dagen) dient een automatisch antwoord ingesteld te worden zodat correspondenten op de hoogte zijn van de langdurige afwezigheid ('out of office').

Hierin moet worden aangegeven:

- de periode dat de medewerker afwezig is;
- dat de mailbox tijdens deze periode niet (of niet frequent) wordt gelezen;
- de contactgegevens van de dienst of medewerker(s) waarbij ze terecht kunnen.

Als je niemand hebt naar wie je kan doorverwijzen, geef dan het **algemeen administratief telefoonnummer 014 47 09 20** van de hulpverleningszone en info@hvztaxandria.be.

Als een medewerker zelf zijn 'out-of-office' niet heeft opgezet kan de ICT-dienst de 'out-of-office' opzetten.

E-mails zijn elektronische berichten, en die zijn net als fysieke brieven in de eerste plaats persoonlijk. Bijgevolg wordt in alle gevallen de privacy en het briefgeheim gerespecteerd. De verzender van een e-mail is steeds verantwoordelijk voor de inhoud van het bericht.

Het is niet toegestaan om door middel van e-mail:

- berichten anoniem of onder een fictieve naam te versturen;
- vertrouwelijke informatie aan derden te verschaffen zonder toestemming van de verantwoordelijke leidinggevende;
- informatie te verstrekken waarvan de medewerker weet of redelijkerwijs kan vermoeden dat de inhoud ervan de hulpverleningszone schade kan berokkenen;
- ketting mailberichten te versturen of het interne netwerk te gebruiken voor de verspreiding van niet professioneel gerelateerde publicaties/rondschrijven die van buiten de organisatie worden aangeboden;
- privé berichten te genereren afkomstig van niet-professioneel gerelateerde nieuwsgroepen, abonnementen op e-zines, nieuwsbrieven en dergelijke.

Indien personeelsleden zich schuldig maken aan bovenvermelde handelingen, kan de toegang tot het e-mailverkeer voor het betrokken personeelslid, geblokkeerd worden op beslissing van de hulpverleningszone.

Bij het versturen van **een mail naar externen** zal er vanuit het mailsysteem automatisch een mail disclaimer worden meegestuurd met een volgende gelijkaardige inhoud:

De hulpverleningszone kan noch de technische integriteit van de inhoud van dit bericht, noch de identiteit van de afzender garanderen. Als u dit bericht per vergissing ontvangen hebt, dan is elke bekendmaking, reproductie, vorm van kopiëren, verdeling of andere verspreiding of gebruik van deze communicatie strikt verboden. Gelieve in dit geval de afzender onmiddellijk te verwittigen en het bericht te verwijderen.

4.3 Bijlagen

Indien u een mail met bijlagen verstuurt naar verschillende personen, worden deze bijlagen meermaals opgeslagen en veroudert deze informatie met soms geen zicht op de meest recente actuele versie. Daarom is het beter om als eigenaar van het document een link naar het document te versturen of het document te delen - met de gepaste rechten - zodat er steeds maar één centrale actuele versie bestaat.



Denk steeds na welke bestanden u aan uw mail toevoegt:

- zijn ze niet te groot? (max grootte 25 Mb);
- zijn alle toegevoegde bestanden echt noodzakelijk? Kunnen we niet met een verwijzing werken?
- Heb ik rekening gehouden met de veiligheids- en/of classificatiegraad van de bestanden? Mag mijn bestemming deze documenten krijgen?
- **Intern** gebruikt u geen bijlagen maar verwijst u naar de plaats op de server waar het document of de informatie is opgeslagen.

4.4 Mails bewaren en archiveren

Permanent bewaren of archiveren in een mailbox doe je best met gebruik te maken van **labels**. Een mail kan meerdere labels krijgen, en kan zo onder meerdere labels teruggevonden worden.

De informatie bewaart u best op netwerkservern of gedeelde drives, deze zijn opgezet voor een correcte verspreiding van de informatie en bewaring.

E-mails (en hun bijlagen) die de status van een 'bestuursdocument' hebben, zijn voor openbare instellingen zoals de hulpverleningszones onderworpen aan de wet van 24 juni 1955 op de archieven. Er bestaat dan ook een wettelijke verplichting om dergelijke e-mails te bewaren. Bestuursdocumenten zijn de documenten die u krijgt of stuurt in het kader van uw beroepsactiviteiten of omwille van een reglementaire bepaling.

4.5 Digitale agenda

De hulpverleningszone stimuleert het gebruik van de digitale agenda. Deze is voor alle personeelsleden met een e-mail account standaard beschikbaar. Ieder is vrij in het aanmaken van extra agenda's en gedeelde agenda's. Er wordt maximaal gebruik gemaakt van vergaderverzoeken bij het beleggen van vergaderingen en overlegmomenten.

4.6 E-mail op mobiele toestellen

De installatie van het professionele e-mail account ('.....@hvztaxandria.be') op persoonlijke toestellen is enkel toegelaten wanneer voldaan aan de vereiste beveiligingsvoorwaarden beschreven in punt [3.10.1 Toegelaten toestellen](#).

Het gebruik van een sterk wachtwoord en **2-staps verificatie** wordt afgedwongen. Indien u uw smartphone of tablet niet meer gebruikt, moet u het professionele mailaccount verwijderen. In geval van verlies of diefstal dient u onmiddellijk ICT te verwittigen en kunnen zij vanop afstand een vernietiging van de gegevens in het professionele account uitvoeren (wipe). Voor IOS toestellen betreft dit een wipe van het ganse toestel, ook het privé-gedeelte.

4.7 Internet gebruik

Het gebruik van het internet en e-mail moet ten dienste staan van de Hulpverleningszone en haar doeleinden. Uitzonderlijk privégebruik kan in beperkte mate wetende dat de werkprestaties er niet onder lijden en het gebruik geen inbreuk vormt op onze gedragscode. Gebruik voor winstbejag, commerciële doeleinden of voor louter amusement zijn niet toegelaten.



Het internet is een wereldwijd computernetwerk dat miljoenen pagina's met informatie bevat. Gebruikers worden erop gewezen dat vele van die pagina's aanstootgevende, expliciet seksuele of ongepaste informatie bevatten. Het is over het algemeen moeilijk elk contact met dit soort informatie te vermijden bij gebruik van het internet. Zelfs onschuldige zoekacties kunnen leiden naar sites met een zeer aanstootgevende inhoud. Bovendien is het mogelijk dat u via uw e-mailadres ongevraagde e-mailberichten met aanstootgevende informatie ontvangt. Gebruikers van het internet doen dat op eigen risico en met de nodige waakzaamheid voor de veiligheid van de ICT-middelen van de hulpverleningszone. De hulpverleningszone is niet verantwoordelijk voor de informatie die gebruikers via internet kunnen inzien of downloaden.

De hulpverleningszone investeert voortdurend in het beschermen van de interne infrastructuur. Eén van de speerpunten is het screenen van de inkomende e-mail op het maildomein @hvztaxandria.be. Het up- of downloaden van software e.a. is verboden en is voorbehouden aan ICT medewerkers. De hulpverleningszone wil hiermee het auteursrecht en de copyright regelgeving respecteren.

De hulpverleningszone behoudt zich het recht om op elk moment de toegang tot websites waarvan zij de inhoud illegaal, ongepast of niet deontologisch verantwoord vindt, te blokkeren voor de gebruiker.

Om de goede werking van het interne netwerk te garanderen, wordt voor de internettoegang gebruik gemaakt van zogenaamde filtersoftware die websites gaat controleren op veiligheidsproblemen. Hierbij worden websites die schade kunnen toebrengen aan het netwerk automatisch geblokkeerd (bv. virussen, malware, phishing ...). Aangezien een automatisch systeem niet feilloos is, kan het gebeuren dat een website of welbepaalde URL, onterecht is geblokkeerd. In dat geval kan het personeelslid de ICT dienst hiervan in kennis stellen.

Het overmatig gebruik maken van breedband verbindingen (streaming video, online gaming, netflix, e.a.) welke niet gerelateerd zijn tot het werk van de hulpverleningszone zijn verboden teneinde geen overmatig beslag te leggen op de professionele bandbreedte.



5 Pers, Sociale Media en digitale communicatiekanalen

5.1 Pers afspraken

Als Hulpverleningszone is het belangrijk dat we eenvormig communiceren naar de buitenwereld toe door enkele duidelijke afspraken op een rij te zetten. Deze afspraken scheppen duidelijkheid over de taken en verantwoordelijkheden van de verschillende betrokkenen. Dit geldt zowel voor de dagelijkse communicatie naar de pers als in crisissituaties.

Voor de reglementering verwijzen we naar [5.7 Juridisch kader](#).

Wat betekent dit voor ons als brandweerm medewerkers?

Het is verboden voor de medewerkers van de HVZ Taxandria om informatie over interventies naar de pers toe te verspreiden. Het is niet toegestaan om als brandweerm medewerker de pers op eigen initiatief te contacteren om deze op de hoogte te brengen van of te informeren over interventies.

Deze instructies dienen strikt nageleefd te worden. Het niet naleven van het beroepsgeheim is strafrechtelijk en tuchtrechtelijk vervolgbaar.

5.1.1 Interne afspraken pers

5.1.1.1 Persaandacht **tijdens** een interventie

Indien de pers bij een standaard interventie om een verklaring vraagt, wordt er steeds doorverwezen naar de hoogst leidinggevende officier van dienst (OVD) ter plaatse. **Enkel de OVD mag zelf de pers te woord staan.** Deze dient zich te beperken tot objectief vastgestelde feiten die mogen en kunnen vrijgegeven worden. Indien deze persoon niet langer ter plaatse is, mag doorverwezen worden naar:

- Tijdens kantooruren: communicatieverantwoordelijke (COM)
- Bij afwezigheid COM: directeur operaties (DIR OPS)
- Bij afwezigheid van COM en DIR OPS: zonecommandant (ZOCO)

5.1.1.2 Pers neemt **achteraf** contact op

Wanneer de pers achteraf contact opneemt mag doorverwezen worden naar de COM. Indien de COM over te weinig informatie beschikt, vraagt deze na wat er gebeurd is bij betreffende OVD. Bij twijfel: niet antwoorden, maar gegevens journalist noteren en hem beloven terug te bellen.

Indien de COM onvoldoende dossierkennis heeft, noteert hij/zij de gegevens van de journalist, contacteert de OVD tijdens het incident en laat deze persoon de journalist terug contacteren.

Bij afwezigheid van de COM, de pers doorverwijzen naar de DIR OPS. Bij afwezigheid van zowel DIR OPS als de COM, naar de ZOCO.



5.1.1.3 Inhoudelijk

Wat mag meegedeeld worden aan de pers?

Tijdens het incident:

- Altijd objectieve feiten
- Aard van het incident
- Afspraken met pers rond verdere informatie na de interventie

Na afhandeling van het incident:

- Straat
- Aard van het incident
- Algemene staat schade
- Uur van de interventie
- Aantal betrokkenen

Info die niet meegegeven wordt:

- Oorzaak van het incident (wij spreken ons niet uit over schuld)
- Specifiek adres
- Gegevens van betrokkenen of slachtoffers (vage beschrijving zoals "jonge moeder met twee kinderen" mag wel)
- Geen eigen mening of interpretatie

5.1.1.4 Cruciale info voor de burger

Indien er een interventie plaatsvindt waarbij het **nuttig is om de burger te informeren** (bv. sluiten van ramen en deuren door rookontwikkeling) stuurt de OVD dit naar de COM via de dispatching. Dit kan info zijn over metingen en risico's rook, geurhinder, concentratie gevaarlijke stoffen, vrijkomen van asbest, roetneerslag, enz. De COM zet de info op sociale media en houdt de communicatieverantwoordelijke van de betreffende gemeente/stad mee op de hoogte.

5.1.2 Afspraken bij crisis

Bij grote branden waarbij de veiligheid of de gezondheid van omwonenden een risico lopen, treedt een **rampenplan** in werking. Maak duidelijk aan de interventieploeg dat nieuwsgierige journalisten of omwonenden altijd doorverwezen moeten worden naar de OVD. Indien het gemeentelijk rampenplan is afgekondigd, is de burgemeester het eerste aanspreekpunt. Raad de journalist aan om de woordvoerder van de burgemeester te contacteren.

5.1.2.1 Afspraken incidenten gemeentelijke bevoegdheid

Indien er een **crisisituatie** is uitgeroepen, is de burgemeester van de respectievelijke gemeente steeds verantwoordelijk voor de communicatie. In samenspraak met de burgemeesters, de noodplanambtenaren en de COM van de gemeenten (en politie) kan



afgesproken worden op welke manier de COM van de HVZ een ondersteunende rol kan bieden.

De COM van de HVZ Taxandria zal in crisissituatie de communicatie van de gemeenten ondersteunen met verwijzing naar de communicatiekanalen van de betreffende gemeenten.

5.1.2.2 Afspraken crisis binnen Hulpverleningszone Taxandria

De voorzitter van de HVZ Taxandria is steeds verantwoordelijk voor de communicatie tijdens een crisis binnen de HVZ Taxandria zelf. Bij afwezigheid, neemt de ondervoorzitter van de HVZ Taxandria deze taak op zich.

5.1.2.3 Interne afspraken

- De voorzitter wordt door de betrokkenen op de hoogte gebracht indien er zich een situatie voordoet die mogelijk vat kan hebben op een medewerker binnen de organisatie, de organisatie of de reputatie van de hulpverleningszone.
- De ZOCO wordt door de betrokkenen op de hoogte gebracht van het incident.
- De ZOCO en de voorzitter beslissen welke stappen verder ondernomen worden, afhankelijk van het incident/de situatie.
- Indien nodig worden het managementteam (MT) en de COM op de hoogte gebracht en bijeen geroepen om verdere strategie te bepalen:
 - o Kernboodschap bepalen
 - o Afspraken rond verdere communicatie naar de pers
 - o Bij persbericht: informatie aanleveren aan COM en deze schrijft persbericht. Deze wordt verstuurd richting perscontacten. Kernboodschap aanhouden!
 - o Bij persconferentie: Uitnodiging wordt verstuurd door COM. Voorzitter van de zone is de persoon die de persconferentie voorziet. Bij afwezigheid: ZOCO – betrokken Clusterverantwoordelijke (CV) – betrokken postoverste of officier. Neutrale plaats kiezen voor interviews (zonder herkenbare achtergronden).

5.2 Juiste communicatiekanaal kiezen voor verspreiden informatie

- De medewerkers mogen werkgerelateerde onderwerpen publiceren mits het geen vertrouwelijke informatie bevat (nooit over interventies) en de hulpverleningszone, haar medewerkers en relaties niet op enige wijze schade toebrengt.
- Sociale media – en zeker de privé-kanalen – zijn niet de juiste kanalen voor het publiceren, versturen of verspreiden van vertrouwelijke en privacy informatie.
- Kies voor de juiste content het juiste communicatiekanaal:
 - **Directe communicatie** - te contacteren personen zijn gekend
 - Onmiddellijke reactie verwacht
 - => **INA interventie app**
 - => **Telefoon/GSM/Google chat app**
 - Niet onmiddellijke reactie verwacht



=> E-mail

- **Indirecte communicatie** - te bereiken personen niet vooraf gekend
 - **Publiek**
 - Statisch en tragere communicatie – kleiner direct bereik – geen reactie verwacht – nieuws met blijvende informatie (bv. nieuwsartikel)
=> website
 - Snelle en vluchtige communicatie – groter bereik – mogelijk reactie – eerder tijdelijke informatie met boodschap naar gemeenschap (bv. actuele dreiging, status van actuele of recent uitgevoerde interventie/gebeurtenis)
=> facebook, BIN, twitter
 - **Privé**
 - Statisch en tragere communicatie – kleiner direct bereik – geen reactie verwacht – nieuws met blijvende informatie (bv. kennisartikel, werkingsprocedure)
=> Intranet, E-mail
 - Snelle en vluchtige communicatie – groter bereik – quasi onmiddellijk reactie verwacht – eerder tijdelijke informatie (bv. (urgente) vraagstelling naar kennis/info, korte informering over actuele of recente interventie)
=> Google chat app, privé WhatsApp groep

5.3 Sociale media: context

Heel wat mensen zijn actief op sociale media. Het woord is er aan de gebruikers: ze brengen mensen en hun verhalen samen, en kunnen op elkaar reageren. Logischerwijs zitten ook heel wat medewerkers van de HVZ Taxandria op verschillende sociale media kanalen. Ook als organisatie zijn we aanwezig op Facebook, Twitter, LinkedIn en Instagram. Zo kunnen we gemakkelijk informatie geven aan de burgers van de verschillende gemeenten in onze hulpverleningszone. Bovendien proberen we te bouwen aan onze reputatie en de naambekendheid van de HVZ Taxandria te vergroten. Dit doen we o.a. met hulp van onze medewerkers die ons ondersteunen en berichten delen. Zeker een troef van deze kanalen.

5.4 Op welke sociale media is de HVZ Taxandria aanwezig?



www.facebook.com/HVZTaxandria



www.twitter.com/HVZTaxandria



www.linkedin.com/company/hvz-taxandria



<https://www.instagram.com/hvztaxandria>



Officiële communicatie op sociale media vanuit onze organisatie gebeurt alleen via de officiële bovenstaande accounts. Het is niet uitgesloten dat er in de toekomst kanalen bijkomen of verdwijnen aangezien sociale media continu evolueert. Officiële, centrale communicatie gebeurt vanuit de zonale accounts.

Facebook/instagram pagina's van de verschillende posten

Momenteel bestaan er naast de officiële Facebook pagina van de HVZ Taxandria, ook enkele facebook- en instagram accounts van verschillende posten.

Samen vormen we één hulpverleningszone. Alle Facebook/instagram accounts die bestaan, maken dus deel uit van de HVZ Taxandria. Daarom is ook de informatie die langs deze pagina's verspreid wordt, communicatie door de hulpverleningszone. Eigen bedenkingen, politiek gekleurde posts en persoonlijke aanvallen zijn dus uit den boze. Hetzelfde geldt voor de bestaande Twitter accounts.

Deze pagina's en accounts blijven bestaan en we geven enkele richtlijnen mee om ze goed te beheren:

- Post ENKEL over interventies als je relevante informatie voor de burger wil delen. Blijf steeds bij objectieve feiten. Hou de communicatieverantwoordelijke van de hulpverleningszone op de hoogte over interventie posts (via sms of zonale facebook pagina). Zo kan maximaal gedeeld worden.
- Spreek duidelijk af wie van de post het beheer van de pagina doet. Duid best een plaatsvervanger aan om de pagina te onderhouden als je langere tijd afwezig bent.
- De ideale post is bondig, helder en werkt met beelden. Vermijd lange posts. Foto's spreken aan.
- Geef op tijd antwoord op reacties, vragen of berichten op je pagina. Reageer liefst binnen de 24u op reacties of vragen.
- Bedank mensen voor hun positieve reacties. Zo straal je een positieve boodschap uit naar je volgers.
- Een Facebook/instagram account is een communicatiemiddel: let dus op taal en stijl. Het mag gerust vlotter zijn dan in een officiële brief. Maar schrijf wel correct en laat hoofdletters en uitroepetekens achterwege: deze komen schreeuwerig over. Schrijf in de wij-vorm, je spreekt in naam van de organisatie.
- Denk goed na voor je in dialoog gaat: geen persoonlijke meningen en laat je niet verleiden door discussies. Verwijder berichten die niet stroken met de spelregels (b.v. racistische, discriminerende of kwetsende boodschappen).

5.5 Sociale media & interventies

Het is steeds gemakkelijker om snel een foto of een video te maken en te delen. **We willen echter duidelijke afspraken maken m.b.t. publicaties van interventies binnen de HVZ Taxandria:**

- Maak geen foto's, selfies of filmpjes van jezelf of van collega's tijdens een incident. Maak ook nooit foto's van slachtoffers. Dit getuigt van weinig respect en discretie.



Tijdens een interventie dragen we professionaliteit hoog in het vaandel, waarbij de hulpverlening centraal staat.

- Tijdens een interventie post je geen berichten online over het incident. Het recht op privacy van de eventuele slachtoffers mag je niet schenden.
- Als hulpverlener ben je gebonden aan het beroepsgeheim (zie artikel 458 van het Strafwetboek) en aan de discretieplicht. Dus zonder (schriftelijke) toestemming mag je geen gegevens over een brand of ongeval doorgeven aan de pers of het 'grote publiek'. Ook het doorsturen van foto's van de schade en van de slachtoffers is niet toegestaan.
- In het kader van RETEX kan de OVD uiteraard wel foto's nemen of deze opdracht doorgeven.

5.6 Drie gouden regels

Het gebruik van sociale media kan onverwachte en onbedoelde gevolgen hebben. Het is belangrijk te beseffen dat medewerkers met berichten op sociale media het imago van de HVZ Taxandria ook (onbewust) kunnen schaden. Sociale media is niet privé, maar ook toegankelijk voor derden.

HVZ Taxandria vertrouwt erop dat zijn medewerkers verantwoord omgaan met sociale media en geeft enkele richtlijnen op om haar medewerkers daarin te ondersteunen.

De richtlijnen hebben betrekking op persoonlijke berichten waarbij er overlap is tussen werk en privé. Wat je doet of zegt, kan de reputatie van de HVZ beïnvloeden, zowel positief als negatief. Je blijft immers altijd een medewerker van onze hulpverleningszone. Iedere gebruiker van sociale media draagt een individuele verantwoordelijkheid.

We vragen je om de **3 gouden regels** hierna te respecteren als je sociale media gebruikt met een (on)rechtstreekse link naar de HVZ Taxandria. Dit geldt ook voor de Facebook/instagram accounts van de posten.

1. Sociale media = transparantie

Iedereen leest mee op sociale media. Wees je ervan bewust dat alles wat je deelt vindbaar is, en ook tegen jou of de HVZ Taxandria gebruikt kan worden.

DO'S ✓

- **Wees loyaal tegenover de HVZ Taxandria.** Als je een probleem wilt aankaarten of kritiek hebt, doe je dat via de interne kanalen, niet via sociale media.
- **Respecteer de wettelijke regels** over auteursrecht, openbare orde, goede zeden en discriminatie.
- **Denk goed na voor je iets online zet.** Op internet is privacy erg beperkt. Vergis je niet: ook als je goede privacy instellingen hebt, kunnen andere mensen gemakkelijk jouw teksten of foto's zien. Het volstaat dat een van je vrienden reageert: zijn vrienden kunnen die reactie zien, een screenshot maken en dat doorsturen. Ook journalisten zoeken dikwijls informatie en foto's op bijvoorbeeld Facebook. Gebruik je gezond verstand als je iets publiceert.
- **Beveilig je accounts** met een veilig paswoord en optimaliseer je privacy instellingen. Zie ook <https://www.mijnonlineidentiteit.nl/social-media-privacy-instellingen>



DON'TS ✗

- **Spreek je als HVZ Taxandria medewerker niet kritisch uit** over incidenten, collega's, overheden en hun medewerkers en de HVZ Taxandria. Beledigingen, laster en obsceniteiten kunnen niet door de beugel.
- **Deel geen interne of vertrouwelijke informatie** van de HVZ Taxandria op sociale media en wees altijd open en eerlijk in je communicatie. Vertel alleen wat je zeker weet en zorg dat de informatie correct is. Interne communicatie is bestemd voor intern gebruik.
- **Spreek niet over collega's op het internet buiten hun weten om.** Online dingen opsporen is gemakkelijk. Plaats geen foto's van andere mensen online zonder hun medeweten. Respecteer hun privacy.

2. Sociale media = constructieve communicatie

De toon die je hanteert voor je online communicatie is best informeel, maar ook respectvol, professioneel en positief. Positieve reacties werken opbouwend en spreken ook andere volgers en fans aan. Bedank mensen voor hun feedback. Negatieve reacties kunnen terecht of onterecht zijn. Merk je negatieve zaken op over de HVZ Taxandria? Deze kan je doorgeven aan de communicatie verantwoordelijke.

DO'S ✓

- Schrijf **constructief** en onderbouw je reactie. Vraag je af of je hetzelfde luidop zou zeggen in een zaal vol met collega's. Want dat is eigenlijk wat je online doet.

DON'TS ✗

- **Scheldtirades en drogredeneringen** laat je best aan je voorbij gaan. Laat je niet verleiden tot discussies.

3. Sociale media = jij bent onze belangrijkste ambassadeur

Pas goed op met het vermengen van je persoonlijke en professionele leven. Houd er altijd rekening mee dat jouw persoonlijke mening geïnterpreteerd kan worden als de mening van de HVZ Taxandria. Denk aan de voorbeeldfunctie die je hebt als brandweerman of -vrouw. Alles wat je zegt en doet, kan verspreid worden via sociale media. Wees trots op je werkgever. Vergeet niet dat mensen jou kennen als werknemer bij onze hulpverleningszone.

DO'S ✓

- **Communiqueer je zelf online? Maak je dan persoonlijk bekend.** Je vermeldt best dat jouw mening niet noodzakelijk die van de HVZ Taxandria is. Maak duidelijk dat je berichten in eigen naam plaatst. Respecteer ook altijd andere meningen en geef vergissingen toe.
- **Trots op je werk?** Deel de berichten van je brandweerpost en de hulpverleningszone en we zijn je eeuwig dankbaar!
- **Netwerken met vrienden** doe je buiten de werkuren of binnen de daarvoor voorziene tijd.



DON'TS X

- Vermijd posts waarbij je **negatieve feedback** geeft op je werkgever.
- Maak geen **accounts aan op naam de HVZ Taxandria** zonder toestemming.
- Treed niet op als **woordvoerder** van de HVZ Taxandria.

5.7 Juridisch kader

- Medewerkers zijn persoonlijk verantwoordelijk voor de inhoud die ze publiceren op sociale media.
- De medewerkers die met hun persoonlijke meningen naar buiten treden via sociale media, zijn hier juridisch aansprakelijk voor.
- Bij twijfel of een publicatie de richtlijnen schaadt, neemt de medewerker contact op met zijn of haar leidinggevende.

Beroepsgeheim

In de omzendbrief van Binnenlandse Zaken van 9 augustus 2011 en het Koninklijk Besluit van 19 april 2014 over het administratief statuut van het operationeel personeel van de hulpverleningszone, wordt er beschreven wat we als brandweerpersoneel wel en niet mogen vertellen aan pers en publiek.

Als hulpverlener ben je gebonden aan het **beroepsgeheim** (zie art. 458 van het Strafwetboek) en aan de **discretieplicht**. Dit houdt in dat je je eigen vrijheid van meningsuiting beperkt om het openbaar en algemeen belang niet te schaden. Dus zonder (schriftelijke) toestemming mag je geen gegevens over een brand of ongeval doorgeven aan de pers of het 'grote publiek'. Ook het doorsturen van foto's van de schade en van de slachtoffers is niet toegestaan.

Art. 13 van het KB van 19 april 2014, beschrijft bovendien dat je als personeelslid principieel spreekrecht hebt over feiten waarvan hij/zij kennis heeft omwille van het uitoefenen van zijn/haar functie. Je mag echter niet zomaar over een interventie met de buitenwereld communiceren: zo mag je het recht op privacy van de slachtoffers niet schenden. Dus geen adressen doorgeven, niet zomaar over de omstandigheden van de brand of een ongeval praten met eender wie er om vraagt.

Sancties

Bij niet-naleving van de principes over het gebruik van sociale media kunnen tuchtmaatregelen worden opgelegd. Respecteer de huisregels en het arbeidsreglement van de HVZ Taxandria. Het spreekt voor zich dat medewerkers van de HVZ Taxandria in hun eigen online communicatie respect hebben voor het beroepsgeheim maar ook voor auteursrechten en privacy.

Het is verboden voor de medewerkers van de HVZ Taxandria om informatie over interventies naar de pers toe te verspreiden. Het is niet toegelaten om als brandweerm medewerker de pers op eigen initiatief te contacteren om deze op de hoogte te brengen van of te informeren over interventies.



6 Mobiel werken en externe toegang

Onder 'mobiel werken' wordt verstaan dat men extern toegang heeft tot informatiesystemen van de hulpverleningszone. Deze manier van werken beoogt een verhoogde beveiliging die de veiligheid van de informatie en het verkeer ervan waarborgt. De ICT-dienst zal een adequate ICT-omgeving uitwerken welke deze informatieveiligheid waarborgt. Tevens bepaalt de ICT-dienst samen met de zone leiding welke personen met welke mobiele toestellen externe toegang zullen krijgen om mobiel te werken. [Zie hoofdstuk 3.9 Mobiele toestellen.](#)

Accounts op de mobiele toestellen eigendom van de hulpverleningszone worden door de ICT-dienst geïnstalleerd. Uitsluitend op persoonlijke toegewezen toestellen mogen persoonlijke e-mailaccounts ingesteld worden. Het is dus verboden om eigen accounts (bv. Gmail) op gemeenschappelijk gebruikte toestellen te installeren.

De gebruiker zal de veiligheidsinstellingen van het toestel, zoals ingesteld door de ICT-dienst, niet wijzigen, ook al is dit technisch mogelijk. Het is verplicht om het toestel van een code te voorzien zodat de toegang tot het toestel beveiligd is. Op mobiele toestellen eigendom van de hulpverleningszone gebruikt voor externe toegang, worden enkel door ICT applicaties geïnstalleerd teneinde een correcte en veilige installatie te waarborgen. De ICT-dienst zal steeds de mogelijkheid hebben om de toegang tot de informatie van hulpverleningszone (gegevens/accounts aanwezig op de smartphone, bv. e-mail) te blokkeren en de gegevens te wissen. In geval van verlies of diefstal wordt de ICT-dienst zo snel mogelijk in kennis gesteld. Het toestel wordt door de ICT-dienst indien mogelijk en nodig vergrendeld en gewist. Dit kan leiden tot het verlies van persoonlijke gegevens die op de smartphone zijn opgeslagen.

7 Informatiebeveiliging

7.1 Login- en paswoord beleid

Om toegang te krijgen tot de verschillende informatiesystemen, moeten de gebruikers zich identificeren door een gebruikersnaam in te voeren die gelinkt is aan een persoonlijke (geheime) code die toelaat de authenticatie te valideren (paswoord). Die paswoorden, of persoonlijke codes, vormen dus een belangrijk aspect van de informatiebeveiliging, in die zin dat ze toegang bieden tot de systemen en informatie. Daarom is het heel belangrijk om een complex paswoord samen te stellen en te kiezen. Dit beleid moet als een 'minimale norm' worden opgevat voor alle systemen van de hulpverleningszone. Ook logins voor toepassingen die via internet ter beschikking worden gesteld dienen aan deze minimale norm te voldoen.

De vereisten van sterke paswoorden:

- moeten minimaal 8 tekens bedragen;
- worden uit een mengeling van kleine letters (a-z), hoofdletters (A-Z), cijfers (0-9) en speciale tekens (&@#!»{}' _+!\$%=: ;?./<>*) samengesteld. Minimaal drie van de vier types (kleine letters, hoofdletters, cijfers en speciale tekens) zullen worden gebruikt;



- hebben een geldigheidsduur van minimaal 1 dag en maximaal zes maanden. Indien mogelijk wordt het periodiek wijzigen van het paswoord afgedwongen door het betreffende systeem;
- moeten van de laatste 5 gebruikte paswoorden verschillen;
- mag de naam van de gebruiker of zijn gebruikersnaam (of een deel ervan) niet bevatten;
- moeten verschillend zijn om toegang te krijgen tot de verschillende externe systemen van de hulpverleningszone (vb.: netwerk, publieke web mail, websites op internet, paswoorden voor mobiele telefoons en Pda's ...). Het hergebruiken van paswoorden voor verschillende toepassingen verhoogd het risico indien uw paswoord wordt gekraakt (hacked);
- het paswoord is bestemd voor persoonlijk gebruik en mag in geen geval aan een andere persoon worden meegedeeld. De gebruiker moet alle redelijke maatregelen treffen om de toegang tot zijn paswoord te beveiligen;
- wanneer de gebruiker ervan op de hoogte wordt gebracht dat een andere persoon zijn paswoord kent of er nog maar een licht vermoeden is van misbruik van de loginnaam en het paswoord, moet de gebruiker het zo snel mogelijk wijzigen;
- Indien geen gebruik gemaakt wordt van een paswoord generator dient de gebruiker zelf een methode te gebruiken waardoor hij de verschillende wachtwoorden kan onthouden zonder deze te noteren of op te slaan zodat deze zichtbaar zijn voor andere personen zoals op post-it's, notitieblokken, onbeschermd bestanden, e.a., denk daarbij aan de onthoudbaarheid door het vormen van een zin waaruit met bepaalde tekens gebruikt tot vorming van een paswoord.

7.2 Clean Desk

Een clean desk policy houdt in dat alle medewerkers ervoor dienen te zorgen dat informatiesystemen, documenten en gegevensdragers niet onbeheerd in ruimten worden achtergelaten, waardoor de kans op verlies, diefstal of beschadiging van gevoelige informatie en bedrijfsmiddelen vermindert. Met een clean desk policy laat de hulpverleningszone duidelijk zien dat ze zorgvuldig omgaat met persoonsgevoelige gegevens.

- tijdens de dag bij verlaten van werkplek: locken van scherm (via de windows-toets + letter 'L');
- sluiten van gevoelige dossiers;
- zoveel mogelijk beveiligd afgedrukte gebruiken en afgedrukte bestanden niet laten liggen aan de printers.

Op het einde van uw dagtaak:

- sluit uw PC af;
- berg je alles op in uw kast(en) of lade(s) en vergrendel deze indien er persoonsgegevens bewaard worden;
- laat niets rondslingeren op de topbladen van de kasten;
- laat geen rommel rondslingeren;
- versnipper papierafval met persoonsgegevens;
- kleef niets op kasten of schermen;
- sluit jouw kasten;



- sluit alle ramen;
- sluit ook lokalen die gevoelige gegevens of middelen bevatten.

Jaarlijks opruimen:

- opruimen van digitale schijfruimtes – oude bestanden die niet meer van dienst zijn of waarvan de bewaartermijn is verstreken verwijderen;
- verwijder gearchiveerde dossiers die de bewaartijd overschreden hebben.

Wanneer een medewerker vermoedt dat iemand misbruik maakt van materiaal dat onbeheerd is achtergebleven, moet hij dit zo snel mogelijk melden aan de betrokken leidinggevende of het informatieveiligheidsteam.

7.3 Antivirus

Bestanden die van buiten de hulpverleningszone afkomstig zijn, inclusief van huis meegenomen dragers (bv. memorystick ...), bestanden die van het internet gedownload zijn (via online diensten, nieuwsgroepen, bulletin boards en andere), bijlagen bij e-mailberichten en door externe personen verstrekte bestanden, kunnen gevaarlijke computervirussen of malware bevatten die het computernetwerk kunnen beschadigen.

Wanneer een gebruiker twijfelt of een bepaald bestand (bv. bijlage aan e-mail) besmet is met een virus neemt hij/zij contact op met de technisch beheerder. In geval van twijfel mag het bestand niet geopend noch bewaard worden op het netwerk vooraleer dit nagekeken werd door de technisch beheerder.

Gebruikers mogen enkel opslagmedia zoals memory sticks, CD Roms of externe harde schijven gebruiken die van de hulpverleningszone zelf afkomstig zijn en brengen deze enkel via een streng beveiligde computer bij ICT op het netwerk zodat het materiaal en de data eerst gescand wordt met een antivirus en -malware software van de hulpverleningszone.

Indien je wordt geconfronteerd met een virus, je computer begint zich verdacht te gedragen, een verdachte e-mail of een verdacht document, moet er onmiddellijk gestopt worden met werken op het ICT-middel, deze afgekoppeld worden van het netwerk en/of het opslagmedium wordt verwijderd van het toestel. **Er dient onmiddellijk contact opgenomen te worden met de ICT-Dienst.**

7.4 Malware en Spam

Malware is een samenvoeging van het Engelse malicious en software (kwaadwillende software) en een verzamelnaam voor kwaadaardige en/of schadelijke software. Malware behoort tot de grootste bedreigingen van ICT-infrastructuur en de daarbinnen aanwezige bedrijfsinformatie door gebruik te maken van **zwakheden in software** (soms ook in hardware) en **onachtzaamheid van gebruikers**. De gevolgen van een malware-infectie kunnen zeer schadelijk en riskant zijn, en leiden tot uitval van systemen, vertraging bij het gebruik van systemen, overname van controle over systemen, het niet beschikbaar zijn van informatie of zelfs het verlies van informatie. Er zijn verschillende malware-varianten. De volgende varianten behoren tot de meest voorkomende malware: virus, worm, spyware, adware, Trojan, tracking cookie, dropper, dialer, rootkit, backdoor, rogueware, ransomware.

Spam slaat op e-mails die zorgen voor de verspreiding van grote getalen van ongewenste berichten die mogelijk malware of virussen kunnen bevatten. Maatregelen tegen Spam en



Malware rusten op verschillende pijlers van de organisatie, nl. beleid, ICT infrastructuur en bewustwording. Een goede samenhang van de verschillende pijlers beoogt de hoogste graad van bescherming. Het 'beleid' dient procesmatig te wijzen op veilige werkmethodes en het veilig gebruiken van middelen. Daarnaast voorzien zij in de nodige budgetten teneinde adequate 'ICT infrastructuur' te kunnen inrichten waardoor de meeste Spam en Malware automatisch worden tegengehouden. Voor systeembeheer is patch management de belangrijkste maatregel en het technisch laten functioneren en controleren van anti-malware software op de verschillende ICT-componenten. Verder dienen zij op de verschillende ICT Componenten notificatie te voorzien zodat alarmering onmiddellijk gebeurt bij een mogelijke besmetting.

De laatste pijler 'Bewustwording' zorgt dat gebruikers abnormale mails en computergedrag herkennen waardoor de opstart van malware wordt verhinderd of de verspreiding ervan wordt belemmerd. De reactiesnelheid van de gebruikers bij abnormaal computergedrag en de onmiddellijke melding aan ICT van mogelijke malware of virussen bepalen in grote mate de mogelijke impact van malware of virussen. Bewustwording zal tevens de gebruikers leren wat een veilige ICT-omgeving inhoudt en wat de risico's zijn van onbeveiligd werken.

7.5 Web filtering

Alle gebruikers dienen zich bewust te zijn van het feit dat de toegang tot het internet gefilterd, gecontroleerd, opgeslagen en geanalyseerd kan worden in overeenstemming met de terzake geldende wetgeving.

De hulpverleningszone heeft het recht gebruik te maken van software waarmee internetsites die expliciet seksuele of andere, niet voor de werkomgeving geschikt geachte informatie bevatten, geïdentificeerd kunnen worden en waarvan de toegang geblokkeerd kan worden (zgn. URL filtering).

Door middel van deze web filter wordt het internetverkeer beveiligd en opgevolgd.

7.6 Phishing

Verschillende organisaties, instanties en firma's waren al het slachtoffer van phishing - de valse e-mails die in hun naam verstuurd werden zijn vaak nog steeds in omloop.

Het gaat hierbij om o.a.:

- Telecomoperatoren zoals Proximus, Telenet, Orange (Mobistar), Scarlet, KPN Telecom ... ;
- Banken zoals ING, Bpost, Record Bank, BNP Paribas Fortis, Argenta ... ;
- Incassobureaus zoals Intrum Justitia, Nederlands Centraal Justitieel Incassobureau, Trivion Incassobureau ... ;
- Microsoft, Netflix, NMBS, booking.com, bol.com, ziekenfondsen ... ;
- Maar ook ... gemeenten, de Federale Politie en de Hulpverleningszones werden reeds slachtoffer.

Sommige phishing-berichten vragen je online krediet te kopen om een boete te betalen en voegen een link naar de site waar je online kan betalen toe. **Klik nooit op dergelijke link!** Betaal ook nooit een klein "bedragje" op vraag een zogenaamde telefonische hulp of techniek om gezegd de gegevens van je bankrekening te kennen.



Hoe goed herken jij valse e-mails? Doe onze grote [phishingtest](#). Phishing kan op verschillende manieren gebeuren. Hieronder beschrijven we enkele vormen en hoe je best erop reageert.

7.6.1 Verdachte e-mail?

- controleer of er een **vreemde domeinnaam** (gedeelte achter het @ teken) in het e-mailadres staat. Normaal duidt de domeinnaam op de organisatie van wie je e-mail hebt ontvangen. Bv. ...@ethias.be;
- is dat NIET het geval? Klik in geen geval op de link die in de mail staat en open NIET de eventuele bijlagen;
- is dat WEL het geval? Kijk naar waar de eventuele links in het document verwijzen en of deze links naar HTTPS-sites gaan. Scan de documenten op virussen door ze eerst te bewaren alvorens te openen;
- stuur de e-mail door naar verdacht@safeonweb.be;
- verwijder de e-mail(s) meteen, ook uit je prullenbak;
- twijfel je aan bepaalde e-mails verwittig dan de ICT dienst.

7.6.2 Verdacht telefoontje? Ook wel Vishing genoemd.

- geef **nooit persoonlijke gegevens** (zoals identiteitsgegevens, kaartnummers, bankgegevens, wachtwoorden of pincodes) **door**;
- doe zeker nooit een betaling zogenaamd ter verificatie van uw gegevens;
- **beëindig** het gesprek meteen;
- **volg** de instructies **niet op**.

7.6.3 Verdachte sms?

- **volg** de instructies **niet op**;
- **vorm geen speciaal nummer om gezegd een functie/optie te activeren**;
- **verwijder** de sms onmiddellijk.

7.7 Social Engineering

De hacker probeert persoonlijk contact te leggen met het slachtoffer. Hij kan zich bijvoorbeeld voordoen als helpdeskmedewerker en de gebruiker opbellen met het verzoek aan diens gebruikersnaam en wachtwoord door te geven om een probleem te verhelpen. Vooraf aan dit contact verzamelt de hacker gerelateerde informatie over het slachtoffer zodat hij het slachtoffer een overtuigend verhaal kan vertellen. Hiervoor worden zoekmachines als Google, sociale netwerksites als Facebook en andere informatiebronnen op het internet gebruikt. Dit is in de praktijk een eenvoudige en effectieve techniek.

Een andere manier om aan informatie te geraken is via e-mail. Een hacker verstuurt een e-mailtje met een belangwekkende maar vertrouwelijk ogende tekst. Zo zullen ze de logo's en de vertrouwde identiteitsgegevens van de organisatie nabootsen. Deze techniek wordt onder meer uitgevoerd bij de phishing-aanval, waarbij gebruikers ertoe worden verleid om op een authentiek ogende site vertrouwelijke gegevens zoals pincodes, paswoorden en creditcardnummers op te geven. Ook de vele e-mail-wormen, zoals Sober en Klez, hanteren deze techniek, waarbij een vertrouwenwekkend of bangmakend mailtje de gebruikers ertoe verleidt ongemerkt een Trojaans paard te laten installeren. De aanvaller kan daarmee



vervolgens de computer controleren en gebruiken voor zijn eigen doeleinden, zoals het versturen van spam.

Een derde aanvalstechniek is fysisch rondsnoffen. De computerkraker probeert vertrouwelijke informatie te krijgen door het snoffen in vuilnisbakken, containers en prullenbakken. Deze techniek heet dumpster diving. Ook probeert een aanvaller rond te neuzen op de diverse plaatsen bij kopieermachines waar wel eens vertrouwelijke documenten worden weggegooid, of verzameld. Hierbij zal de hacker wel eerst een vorm van insluiping moeten uitvoeren om het gebouw of het terrein waar de vertrouwelijke gegevens te vinden zijn binnen te komen.

8 Aanmelden van storingen, problemen en/of wensen

8.1 Storingen en problemen

Hier maken we een onderscheid tussen dringende en niet dringende storingen en problemen.

Een dringende storing is wanneer omwille van de storing de hulpverlening en werking van HVZ Taxandria in het gedrang komt. Ook wanneer een werknemer zijn taak niet meer kan uitvoeren omwille van een storing of probleem wordt dit als dringend aanzien.

Een niet-dringende storing wil zeggen dat men nog verder kan werken doch dat bepaalde dingen niet correct functioneren.

8.1.1 Dringende Storing

Een dringende storing moet steeds telefonisch gemeld worden aan de ICT-dienst. Hier zal in de mate van het mogelijke onmiddellijk gevolg aan gegeven worden door de ICT-dienst.

8.1.2 Niet-dringende Storing

Niet dringende storingen moeten gemeld worden aan ICT via mail. Probeer je probleem zo volledig mogelijk te omschrijven en te documenteren met screenshots en/of een foto.

9 Incidenten Meldplicht inbreuk persoonsgegevens en sancties

9.1 Contactpersoon meldplicht

Algemeen mailadres voor het melden van incidenten is: privacy@hvztaxandria.be

Vergeet ook zeker niet de **verantwoordelijke afdeling** te verwittigen en/of voor technische zaken de **ICT Dienst**.

9.2 Meldingsplicht

De GDPR voert een nieuw meldsysteem in voor inbreuken op de beveiliging en het lekken van persoonsgegevens. De GDPR omschrijft dit begrip in artikel 4.12 als volgt: 'een inbreuk op de beveiliging die per ongeluk of op onrechtmatige wijze leidt tot de vernietiging, het



verlies, de wijziging of de ongeoorloofde verstrekking van of de ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte gegevens’.

Een inbreuk in verband met persoonsgegevens kan, wanneer dit probleem niet tijdig en op passende wijze wordt aangepakt, resulteren in lichamelijke, materiële of immateriële schade voor natuurlijke personen, zoals verlies van controle over hun persoonsgegevens of de beperking van hun rechten, discriminatie, identiteitsdiefstal of -fraude, financiële verliezen, ongeoorloofde ongedaan making van pseudonimisering, reputatieschade, verlies van vertrouwelijkheid van door het beroepsgeheim beschermde persoonsgegevens, of enig ander aanzienlijk economisch of maatschappelijk nadeel voor de natuurlijke persoon in kwestie.

Voorbeelden van incidenten:

- phishingmail met een link ontvangen waarop je geklikt hebt;
- een pop-up op het scherm van een medewerker dat aangeeft dat er malware (bv. een virus) is gedetecteerd op de computer van de medewerker;
- een collega geeft het privé Gsm nummer aan een burger i.v.m. een actuele opdracht, maar de burger misbruikt te pas en te onpas dit contactnummer en geeft het bovendien nog door aan andere kennissen;
- camerabeelden die via Wetransfer werden verzonden (aan lokale politie) en die door een onbevoegde onderschept zijn om gebruikt te worden om personen af te persen;
- de diefstal/gebruik van identiteitsgegevens van andere collega/burger (elektronische identiteitskaarten, paspoorten, certificaten);
- de diefstal van officiële stempels voor op documenten uit te vaardigen door het bestuur;
- verloren of gestolen apparatuur welke informatie/persoonsgegevens bevat
 - (radiozender, computerapparatuur en randapparatuur met gegevensdragers, Smartphones ...);
- een interventieverslag met niet bewezen feiten verstuurd aan de verkeerde bestemming verzekering tegenpartij;
- delen uit interventieverslagen/personneelsdossiers die zonder meer in het algemeen papierafval terechtkomen, en gelezen en verspreid worden door externen (niet bevoegden);
- ongeoorloofde opzoeking en informatieverschaffing op vraag van derden (al dan niet onder dwang of als drukingsmiddel en reactie op beleidsbeslissingen);
- een tijdelijke medewerker die toegang krijgt tot gevoelige dossiers door een onbewaakte computer of door niet opgeborgen dossier;
- toegang tot persoonsgegevens door foutief ingestelde toegangsrechten;
- een sleutel verloren van een ruimte of kast waar persoonsgegevens worden bewaard.

Volgens de GDPR dienen incidenten binnen de 72u aan de toezichthoudende autoriteit, in ons geval het GBA, gemeld te worden door de Data Protection Officer (DPO). Zie ook <https://www.gegevensbeschermingsautoriteit.be/professioneel/acties/datalek-van-persoonsgegevens>

Daarnaast is het belangrijk dat we leren uit mogelijke incidenten en zo mogelijk maatregelen treffen om de kans en gevolgen van risico's te beperken of uit te sluiten. Het is dan ook nodig



dat we met het informatieveiligheidsteam incidenten evalueren, de risico's en maatregelen in kaart brengen en opvolgen.

9.3 Meldingsprocedure

Incidenten of inbreuken dienen we in het kader van de privacywetgeving (GDPR) te registreren en te documenteren (art 33§5).

Indien er een reële kans is dat persoonsgegevens zijn geëkt, dienen we dit incident te melden bij de GBA (Gegevensbeschermingautoriteit). Wanneer we achten dat er geen melding aan de GBA nodig is, dienen we deze beslissing te argumenteren.

Daarnaast, indien de kans reëel is op enige vorm van schade/gevolgen voor één of meerdere natuurlijke personen, dienen we het incident eveneens te melden aan de betrokkene(n).

Ook hier moeten we staven wanneer we de melding niet doen. Voor melding van een incident aan de GBA dienen we het formulier te gebruik zoals beschikbaar op de website van GBA, welke terug te vinden is onder volgende link: [meldformulier-voor-gegevenslekken](#)

Interne verwerking incident:

- Incident registreren in het 'incidentenregister'
- Registratie met volgende gegevens:
 - omschrijving Incident;
 - vastgesteld door;
 - datum en tijd vaststelling;
 - datum en tijd voorval incident;
 - manier van vaststelling en/of melding: vb. melding via telefoon;
 - oorzaak incident: vb. intern/extern - systeem technische fouten/menselijke fouten accidenteel/kwaad opzet;
 - aard van getroffen gegevens: welk soort gegevens werden geïmpacteerd?
Voorbeelden zijn: persoonsgegevens, medische gegevens, rijksregisternummer, financiële gegevens, login gegevens, beeldmateriaal, enz. aard van de gegevens die getroffen zijn door het gegevenslek;
 - betrokkene(n) van wie gegevens geëkt;
 - onmiddellijke maatregelen risicobeperking;
 - onmiddellijke maatregelen risicobeperking;
 - datum en tijd tijdelijke maatregelen;
 - classificatie;
 - geschatte impact/gevolgen;
 - GBA ingelicht? argumentatie + volledige of tijdelijke melding + datum;
 - betrokkene(n) ingelicht? argumentatie + datum;
 - nog te nemen maatregelen organisatorisch: mens en organisatie;
 - nog te nemen maatregelen technisch: techniek en middelen;
 - verantwoordelijke maatregelen;
 - datum en tijd planning definitieve maatregelen;
 - datum en tijd uitvoering definitieve maatregelen;
 - evaluatie: verholpen, laag risico, blijvend risico, blijvend hoog risico;
 - status: 'Gemeld', 'In behandeling', 'Nog Evalueren', 'Afgewerkt'.



- Verwittigen van de betrokken dienst zodat zij zo mogelijk eerst maatregelen treffen om het incident en de gevolgen te beperken.
- Verwittigen van het IVT en de DPO's.
- Indien de kans reëel is dat persoonsgegevens geëkt geweest zijn, melding nodig bij GBA – invullen en koppelen formulier GBA; indien we niet melden dienen we te argumenteren waarom niet.
- Indien de kans reëel op enige vorm van schade/gevolgen voor één of meerdere natuurlijke personen dienen we ook een melding te doen aan de betrokken personen zelf. Dit in zoverre de inspanning om de melding uit te voeren niet buitenproportioneel is t.o.v. de mogelijk schade/gevolgen. Indien de individuele melding niet mogelijk is overwegen we een melding via publieke media, voor zover deze berichtgeving niet een gevaar vormt voor een strafrechtelijk of bestuurlijk onderzoek. Bij twijfel vragen we eerst het advies bij het GBA.
- Vervolgens met de verantwoordelijke dienst/organisatie bepalen of nog verdere maatregelen (organisatorisch of technisch) nodig zijn om de kans op herhaling en/of de impact en gevolgen te beperken. Deze gegevens eveneens in de ISLP melding ingeven.
- Tot slot met het IVT en de verantwoordelijke dienst de incidenten, de getroffen maatregelen en de gevoerde communicatie(s) evalueren en opvolgen tot het incident kan worden afgesloten.



9.4 Sancties

We streven ernaar om in een 'open cultuur' om te gaan met informatieveiligheid en privacy. Het is belangrijk dat mensen niet geremd zullen zijn om inbreuken/incidenten te melden, zodat de organisatie onmiddellijk de nodige maatregelen kan treffen om de schade te beperken. We zullen dan ook steeds trachten om in onderlinge communicatie onze medewerkers te informeren over hoe we de kans op incidenten kunnen uitsluiten of minimaliseren. Enkel in laatste instantie of bij het doelbewuste niet naleven van deze gedragscodes kunnen de vastgestelde inbreuken op deze policy aanleiding geven tot sancties. Hiervoor verwijzen we voor het administratief personeel en het operationeel personeel van de hulpverleningszone naar het resp. [arbeidsreglement](#) zoals goedgekeurd door de zoneraad.

De werkgever kan de toegang tot de bedrijfssystemen geheel of gedeeltelijk intrekken:

- om de belangen van de organisatie te beschermen;
- om dienstredenen (bv. om de continuïteit van de dienst te vrijwaren);
- om de veiligheid van de medewerkers en de hulpverleningszone te vrijwaren;
- bij een overtreding van deze gedragscode of van andere onderrichtingen;
- wanneer de toegang niet langer kan worden gerechtvaardigd.

Deze opsomming is niet limitatief.

Voor zwaardere inbreuken op informatieveiligheid en/of schendingen van het beroepsgeheim verwijzen we naar het Koninklijk Besluit tot bepaling van het administratief statuut van het operationeel personeel van de hulpverleningszones; Boek 10' - 19 april 2014.

Voor administratieve medewerkers verwijzen we naar de [rechtspositieregeling \(RPR\)](#).



10 Privacy, toezicht en controle

10.1 Geen Privacy waarborg

Medewerkers worden voor het verrichten van hun werkzaamheden voorzien van computers en krijgen toegang tot het netwerk en internet ter ondersteuning van de dienstverlening. Zij mogen bij gebruikmaking van de computerapparatuur van de hulpverleningszone niet veronderstellen dat hun privacy bij al wat zij aanmaken, opslaan, verzenden of ontvangen gewaarborgd blijft.

De computerinfrastructuur is eigendom van de hulpverleningszone en het gebruik wordt gedeeld in de hulpverleningszone, waardoor mogelijk zaken die voor privédoeleinden werden verricht, onvrijwillig kunnen worden opgemerkt door collega's en/of ICT-monitoringssystemen. Wij vragen dan ook om het privégebruik op onze computerinfrastructuur in dit kader te beperken en zeker zaken te vermijden die voor u persoonlijk heel privacy gevoelig liggen.

10.2 Toezicht en controle

De hulpverleningszone respecteert het recht op bescherming van de persoonlijke levenssfeer waarover de gebruikers van ICT-middelen beschikken in het kader van de arbeidsrelatie en van de rechten en plichten die deze relatie met zich meebrengt voor alle partijen.

De gebruikers erkennen het principe volgens hetwelk de hulpverleningszone het recht heeft toezicht en controle uit te oefenen op het gebruik informatiesystemen door de werknemers in het kader van de uitoefening van hun contractuele verplichtingen, ook wanneer dit gebruik onder de persoonlijke levenssfeer valt.

10.2.1 Doeleinden van de controle

De controle van elektronische communicaties is enkel mogelijk voor het nastreven van volgende doelstellingen:

- het voorkomen van ongeoorloofde of lasterlijke feiten, feiten die strijdig zijn met de goede zeden of de waardigheid van een andere persoon kunnen schaden;
- de bescherming van de belangen van hulpverleningszone die vertrouwelijk zijn alsook het tegengaan van ermee in strijd zijnde praktijken;
- de veiligheid en/of de goede technische werking van de IT-netwerksystemen van de hulpverleningszone, met inbegrip van de controle op de kosten die ermee gepaard gaan alsook de fysieke bescherming van de installaties van de onderneming;
- de naleving te goeder trouw van de in hulpverleningszone geldende principes en regels voor het gebruik van communicatiemiddelen en online technologieën.

De analyse van de gegevens over het gedrag of de activiteiten van een personeelslid worden slechts uitgevoerd indien er ernstige aanwijzingen bestaan die een laakbaar, ongepast of verboden gedrag doen vermoeden, of als er bijzondere omstandigheden zijn die rechtvaardigen dat de verzamelde gegevens worden geraadpleegd. Deze controle kan enkel uitgevoerd worden in opdracht van de zonecommandant en mag in principe geen inmenging in de persoonlijke levenssfeer van de gebruiker tot gevolg hebben. Als de controle toch een



inmenging in de persoonlijke levenssfeer tot gevolg heeft, zal deze inmenging tot een minimum beperkt worden.

Indien naar aanleiding van een globale controle of op basis van een officiële klacht onregelmatigheden worden vastgesteld in het kader van de controledoeleinden vermeld in de punten van 10.2.1 (doeleinden van de controle), kunnen de gegevens direct geïndividualiseerd worden teneinde de identiteit te achterhalen van de perso(o)n(en) die verantwoordelijk is (zijn) voor de onregelmatigheid. Dit kan enkel uitgevoerd worden na opdracht van de zonecommandant.

Als de doelstelling echter verband houdt met het te goeder trouw naleven van de in de onderneming geldende regels en beginselen inzake het gebruik van de technologieën, gebeurt de individualisering volgens een driestappenprocedure:

- **Voorafgaande voorlichting:**

De gebruiker wordt vóór elke individualisering op de hoogte gebracht van de niet-naleving van één van de in de onderneming vastgestelde gebruiksregels. Deze voorlichting heeft tot doel de gebruiker op een duidelijke en begrijpelijke wijze in te lichten over het bestaan van de onregelmatigheid en over het feit dat de elektronische online communicatiegegevens geïndividualiseerd zullen worden wanneer een dergelijke onregelmatigheid opnieuw vastgesteld wordt.

- **Geïndividualiseerde controle:**

Wanneer er opnieuw een onregelmatigheid vastgesteld wordt, kan er overgegaan worden tot een geïndividualiseerde controle teneinde de identiteit op te sporen van de persoon (of personen) die verantwoordelijk is (zijn) voor de onregelmatigheid

- **Opvolging van het incident:**

De geïdentificeerde gebruiker heeft de mogelijkheid om tijdens een onderhoud uitleg te geven. Dit onderhoud heeft plaats vóór iedere beslissing of evaluatie die de gebruiker individueel kan raken. Het onderhoud heeft tot doel de gebruiker de kans te geven zijn bezwaren met betrekking tot de voorgenomen beslissing of evaluatie uiteen te zetten en het gebruik van de hem ter beschikking gestelde elektronische online communicatiemiddelen te rechtvaardigen. Tijdens dit onderhoud kan de gebruiker zich eventueel, op zijn verzoek, laten bijstaan door zijn vakbondsafgevaardigde.

11 Overige bepalingen

Deze gedragscode ICT en Informatieveiligheid wordt ingevoerd in onze hulpverleningszone via een intentieverklaring waarbij we als interne en externe medewerker van de hulpverleningszone, zoals bepaald in [1.3 Toepassingsgebied](#), zo goed mogelijk zullen trachten deze gedragscode na te leven.



Aangezien dit een eerste versie is van de gedragscode kan het zijn dat er nog mogelijk fouten of onduidelijkheden kunnen bevatten. Eventuele opmerkingen, onduidelijkheden of aanvullingen kan je doorgeven via het mailadres privacy@hvztaxandria.be.



Bijlage 6 : Integraal alcohol- en drugsbeleid

1. Inleiding

Het alcohol- en drugsbeleid van hulpverleningszone Taxandria heeft als doel om functioneringsproblemen ten gevolge van alcohol -en/of druggebruik te voorkomen en adequaat te reageren wanneer deze zich toch voordoen. Het is tevens een middel om deze problemen een stap voor te blijven of ten minste het verergeren van de problematiek te voorkomen.

Belangrijk in dit beleid is de verantwoordelijkheid van alle personeelsleden van de zone, leidinggevend, administratieve en operationele medewerkers, ambulance en brandweer; beroeps- en vrijwilligerskader. De nadruk wordt gelegd op een sterke preventieve benadering, waarbij het de voornaamste bedoeling is eenieder te confronteren met de mogelijke gevolgen die het gebruik van alcohol en/of drugs kan hebben binnen de werksituatie. Transparantie, professionalisme, efficiëntie, en de waarden integriteit en respect zijn sleutelwoorden voor het alcohol- en drugsbeleid van onze zone.

De te volgen regels en procedures voor het uitvoeren van een alcohol of drugtest zijn opgenomen in boek 11 (KB1) en moeten onverminderd worden toegepast.

De concrete regels die opgenomen zijn slaan op:

- de aard van de testen die kunnen afgenomen worden;
- de werknemers die aan de testen kunnen onderworpen worden;
- de procedure die gevolgd moet worden bij het afnemen van deze testen;
- de personen die bevoegd zijn voor het afnemen van deze testen;
- de tijdstippen waarop kan getest worden;
- de mogelijke gevolgen van een positief testresultaat

Voor het administratief personeel moet de graad van officier zoals opgenomen in art 280 (KB1) worden begrepen als directeur bedrijfsvoering. De regels en procedures worden opgenomen in de rechtspositieregeling.

Het integraal alcohol- en drugsbeleid is opgesplitst in vier deelsegmenten, de vier pijlers.

De eerste pijler is het voorkomingsbeleid, preventiebeleid. Het zijn de regels voor de personeelsleden i.v.m. het gebruik van alcohol en/of drugs. Deze regels geven de grenzen aan om functioneringsproblemen ten gevolge van alcohol en/of drugs te voorkomen.

De tweede pijler behandelt de mogelijke procedures voor het aanpakken van functioneringsproblemen. De rol van de leidinggevende is hierbij cruciaal, onder meer voor de opvolging van het personeelslid.

De derde pijler is een zeer belangrijke pijler voor het welslagen van het alcohol- en drugsbeleid. Deze pijler is de interne hulpverlening met garantie van vertrouwelijkheid en respect voor de privacy van het individu. De zone moet binnen de organisatie een kader creëren waarin de arbeidsarts, de vertrouwenspersonen, de preventieadviseur, preventieadviseur psycho-sociaal welzijn, enz. op optimale wijze hun rol in het integraal alcohol- en drugsbeleid kunnen opnemen.

De vierde pijler is informatie verstrekken en opleiden. Zowel leidinggevend en als medewerkers moeten transparant geïnformeerd en/of opgeleid worden over het beleid en passende instructies krijgen. De leidinggevende moet alert zijn voor alcohol- en drugsproblemen en tussenkomen wanneer dat vereist is.

Over de vier pijlers heen wordt er ingezet op de primaire preventie: voorkomen; de secundaire preventie: vaststellen om erger te voorkomen en de tertiaire preventie: de interne hulpverleningsmogelijkheden en opvolging.

2. Uitgangspunt

Als hulpverleningszone kunnen we stellen dat alle personeelsleden een voorbeeldfunctie hebben. Voor werkgerelateerd gebruik van alcohol geldt een principieel verbod. Dit omvat elk gebruik kort voorafgaand aan het werk of tijdens de werktijd, inclusief de lunchpauzes en de weg naar het werk. Voor niet-alcoholische dranken die de perceptie van alcoholgebruik zouden kunnen geven, geldt eenzelfde uitgangspunt voor wat betreft gebruik kort voorafgaand aan het werk of tijdens de werktijd, inclusief de lunchpauzes.

Het uitgangspunt van het alcohol- en drugsbeleid van de zone bestaat erin om het disfunctioneren op het werk ten gevolge van middelengebruik te voorkomen en te verhelpen. Dit geldt voor alle personeelsleden. Alle personeelsleden hebben hun rol en verantwoordelijkheid. Informele en dagelijkse contacten, evenals formele gesprekken in geval van functioneringsproblemen, zijn zeer belangrijk om mogelijke problemen vroegtijdig te detecteren, escalatie te voorkomen en verbetering te bewerkstelligen. De rol van aangepaste begeleiding intern en extern en een daadwerkelijke opvolging door de leidinggevend en zijn van essentieel belang.

Voor wat het gebruik van illegale drugs betreft, geldt een absoluut verbod. De zone verwacht dat de personeelsleden deze nultolerantie respecteren en zich ook buiten de diensturen onthouden van het gebruik van illegale middelen.

Volgende doelstellingen en acties worden vooropgesteld:

- Bewustmaken en bespreekbaar maken van de problematiek binnen onze organisatie;
- Sensibilisering van alle personeelsleden met betrekking tot deze problematiek, eveneens bij sociale activiteiten die werkgerelateerd zijn;
- Voorkomen dat het gebruik van alcohol overgaat in probleemgebruik;
- Aandacht hebben voor de problematiek binnen de opleidingen;
- Het opleggen van een principieel verbod op werkgerelateerd gebruik van alcohol. De omstandigheden en de voorwaarden waaronder afwijkingen op dit principiële verbod mogelijk zijn, zullen specifiek worden vastgelegd;
- Het doen naleven van het absoluut verbod van illegale drugs;
- Vanuit de evaluatie van het functioneren van medewerkers toezien op een zo vroeg mogelijke herkenning van probleemsituaties, met bijzondere aandacht voor de bepalende rol van alle leidinggevend en;
- Het vastleggen van een procedure voor de verwijdering van het personeelslid van de werkvloer indien een disfunctioneren van de werknemer mogelijk te wijten is aan alcohol- en/of druggebruik;
- Het zorgen voor een begeleiding van probleemgebruikers, in overleg met de interne en externe dienst preventie en bescherming op het werk.

3. Regels en afspraken

Dit deel bevat de regels die gelden voor wat betreft de beschikbaarheid van alcohol en drugs op de werkplaats en wordt het principieel verbod op werkgerelateerd gebruik verder toegelicht. De bedoeling is duidelijk aan te geven welk gedrag niet getolereerd wordt binnen de organisatie.

Voor wat illegale drugs betreft geldt er een absolute nultolerantie voor wat betreft het bezit, gebruik, de verkoop en de verdeling van illegale drugs. Dit geldt ook voor het occasioneel recreatief gebruik

De personeelsleden gebruiken geen alcohol bij het uitoefenen van hun taak, tijdens de dienst, tijdens de wachtdienst, als men zich beschikbaar heeft gesteld op de arbeidsplaats. Zij waken er bovendien over om zich bij de aanvang van de dienst niet onder invloed van alcohol aan te bieden. Van personeelsleden wordt verwacht dat zij hun taken uitvoeren zonder enige indicatie van alcoholgebruik.

Werkgerelateerd alcoholgebruik wordt niet getolereerd. Door de zonecommandant kan toestemming worden verleend om voor bepaalde gelegenheden festiviteiten, georganiseerde activiteiten,... af te wijken van deze regel. Ongeacht de toestemming van de zonecommandant is het eenieders verantwoordelijkheid de wetgeving betreffende de verkeersveiligheid en openbare dronkenschap na te leven.

Het gebruik van medicatie op voorschrift van de behandelende arts is een persoonlijke aangelegenheid. Sommige medicijnen zoals slaap- en kalmeringsmedicijnen, medicijnen tegen depressie, allergie of psychose, zware pijnstillers maken suf en slaperig. Het behoort tot de verantwoordelijkheid van het personeelslid die de middelen kreeg voorgeschreven om de arbeidsarts hierover in te lichten. Het is aan het personeelslid om erover te waken dat de eventuele nadelige gevolgen van het gebruik van medicatie op geen enkele manier een invloed kan hebben op de omgeving van het personeelslid en op de werkvloer. Mochten er toch functioneringsproblemen voordoen, die mogelijk te wijten zijn aan gebruik van voorgeschreven medicatie, dan bespreekt de hiërarchische leidinggevende in overleg met de arbeidsarts dit met het personeelslid.

4. Procedure bij illegale drugs

Voor illegale drugs geldt een absoluut verbod. Bij kennisname of vaststelling van drugsfeiten wordt de politie verwittigd en wordt een proces-verbaal opgemaakt. Bij vaststelling of kennisname van drugsfeiten via de gerechtelijke overheden zal de regelgeving en procedure opgenomen in boek 10 (KB1) : 'Tuchtregeling' en boek 12 (KB1): 'schorsing in het belang van de dienst' worden gevolgd. Voor het niet operationeel personeel wordt in de rechtspositieregeling de procedure en regelgeving opgenomen.

5. Vaststelling van een functioneringsprobleem bij een medewerker

Een functioneringsprobleem stelt zich als een medewerker de normale verwachtingen van de arbeidsrelatie niet meer nakomt met als gevolg dat hij/zij op dat ogenblik niet meer vlot en efficiënt functioneert. Wanneer een medewerker niet functioneert zoals het zou moeten, kan dit risico's inhouden voor het welzijn en veiligheid van de personeelsleden, de dienstverlening naar de burger en de verhoging van het risico op arbeidsongevallen. Het functioneringsprobleem kan mogelijk zijn oorzaak vinden in alcohol, drugs, medicatie. Iedereen die in contact komt met de betrokkene kan de leidinggevende inlichten over het disfunctioneren.

Indien de leidinggevende opmerkt dat de medewerker geen controle meer heeft over zijn handelingen, zal deze de nodige veiligheidsmaatregelen nemen en het personeelslid verzoeken zijn/haar werkzaamheden onmiddellijk te stoppen.

De leidinggevende zal nagaan of het verlies van controle en/of functioneringsproblemen vermoedelijk ten gevolge zijn van alcoholgebruik.

Indien de leidinggevende vermoedt of vaststelt dat de functioneringsproblemen het gevolg zijn van een andere oorzaak dan gebruik van alcohol of illegale drugs zullen aangepaste maatregelen moeten worden voorzien in overleg met de arbeidsarts en/of directeur bedrijfsvoering. Deze maatregelen maken geen onderdeel uit van dit document.

6. Functioneringsproblemen vermoedelijk ten gevolge van alcoholgebruik en/of druggebruik

Bij functioneringsproblemen waarbij het gedrag van het personeelslid vermoedelijk te wijten is aan alcoholgebruik zal de leidinggevende het disfunctioneren schriftelijk vastleggen. De leidinggevende noteert een kort verslag in het voorlichtingsrapport met vermelding van datum, uur en plaats. De naam van de persoon die de leidinggevende op de hoogte gebracht heeft van het disfunctioneren moet worden opgenomen in het verslag.

De medewerker kan aan een ademtest en/of speekseltest onderworpen worden. Het personeelslid mag een wachttijd vragen van 15 minuten.

De medewerker dateert en tekent het verslag voor kennisname op het document. Bij niet tekenen van het verslag of bij niet akkoord, vermeldt de medewerker de reden van niet ondertekening.

De medewerker kan zelf vragen om aan een ademtest en/of speekseltest onderworpen te worden om het vermoeden van misbruik te weerleggen.

Indien de ademtest $\neq$ S of de ademanalyse voor de opsporing van alcohol een resultaat meet dat ten minste gelijk is aan de norm, bepaald in de wetgeving (W4), moeten onmiddellijk veiligheidsmaatregelen genomen worden.

Indien de speekseltest voor de opsporing van drugs een positief testresultaat geeft moeten onmiddellijk veiligheidsmaatregelen genomen worden.

Dit omwille van de veiligheid van het personeelslid, de omgeving en de andere personeelsleden.

Volgende veiligheidsmaatregelen moeten genomen worden :

- De leidinggevende zal het personeelslid verzoeken zijn/haar werkzaamheden onmiddellijk te stoppen.
- Het personeelslid mag niet deelnemen aan de uitvoering van de opdrachten van zijn ambt afhankelijk van het resultaat van de ademtest, ademanalyse of speekseltest zoals opgenomen in punt 9 ' Procedure en regels bij vaststelling van een functioneringsprobleem bij een medewerker die uiterlijke kenmerken van mogelijk alcohol- en of drugsmisbruik vertoont.'
- Bij medische problemen onmiddellijk contact opnemen met een arts of het noodnummer 112.
- Het personeelslid heeft recht op een telefoontje om te voorzien in vervoer. Alle kosten van vervoer vallen ten laste van het betrokken personeelslid.
- Bij agressie of indien nodig, de noodzakelijke politionele maatregelen laten stellen bijvoorbeeld bij het willen besturen van een voertuig.

Bij het vermoeden van druggebruik worden de bepalingen opgenomen in '9 In detail : Procedure en regels bij vaststelling van een functioneringsprobleem bij een medewerker die uiterlijke kenmerken van mogelijk alcohol- en of drugsmisbruik vertoont' van kracht.

Opvolging functioneringsproblemen ten gevolge van alcoholgebruik

De leidinggevende overloopt met het betrokken personeelslid het kort verslag in het voorlichtingsrapport en heeft een functioneringsgesprek met de betrokkene voor aanvang van de volgende dienst, indien dit door omstandigheden niet mogelijk is, zo snel mogelijk ten laatste binnen de week na hervatting van de dienst. Het functioneringsgesprek wordt vastgelegd in een verslag. Dit verslag kan worden gebruikt als basis indien een gelijksoortig disfunctioneren opnieuw voorvalt.

Dit functioneringsgesprek heeft volgende doelstellingen:

- vaststellen of de betrokkene goed kan functioneren;
- de vastgestelde feiten bespreken en de betrokkene de kans geven over de feiten na te denken en uitleg te verschaffen;
- op een constructieve wijze de invloed van het disfunctioneren op de werkvloer, organisatie, veiligheid en personeelslid duidelijk maken. Het is belangrijk om erop te wijzen dat de situatie zich niet mag herhalen;
- verwachtingen van de dienst, directe collega's en andere personeelsleden verduidelijken;
- het verslag wordt gedateerd en door beide partijen ondertekend. Indien het personeelslid weigert het verslag te tekenen, wordt hiervan akte genomen in het verslag en zal dit verslag per aangetekend schrijven aan hem/haar bezorgd worden ter kennisgeving;
- aan de medewerker wordt een kopie van de ondertekende schriftelijke vaststelling en het verslag van het functioneringsgesprek gegeven. De medewerker tekent het verslag van het functioneringsgesprek voor kennisname.

Iemand kan eenmalig te veel drinken, hij/zij is aangeschoten, zat, laveloos of knock-out. Dit is acuut gebruik/misbruik. Het gaat hier om een éénmalig voorval waarbij het gedrag van het personeelslid vermoedelijk te wijten is aan occasioneel alcoholgebruik.

Bij éénmalig acuut gebruik krijgt de betrokkene de mogelijkheid de afwezigheid te regulariseren door het opnemen van verlof, meeruren of opdrachten. Dit wordt opgenomen in het voorlichtingsrapport.

Indien de functioneringsproblemen door alcoholgebruik zich herhalen zal het personeelslid worden geschorst voor de volgende 24 uur na vaststelling, het personeelslid mag zich de volgende 24 uur niet beschikbaar stellen. Voor de duur van schorsing zal het personeelslid geen loon, vergoeding, premie, maaltijdcheque of andere compensatie ontvangen.

Een medisch attest wordt in geen van beide situaties aanvaard als regularisatie.

De te volgen procedure en regels zijn, in detail beschreven, terug te vinden aan het einde van deze bijlage.

Bijkomende opvolging bij recidieven

Vanaf een tweede inbreuk of hervat is verdere opvolging van het personeelslid aangewezen. In overleg met de directeur bedrijfsvoering wordt intern een persoon aangeduid ter ondersteuning van de leidinggevende en als tweede aanspreekpunt voor de betrokkene. Het personeelslid wordt voor externe hulpverlening doorverwezen naar de arbeidsarts. De arbeidsarts wordt door de personeelsdienst of de leidinggevende vooraf geïnformeerd over de feiten. De arbeidsarts zal, na een vertrouwelijk gesprek met het personeelslid, interne of externe hulpverlening op maat voorstellen aan het personeelslid. De arbeidsarts neemt niet de rol op van behandelend arts.

De arbeidsarts informeert de leidinggevende. Indien het personeelslid geen gebruik wenst te maken van deze mogelijkheid, zal dit worden genoteerd in het voorlichtingsrapport. De nodige tijd en eventuele kosten, verbonden aan de hulpverlening, zijn ten laste van het personeelslid.

Een evaluatiemoment wordt door de leidinggevende ingelast één maand na de feiten. Uiterlijk drie maanden na het eerste functioneringsgesprek moet er een opvolgingsgesprek plaatsvinden. Afhankelijk van het functioneren of op vraag van het personeelslid kunnen meerdere opvolgingsgesprekken worden ingepland.

Het voorlichtingsrapport, het verslag van het functioneringsgesprek met eventuele bijlage wordt na een duplicaat te hebben bezorgd aan het personeelslid onder gesloten omslag met vermelding van naam van de betrokkene, datum en het woord 'VERTROUWELIJK' opgenomen in het persoonlijk dossier van de betrokkene bij de personeelsdienst.

De leidinggevende moet erover waken de medewerker niet overmatig aan een ademtest te onderwerpen.

7. Informatie opleiding en hulpverlening

Een integraal alcohol- en drugbeleid kan maar slagen mits motivatie en engagement van elke medewerker. Daarom is het belangrijk om medewerkers op alle niveau's en alle locaties ongeacht statuut te informeren en te sensibiliseren over het belang van een preventieve aanpak en zijn maatschappelijke voorbeeldfunctie. Zeker in uniform is men zeer herkenbaar en is het van belang om correct om te gaan met alcohol en drugs.

Elke medewerker kan op vrijwillige basis een beroep doen op de personeelsdienst voor een vertrouwelijk gesprek ivm zijn/haar alcohol- of drugsproblematiek. Dit vertrouwelijk gesprek valt onder het gedeeld beroepsgeheim. Tijdens een eerste gesprek tracht de personeelsdienst de ernst van het probleem in te schatten en verschaft indien mogelijk informatie over de verschillende andere personen of gespecialiseerde hulpverleningscentra die de medewerker en zijn/haar gezin bij een eventuele behandeling van de specifieke problematiek kunnen ondersteunen. De personeelsdienst staat niet in voor eventuele begeleiding en heeft enkel een informerende functie.

En tot slot: het integraal alcohol- en drugbeleid in onze zone en dit document mag geen statisch gegeven zijn maar moet dynamisch mee-evolueren met de noden van onze personeelsleden en onze hulpverleningszone.

8. Aanvullende informatie

- **Dronkenschap:** de toestand van een persoon die zodanig onder invloed is van alcoholische drank dat hij geen bestendige controle over zijn handelingen meer heeft, zonder daarom noodzakelijk het zelfbewustzijn van deze daden te hebben verloren.
- **Intoxicatie:** de wetenschappelijk verantwoorde kwantitatieve medische vaststelling van het alcoholgehalte in het bloed of de aanwezigheid van drugs in de urine.
- Meetresultaten van alcohol- of drugtesten mogen niet met persoonsgegevens worden opgenomen in een bestand voor verwerking of opvolging.
- De maximaal toegestane alcoholconcentratie voor rijbewijscategorieën C en D is vanaf 01 januari 2015 verlaagd van 0,22 naar 0,09 milligram per liter uitgeademde alveolaire lucht (UAL). Deze alcohollimiet is ook van toepassing op wie beroepsmatig personen vervoert waarvoor dezelfde medische criteria gelden als voor vrachtwagen- en buschauffeurs.

Wetgeving

KB1. (sd). Koninklijk Besluit van 19 april 2014 tot bepaling van het administratief statuut van het operationeel personeel van de hulpverleningszones.

W1. (sd). Wet van 15 mei 2007 betreffende de civiele veiligheid.

W3. (sd). Strafwetboek.

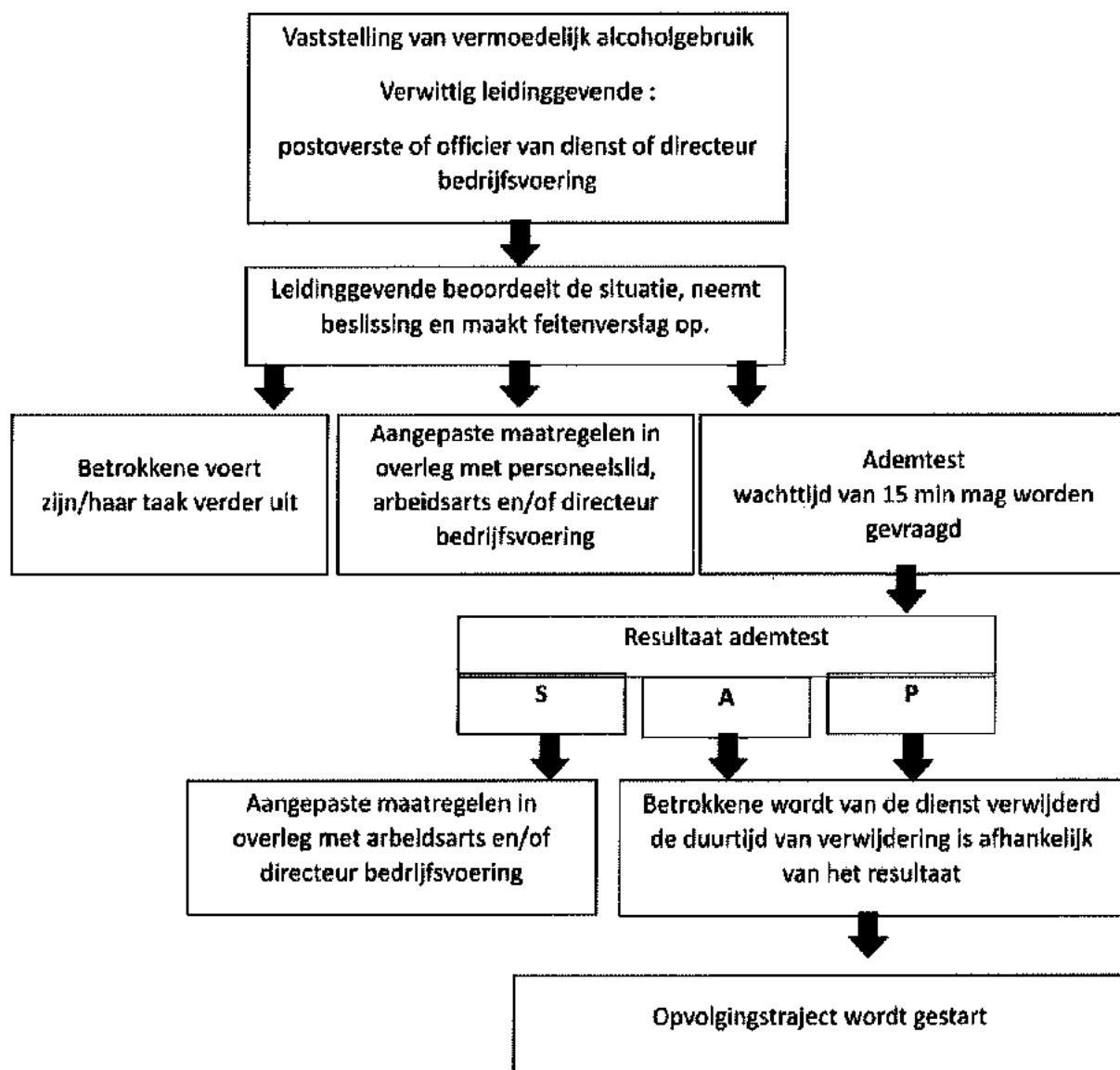
W4. (sd). Wet van 16 maart 1968 betreffende de politie over het wegverkeer Art.60,\$1 eerste lid.

Hulpverlening

<https://www.alcoholhulp.be> : Je drinkt regelmatig en stelt jezelf de vraag of je drinken mogelijk schadelijk is voor je gezondheid. Of je bent gewoon nieuwsgierig. Neem even tijd en vul de test in, nadien krijg je een persoonlijk advies. Deelname is anoniem, je hoeft jezelf dus niet aan te melden.

www.tele-onthaal.be : Je kan er 24u op 24u terecht via chat of telefoonnummer 106.

STROOMSCHEMA BIJ VASTSTELLING VAN FUNCTIONERINGSPROBLEMEN VERMOEDELIJK TEN GEVOLGE VAN ALCOHOLGEBRUIK



9. In detail : Procedure en regels bij vaststelling van een functioneringsprobleem bij een medewerker die uiterlijke kenmerken van mogelijk alcohol- en of drugsmisbruik vertoont.

De zonecommandant of zijn afgevaardigde duidt alle medewerkers aan, die als gedelegeerden zullen optreden bij de afwerking van de hierna uiteengezette procedure tot vaststelling van misbruik van alcohol en/of drugs. Deze ambtenaren worden verder in de tekst aangeduid onder de benaming "de bevoegde ambtenaar". Onder "diensturen" worden alle werkuren/arbeidstijd verstaan die, op welk tijdstip ook, in opdracht van de zone worden gepresteerd.

De bevoegde ambtenaar verwerkt gegevens met betrekking tot de procedure, in het "voorlichtingsrapport vermoedelijk gebruik van alcohol en/of middelen" zie bijlage Formulieren FORM B.1, hierna kortweg "verslag" genoemd.

Conform de onderrichtingen ter zake, vult de bevoegde ambtenaar naargelang het verloop van de procedure de voor hem bestemde rubrieken van het verslag in. Nadat hij/zij de procedure heeft afgewerkt, maakt de bevoegde ambtenaar het verslag over aan de zonecommandant of zijn/haar afgevaardigde. Al wie vaststelt dat een personeelslid (in de tekst verder aangeduid onder de benaming "de betrokkene") tijdens de diensturen hetzij gedragingen vertoont die wijzen op misbruik van alcohol en/of drugs, hetzij alcoholische dranken en/of drugs tot zich heeft genomen, maakt zijn/haar bevindingen onmiddellijk over aan de officier van dienst, deze verwittigt de bevoegde ambtenaar. De bevoegde ambtenaar begeeft zich ter plaatse en vult de volgende gegevens in het verslag: naam, personeelsnummer en functie van de betrokkene evenals de dienst waarop deze is tewerkgesteld de datum, het uur waarop de feiten door hem/haar werden vastgesteld, een gedetailleerde beschrijving van de uiterlijke kentekenen van intoxicatie door alcohol en/of drugs en eventuele getuigen.

De bevoegde ambtenaar vraagt de eventuele getuigen of officier van dienst mede het verslag te ondertekenen. De bevoegde ambtenaar beslist of de betrokkene al dan niet zijn normale taak verder kan uitoefenen. Hij/zij onderwerpt de betrokkene daarvoor aan een ademtest en/of speekseltest.

Er zijn daartoe minstens 2 gehomologeerde apparaten beschikbaar.

De bevoegde ambtenaar treft de nodige maatregelen om dit apparaat ter plaatse te brengen of begeeft zich met de betrokkene naar de plaats waar de test kan worden afgenomen.

Indien bovenvermelde apparaten/testen niet beschikbaar zijn, neemt de bevoegde ambtenaar contact op met het dichtstbijzijnde politiebureau of de dichtstbijzijnde dienst waarop zich een dergelijk toestel bevindt, en meldt aan de dienstverantwoordelijke, dat hij zich met de betrokkene en vergezeld van een getuige voor een ademtest/ speekseltest zal aanmelden.

9.1. Ademtest

Het personeelslid dat verzocht wordt de ademtest te ondergaan mag een wachttijd vragen van vijftien minuten.

Aflezing "A"

Uit de ademtest blijkt dat het alcoholgehalte in de uitgeademde lucht van de betrokkene lager is dan 0,35 mg/liter, maar hoger dan 0,09 mg/liter

- 1 de bevoegde ambtenaar stelt de betrokkene gedurende drie uur na de ademtest op non-actief of schorst de arbeidsovereenkomst en duidt een personeelslid aan om er toezicht op te houden dat de betrokkene zijn bevel naleeft.
- 2 na verloop van deze periode neemt de bevoegde ambtenaar opnieuw een ademtest af van de

betrokkene en laat hem zijn normale taak hervatten indien deze ademtest negatief is (aflezing "S")

- 3 blijft de aflezing "A" dan treft de bevoegde ambtenaar de nodige maatregelen om de betrokkene uit de dienst te verwijderen:
 - a) de bevoegde ambtenaar noteert het uur waarop de betrokkene de dienst verlaat, alsook de naam en het personeelsnummer van de begeleider(s) in het verslag en voegt dit laatste bij het persoonlijk dossier van de betrokkene.
 - b) Hij/zij maakt een kopie van het verslag over aan de arbeidsarts, waarbij hij/hij deze ambtshalve verzoekt de betrokkene op te roepen voor een gezondheidsbeoordeling.
- 4 de bevoegde ambtenaar maakt het verslag over aan de zonecommandant of zijn/haar afgevaardigde.
- 5 de zonecommandant of zijn/haar afgevaardigde neemt kennis van de preventieve voorstellen ter zake van de arbeidsarts, gaat na of de betrokkene al dan niet het voorwerp is van preventieve maatregelen inzake misbruik van alcohol en/of drugs in de voorbije periode van zes maanden en beslist op basis van deze gegevens of hij/zij al dan niet ten laste van de betrokkene een feitenverslag zal opstellen.

Aflezing "P"

Uit de ademtest blijkt dat het alcoholgehalte in de uitgeademde lucht van de betrokkene gelijk aan of hoger is dan 0,35 mg/liter:

- 1 de bevoegde ambtenaar treft de nodige maatregelen om de betrokkene uit de dienst te verwijderen:
 - a) De bevoegde ambtenaar noteert het uur waarop de betrokkene de dienst verlaat, alsook de naam en het personeelsnummer van de begeleider(s) in het verslag en voegt dit laatste bij het persoonlijk dossier van de betrokkene;
 - b) Hij/zij maakt een kopie van het verslag over aan de arbeidsarts, waarbij hij/zij deze ambtshalve verzoekt de betrokkene op te roepen voor een gezondheidsbeoordeling.
- 2 de bevoegde ambtenaar maakt het verslag over aan de zonecommandant of zijn/haar afgevaardigde.
- 3 de arbeidsarts gaat over tot het voorstellen van preventieve maatregelen aan de zonecommandant of zijn/haar afgevaardigde.
- 4 de zonecommandant of zijn/haar afgevaardigde neemt kennis van de preventieve voorstellen ter zake van de arbeidsarts, gaat na of de betrokkene al dan niet reeds het voorwerp is van preventieve maatregelen inzake misbruik van alcohol en/of drugs, en stelt op basis van deze gegevens een feitenverslag op ten laste van de betrokkene.

Aflezing "S"

Uit de ademtest blijkt dat het alcoholgehalte in de uitgeademde lucht van de betrokkene lager is dan 0,09 mg/liter en betrokkene vertoont uiterlijke tekenen van intoxicatie door alcohol en/of drugs.

- 1 De bevoegde ambtenaar zorgt eventueel voor medische hulp en treft de nodige maatregelen om de betrokkene onder begeleiding uit de dienst te verwijderen
- 2 De bevoegde ambtenaar noteert het uur waarop de betrokkene de dienst verlaat, alsook de naam en het personeelsnummer van de begeleider(s) in het verslag en voegt dit laatste bij het persoonlijk dossier van de betrokkene; hij/zij maakt een kopie van het verslag over aan de arbeidsarts, waarbij hij/zij deze ambtshalve verzoekt de betrokkene op te roepen voor een gezondheidsbeoordeling
- 3 De bevoegde ambtenaar maakt het verslag over aan de zonecommandant of zijn/haar afgevaardigde.
- 4 De arbeidsarts gaat indien van toepassing over tot doorverwijzen van de betrokkene en maakt een verslag over aan de zonecommandant of zijn/haar afgevaardigde. Indien er sprake is van mogelijk misbruik van alcohol of drugs gaat de arbeidsarts over tot het voorstellen van preventieve maatregelen aan de zonecommandant of zijn/haar afgevaardigde.

- 5 De zonecommandant of zijn afgevaardigde neemt kennis van het verslag van de arbeidsarts. Afhankelijk van het verslag van de arbeidsarts gaat de zonecommandant of zijn/haar afgevaardigde na of de betrokkene al dan niet reeds het voorwerp is van preventieve maatregelen inzake misbruik van alcohol en/of drugs, en beslist op basis van deze gegevens of hij/zij al dan niet een schriftelijke verwittiging zal overmaken, waarin hij/zij waarschuwt dat bij de eerstvolgende herhaling van een gelijkaardig vergrijp hij/zij mogelijk een feitenverslag zal opstellen.

9.2. Procedure bij 'at random' alcoholtest

Op vraag van de zonecommandant of zijn/haar afgevaardigde zullen de officieren van dienst of postoverste 'at random' alcohol-ademtests afnemen. Die alcohol-ademtests zullen gebeuren: onaangekondigd, op een willekeurig tijdstip, overdag of 's nachts, tijdens weekdays en in het weekend, in een of meerdere posten. De zonecommandant of zijn/haar afgevaardigde onderwerpt op dezelfde wijze de officieren aan de test. Het personeelslid dat verzocht wordt de ademtest te ondergaan mag een wachttijd vragen van vijftien minuten.

Naargelang de uitslag van de ademtest, zal de officier van dienst, de postoverste, de zonecommandant of zijn afgevaardigde (bevoegde ambtenaren) drie gevallen onderscheiden.

Aflezings "S"

Uit de ademtest blijkt dat het alcoholgehalte in de uitgeademde lucht van de betrokkene lager is dan 0,09 mg/liter: de bevoegde ambtenaar laat de betrokkene zijn normale taak verder uitoefenen.

Bij aflezing "A" en aflezing "P"

De bevoegde ambtenaar volgt dezelfde werkwijze als beschreven onder punt 9.1. Ademtest afhankelijk van de aflezing "A" of "P".

9.3. Speekseltest

Bij vermoeden van druggebruik zal het betrokken personeelslid steeds voorwerp uitmaken van een speekseltest. De speekseltest-kits bevinden zich op Noord-Brabantlaan en in de posten te Hoogstraten en Turnhout.

De speekseltest wordt afgenomen door een gedelegeerd medewerker, overeenkomstig de richtlijnen van de fabrikant.

Het afnemen van de speekseltest gebeurt met inachtnaam van de bepalingen van boek 11, titel 3 van het KB administratief statuut.

Indien een positieve speekseltest wordt afgelegd, wordt het betrokken personeelslid van het werk verwijderd tot het einde van de dienst.

9.4. Weerspannigheid

Indien de betrokkene tijdens de procedure weerspannig is (bijvoorbeeld, indien hij/zij weigert de procedure gewillig te ondergaan of de dienst te verlaten, ontoelaatbare daden stelt, enzovoort), zal de bevoegde ambtenaar de betrokkene beschouwen als onbevoegd en hem/haar in het belang van de algemene veiligheid onmiddellijk uit de dienst laten verwijderen.

Hiertoe zal de bevoegde ambtenaar de hulp inroepen van de politie, die een proces-verbaal zal opmaken van de feiten.

De bevoegde ambtenaar vermeldt deze feiten in het verslag en maakt het verslag over aan de zonecommandant.

De zonecommandant maakt ten laste van de betrokkene een feitenverslag op in het raam van de procedure tot aanpak van misbruik van alcohol en/of drugs, waarin hij/zij het gedrag van de betrokkene en de tussenkomst van de politie als bijkomende bezwarende omstandigheden vermeldt.

Het spreekt voor zich dat het stellen van elke ongeoorloofde handeling, al dan niet gepaard met misbruik van alcohol en/of drugs, aanleiding kan geven tot het opstellen van een feitenverslag.

9.4. Weigering een ademtest af te leggen

Indien de betrokkene weigert een ademtest af te leggen, zal de bevoegde ambtenaar handelen als volgt:

- 1 Er bestaan gegronde redenen dat het om misbruik van alcohol gaat:
 - de bevoegde ambtenaar zet de procedure voort alsof een positieve ademtest werd afgenomen
 - de zonecommandant of zijn afgevaardigde stelt ten laste van de betrokkene een feitenverslag op in het raam van de procedure tot aanpak van misbruik van alcohol en/of drugs, waarin hij de weigering een ademtest af te leggen als bezwarend element vermeldt.
- 2 Er bestaan geen gegronde redenen dat het om misbruik van alcohol gaat:
 - De bevoegde ambtenaar zorgt eventueel voor medische hulp en treft de nodige maatregelen om de betrokkene onder begeleiding uit de dienst te verwijderen
 - De bevoegde ambtenaar noteert het uur waarop de betrokkene de dienst verlaat, alsook de naam en het personeelsnummer van de begeleider(s) in het verslag en voegt dit laatste bij het persoonlijk dossier van de betrokkene; hij/zij maakt een kopie van het verslag over aan de arbeidsarts, waarbij hij/zij deze ambtshalve verzoekt de betrokkene op te roepen voor een gezondheidsbeoordeling
 - De bevoegde ambtenaar maakt het verslag over aan de zonecommandant of zijn/haar afgevaardigde.

9.5. Weigering een speekseltest af te leggen

Indien de betrokkene weigert een speekseltest af te leggen, zal de bevoegde ambtenaar handelen als volgt:

- Van de eventuele weigering van de speekseltest en de aangevoerde reden wordt melding gemaakt op het rapport.
- Met een weigering wordt gelijkgesteld, het niet reglementair afleggen van de speekseltest.

Bij een positieve ademen/of speekseltest richt de zonecommandant zich naar de aanwijzingen die de arbeidsarts hem/haar ter zake geeft en evalueert of hij/zij al dan niet een feitenverslag in het raam van de procedure tot aanpak van misbruik van alcohol en/of drugs ten laste van de betrokkene zal opmaken



VERTROUWELIJK

Hulpverleningszone Taxandria

(Dit voorlichtingsrapport is opgenomen in bijlage formulieren FORM B.1)

VOORLICHTINGSRAPPORT VERMOEDELIJK GEBRUIK VAN ALCOHOL EN/OF MIDDELEN

A: VERSLAG

1. Gegevens over het betrokken personeelslid:

Naam:

Personeelsnummer:

Functie:

Post / Dienst:

Adres :

Tel / GSM :

2. Vaststellingen:

Datum en uur van de feiten:

Vaststeller(s): (Naam; graad en functie)

Getuigen: (Naam; graad en functie)

Vastgestelde uiterlijke tekenen:

(kort feitelijk verslag: aanwijzingen die tot de vaststelling leiden)

Uitvoering van een alcoholtest op vraag van leidinggevende: JA/NEE

Resultaat van de ademtest

Uur van vertrek naar de plaats waar het toestel zich bevindt :

Naam van de begeleider(s):

Eerste ademtest werd afgenomen om uur: Resultaat van de ademtest: eerste test:....

Tweede test (15 minuten na de eerste test indien aflezing $\neq$ S)

Resultaat : ...

Resultaat van de ademanalyse op vraag van het betrokken personeelslid :

- Ademanalyse werd afgenomen omuur : Resultaat :

3. Genomen veiligheidsmaatregelen:

Datum en uur van de stopzetting van de activiteit:

Duur van de schorsing: rest van de werktijd/24u

Opgemaakt te.....op.....

Getuigen:

Vaststeller(s):

Personeelslid :

Handtekening:

Handtekening:

Handtekening

(kopie van deze schriftelijke vaststelling wordt aan de medewerker gegeven.)

B: FUNCTIONERINGSGESPREK

(standaardformulier)

C: AFSPRAKEN REGULARISATIE

--

Opgemaakt te.....op.....

Leidinggevende:

Personeelslid

Handtekening:

Handtekening:

D: BIJKOMENDE OPVOLGING

Gegevens ondersteunend personeelslid :

(Naam; graad en functie)

Datum informeren van arbeidsarts :

Datum en kort verslag van de arbeidsarts aan de leidinggevende :

Datum evaluatie (één maand na de feiten):

Kort verslag evaluatie :

Opgemaakt te.....op.....

Leidinggevende:

Personeelslid

Handtekening:

Handtekening:

Datum opvolgingsgesprek (uiterlijk 3 maanden na de feiten):

Kort verslag opvolgingsgesprek :

Opgemaakt te.....op.....

Leidinggevende:

Personeelslid

Handtekening:

Handtekening:

(Dit voorlichtingsrapport is opgenomen in bijlage formulieren FORM B.3) (nieuw formulier)

VOORLICHTINGSRAPPORT VERMOEDELIJK GEBRUIK VAN ILLEGALE DRUGS

A: VERSLAG

1. Gegevens over het betrokken personeelslid:

Naam:

Personeelsnummer:

Functie:

Post/Dienst:

Adres :

Tel / GSM :

2. Vaststellingen:

Datum en uur van de feiten:

Vaststeller(s): (Naam; graad en functie)

Getuigen: (Naam; graad en functie)

Vastgesteld:

(kort feitelijk verslag: aanwijzingen die tot de vaststelling leiden)

Was een speekseltest mogelijk? JA/NEE

Indien NEE, vermeld hieronder de reden(en)

Reden(en):

→ Test DRÄGER DrugCheck® 3000

REF- en LOT-nummer :

Geldigheidsdatum:

→ Werden de voorschriften, gebruiksaanwijzing en hygiëne geëerbiedigd ? JA/NEE

→ Datum en uur van de speekseltest:

→ Plaats van de speekseltest:

Resultaat van de test: duidt hieronder de stoffen op waarvoor positief werd getest.

- *Amfetamine (AMP)*
- *Cocaïne (COC)*
- *MDMA (MET)*
- *Opiaten (OPI)*
- *Tetrahydrocannabinol (THC)*

Bij het voorlichtingsrapport wordt de speekseltest en foto van het resultaat van de speekseltest toegevoegd. Deze wordt gedag-, genaamtekend en geparafeerd door het betrokken personeelslid en de vaststeller. De getuige ondertekent desgevallend de test mee.

Naamtekening vaststeller,

naamtekening betrokken personeelslid,
voor kennisname,

Indien het betrokken personeelslid weigert te ondertekenen, of hiertoe niet in staat is, geef hieronder de reden daarvoor:

3. Te nemen maatregelen (duid aan welke maatregelen werden genomen)

Geen van de stoffen werd gedetecteerd

→Drempelwaarde(n) is (zijn) niet overschreden

Te nemen maatregelen:

- ☐ Indien nog geen alcoholtest werd afgenomen, neem een alcoholtest af
- ☐ Indien een alcoholtest werd afgenomen, ga naar 4

Eén of meerdere stoffen werden gedetecteerd

Drempelwaarde(n) is (zijn) overschreden

Te nemen maatregelen:

- ☐ Betrokken personeelslid wordt van het werk verwijderd tot het einde van de dienst.
- ☐ Betrokken personeelslid heeft recht op een telefoontje om te voorzien in vervoer. Alle kosten van vervoer vallen ten laste van het betrokken personeelslid.

Test werd geweigerd of test werd niet reglementair afgelegd

→gelijkgesteld met een test die een positief test.

→Drempelwaarde(n) is (zijn) overschreden

→Te nemen maatregelen:

- ☐ Betrokken personeelslid wordt van het werk verwijderd tot het einde van de dienst.
- ☐ Betrokken personeelslid heeft recht op een telefoontje om te voorzien in vervoer. Alle kosten van vervoer vallen ten laste van het betrokken personeelslid.

4. Beoordeling van de vastgestelde uiterlijke kenmerken op vlak van veiligheid.

→ **Hiërarchisch** meerdere besluit, op basis van de vastgestelde uiterlijke kenmerken, dat:

- ☐ de veiligheid van betrokken personeelslid, die van zijn collega's of van andere personen niet in het gedrang komt. Het personeelslid kan het werk onmiddellijk hervatten.
- ☐ de veiligheid van betrokken personeelslid, die van zijn collega's of van andere personen in het gedrang komt en neemt volgende veiligheidsmaatregelen:
- 0
- 0
- 0

Opgemaakt te.....op.....

Vaststeller(s): Personeelslid :

Handtekening: _____ Handtekening _____

(kopie van deze schriftelijke vaststelling wordt aan de medewerker gegeven.)



Hulpverleningszone Taxandria

Bijlage 12 : Uurroosters

De gemiddelde wekelijkse arbeidsduur van alle personeelsleden in voltijds dienstverband wordt vastgelegd op 38 uren. De waarde van een gemiddelde werkdag bedraagt 7,6 uren. Een week loopt van maandag tot en met zondag.

Bij een tijdelijke vermindering van de gemiddelde werkweek, zoals bijvoorbeeld bij loopbaanonderbreking voor ouderschapsverlof, wordt de inactiviteitsdag in onderling overleg met de werknemer en het afdelingshoofd en rekening houdend met de dienstorganisatie vastgelegd in een individuele overeenkomst.

Uurroosters kunnen tijdelijk en uitzonderlijk volgens de noodwendigheid van de dienst gewijzigd worden door de zonecommandant of zijn afgevaardigde of op vraag van het personeelslid binnen de wettelijke bepalingen.

Operationeel personeel vrijwilligerskader wordt ingezet op basis van noodwendigheid en beschikbaarheidssysteem met uitzondering van de hieronder opgenomen specifieke inzet.

1. Vast 12-uurrooster voor het operationeel beroepspersoneel post Dispatch in ploegendienst.

De operationele beroeps brandweerlieden werken van (D) 7u tot 19u en (N) 19u tot 7u volgens een 8-weken rotatiesysteem. D = Dag, N = Nacht en * = Dienst in post Turnhout, post Hoogstraten of dispatching.

De gemiddelde wekelijkse arbeidsduur van de personeelsleden post Dispatch bedraagt 38 uren.

	ma	di	woe	do	vrij	zat	zon
1		D 12	D 12			N 12	N 12
2			D 12	D 12	N 12		
3	D 12	D 12		*D 12	D 12		
4	D 12	N 12			D 12		
5		D 12	N 12			D 12	D 12
6			D 12	N 12			
7	D 12			D 12	D12		
8	N 12			D 12			

2. Vast 12-uurrooster voor het operationeel beroepspersoneel post Hoogstraten in ploegendienst.

De operationele beroepsbrandweerlieden werken van 7u tot 19u volgens een 18-weken rotatiesysteem.

De gemiddelde wekelijkse arbeidsduur van de personeelsleden post Hoogstraten bedraagt 38 uren.

Voor de overige uren worden ambulanciers-vrijwilligers ingeroosterd met een flex-systeem.

	ma	di	woe	do	vrij	zat	zon
1	12	12		12	12	vrij	vrij
2	12		12	12		vrij	vrij
3	12	12		12		vrij	vrij
4		12	12		12	vrij	vrij
5	12		12		12	vrij	vrij
6	12		12	12		vrij	vrij
7	12	12		12	12	vrij	vrij
8		12	12		12	vrij	vrij
9	12		12	12		vrij	vrij
10		12	12		12	vrij	vrij
11	12		12	12		vrij	vrij
12		12	12		12	vrij	vrij
13	12	12		12	12	vrij	vrij
14	12		12		12	vrij	vrij
15		12		12	12	vrij	vrij
16	12	12		12		vrij	vrij
17	12		12	12		vrij	vrij
18		12	12		12	vrij	vrij

3. Vast 12-uurrooster voor het operationeel beroepspersoneel post Turnhout in ploegendienst.

De gemiddelde wekelijkse arbeidsduur van de personeelsleden post Turnhout bedraagt 38 uren.

Dagrooster - 12-uren systeem TU dienst a

(min. 10 pers. op dienst ma-za en min. 8 pers. op dienst zon- en feestdagen)

	ma	di	woe	do	vrij	zat	zon
	12	12			12		
		12	12			12	12
			12	12			12
	12			12	12		

Dagrooster - 12-uren systeem TU dienst b

(min. 10 pers. op dienst ma-za en min. 8 pers. op dienst zon- en feestdagen)

	ma	di	woe	do	vrij	zat	zon
			12	12			12
	12			12	12		
	12	12			12		
		12	12			12	12

Nachtrooster - 12-uren systeem TU dienst a

(2 personen op dienst)

	ma	di	woe	do	vrij	zat	zon
	12	12					
		12	12				12
			12	12			12
	12			12			

Nachtrooster - 12-uren systeem TU dienst b

(2 personen op dienst)

	ma	di	woe	do	vrij	zat	zon
			12	12			12
	12			12			
	12	12					
		12	12				12

4. Glijdende werktijd

Glijdende werkroosters zijn van toepassing op de administratieve personeelsleden, het operationeel beroepspersoneel middenkader niet in ploegendienst, het operationeel beroepspersoneel hoger kader en de operationele medewerkers in wedertewerkstelling.

De contractuele en statutaire niet operationele personeelsleden zijn onderworpen aan de bepalingen van de Arbeidstijdwet van 14 december 2000 tot vaststelling van sommige aspecten van de organisatie van de arbeidstijd in de openbare sector. Zoals bepaald door de Arbeidstijdwet van 14 december 2000 mogen deze personeelsleden niet meer dan 11 uur per dag werken.

Rooster glijdende werktijd - voltijds werkregime

ma	di	woe	do	vrij	zat	zon
7,6	7,6	7,6	7,6	7,6	vrij	vrij

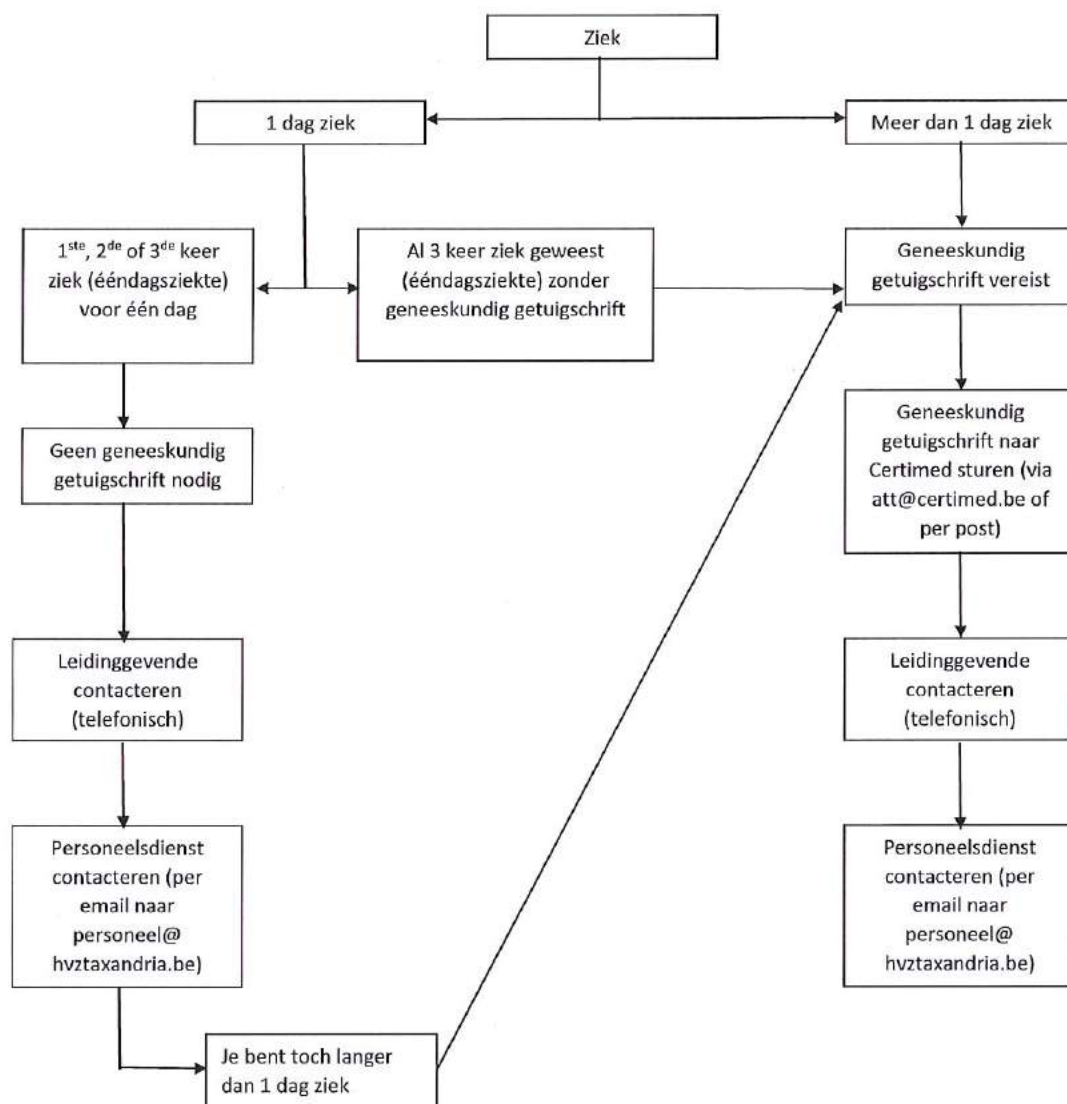
Het uurrooster van personeelsleden met een niet-voltijds werkregime wordt opgenomen in de individuele overeenkomst.



Melding afwezigheid wegens ziekte / privé-ongeval

Administratieve medewerkers

Wat te doen bij ziekte



Verwittiging bij afwezigheid

Elke afwezigheid wegens ziekte / ongeval (of verlenging ervan) meldt het personeelslid **onmiddellijk** aan zijn leidinggevende (telefonisch) en aan de personeelsdienst (per email via personeel@hvztaxandria.be). Deze melding dient de leidinggevende te bereiken uiterlijk vóór 10.00 uur.

Geneeskundig getuigschrift

Het KB van 19 april 2014 betreffende het administratief statuut van het operationeel personeel van de hulpverleningszones, voorziet een typedocument. Dit typedocument is het **verplicht** te gebruiken geneeskundig getuigschrift. Dit moet volledig worden ingevuld, inclusief diagnose. Het geneeskundig getuigschrift kan het ook downloaden: www.hvztaxandria.be.

Voor alle duidelijkheid: **enkel** dit typedocument geldt als geneeskundig getuigschrift. Het personeelslid vult deel 1 in met zijn persoonlijke gegevens, de behandelende geneesheer vult het 2^{de} deel in.

Het **volledig ingevulde** geneeskundig getuigschrift wordt **enkel** bezorgd aan CERTIMED:

1) per email onmiddellijk na doktersbezoek: att@certimed.be (24/24);

OF:

2) via de post via de voorgedrukte enveloppe (post betaald door bestemming)

3) via de post via enveloppe (met postzegel) naar:

CERTIMED vzw

t.a.v. de hoofdgeneesheer

DA 853-332-9

1070 Anderlecht

Let op: uiterlijk de **tweede** dag van de afwezigheid dient het geneeskundig getuigschrift verstuurd te zijn naar CERTIMED. De poststempel of datum van de email dient als bewijs.

Wat te doen bij ziek naar huis

Als je ziek naar huis gaat, breng je je directe leidinggevende op de hoogte. Je leidinggevende brengt de personeelsdienst op de hoogte per email aan personeel@hvztaxandria.be.

- Ziek naar huis = gewerkte dag (uren gelijk aan shifturen). Dit vermindert je saldo van de ziektedagen niet.
- De gewerkte uren worden geteld. De resterende uren worden aangevuld met 'ziek naar huis' totdat de volledige dag gevuld is.
- Je krijgt maaltijdcheque a rato de effectief gewerkte uren.

Wat te doen bij ééndagsziekte

Als je één dag ziek bent, maar niet naar de dokter gaat, breng je je directe leidinggevende op de hoogte. Dit kan **maar 3 keer per kalenderjaar**. Je leidinggevende brengt de personeelsdienst op de hoogte per email aan personeel@hvztaxandria.be.

- Ééndagsziekte = vermindert het saldo van je ziektedagen.
- Let op! Ééndagsziekte kan niet genomen worden na een dag ziek naar huis. Indien je na een dag ziek naar huis nog afwezig bent, moet je een doktersbriefje hebben. Ook kan je geen meerdere dagen na elkaar ééndagsziekte nemen.

Dienst Financiën

6	2023_ZR_00048	Eindrekening bijzondere rekenplichtige en waarnemend bijzondere rekenplichtige per 31/12/2022 - Goedkeuring GOEDGEKEURD
---	---------------	--

Beschrijving

Aanleiding en context

De eindrekening van vorige bijzondere rekenplichtige Hilde Van Nuffel en waarnemend bijzondere rekenplichtige Roger Caymax werd afgesloten op 31/12/2022.

Argumentatie

De eindrekening per 31 december 2022 wordt vastgesteld als volgt:

Begrotingsrekening:

Algemeen begrotingsresultaat van het dienstjaar	1.149.245,68
• Gewone dienst	1.107.590,43
• Buitengewone dienst	41.655,25
Boekhoudkundig resultaat van het dienstjaar	6.970.378,20
• Gewone dienst	1.252.008,90
• Buitengewone dienst	5.718.369,30
Over te dragen vastleggingen	5.821.132,52
• Gewone dienst	144.418,47
• Buitengewone dienst	5.676.714,05

Algemene boekhouding:

Balans per 31 december 2022 geeft het volgende overzicht:

	Activa		Passiva
Vlottende activa	7.598.875,15	Schulden	3.508.496,95
Vaste activa	8.535.638,74	Eigen vermogen	12.626.016,94
Totaal activa	16.134.513,89	Totaal passiva	16.134.513,89

De resultatenrekening bevat de volgende cijfers:

Exploitatieresultaat (nadelig)	- 1.726.221,21
Over te dragen uitzonderlijk resultaat (batig)	33.334,81

Totaal bedrag van de uitstaande vorderingen bedraagt 3.024.691,04 euro.

Totaal bedrag van de uitstaande schulden bedraagt 685.931,69 euro

Financiële rekeningen

De financiële rekeningen worden op 31 december 2022 als volgt vastgesteld:

ING Zichtrekening	4.202.035,07
Belfius Zichtrekening	371.124,82
BPOST Zichtrekening	1.358,72
Totaal volgens rekeninguittreksels	4.574.518,61

Toestand van de financiële rekeningen volgens de boekhouding :

Totaal van de klasse 5	4.574.518,61
Interne overboekingen (AR 56000)	0,00
Betalingen in uitvoering (AR 58001)	0,00
Totaal financiële rekeningen	4.574.518,61
Te verantwoorden verschil	0,00

Er is volledige overeenstemming tussen de algemene en de budgettaire boekhouding.

Er is volledige overeenstemming tussen de boekingen en de kasmiddelen.

Juridische grond

Wet van 15 mei 2007 betreffende de civiele veiligheid (B.S. 31.07.2007) en (erratum 01.10.2007).

Het Koninklijk besluit van 19 april 2017 (B.S. 12.12.2017 – Ed.2) houdende het algemeen reglement op de boekhouding van de hulpverleningszones.

Besluit

Artikel 1

De eindrekening van vorige bijzondere rekenplichtige Hilde Van Nuffel en waarnemend bijzondere rekenplichtige Roger Caymax tot en met 31/12/2022 wordt goedgekeurd.

Artikel 2

De raad verleent kwijting aan Hilde Van Nuffel en Roger Caymax als bijzondere rekenplichtige voor de boekhouding van de Hulpverleningszone Taxandria tot en met 31/12/2022.

7	2023_ZR_00049	Rekening 2022 - Vaststelling GOEDGEKEURD
---	---------------	---

Beschrijving

Aanleiding en context

De zoneraad stelt in de loop van het eerste kwartaal van ieder jaar de rekening van het voorgaande jaar vast. Deze rekening omvat de begrotingsrekening, de resultatenrekening, de balans en een verslag (art. 88 wet civiele veiligheid van 15 mei 2007).

Argumentatie

De rekening 2022 vertoont de volgende resultaten:

Begrotingsrekening:

Algemeen begrotingsresultaat van het dienstjaar	1.149.245,68
• Gewone dienst	1.107.590,43
• Buitengewone dienst	41.655,25
Boekhoudkundig resultaat van het dienstjaar	6.970.378,20
• Gewone dienst	1.252.008,90
• Buitengewone dienst	5.718.369,30
Over te dragen vastleggingen	5.821.132,52
• Gewone dienst	144.418,47
• Buitengewone dienst	5.676.714,05

Algemene boekhouding:

Balans per 31 december 2022 geeft het volgende overzicht:

	Activa		Passiva
Vlottende activa	7.598.875,15	Schulden	3.508.496,95
Vaste activa	8.535.638,74	Eigen vermogen	12.626.016,94
Totaal activa	16.134.513,89	Totaal passiva	16.134.513,89

De resultatenrekening bevat de volgende cijfers:

Exploitatieresultaat (nadelig)	- 1.726.221,21
Over te dragen uitzonderlijk resultaat (batig)	33.334,81

Juridische grond

Wet van 15 mei 2007 betreffende de civiele veiligheid (B.S. 31.07.2007) en (erratum 01.10.2007).
Het Koninklijk besluit van 19 april 2017 (B.S. 12.12.2017 – Ed.2) houdende het algemeen reglement op de boekhouding van de hulpverleningszones.

Besluit

Artikel 1

De zoneraad stelt de rekening 2022 vast.

Artikel 2

De rekening 2022 vertoont de volgende resultaten:

Begrotingsrekening:

Algemeen begrotingsresultaat van het dienstjaar	1.149.245,68
---	--------------

• Gewone dienst	1.107.590,43
• Buitengewone dienst	41.655,25
Boekhoudkundig resultaat van het dienstjaar	6.970.378,20
• Gewone dienst	1.252.008,90
• Buitengewone dienst	5.718.369,30
Over te dragen vastleggingen	5.821.132,52
• Gewone dienst	144.418,47
• Buitengewone dienst	5.676.714,05

Algemene boekhouding:

Balans per 31 december 2022 geeft het volgende overzicht:

	Activa		Passiva
Vlottende activa	7.598.875,15	Schulden	3.508.496,95
Vaste activa	8.535.638,74	Eigen vermogen	12.626.016,94
Totaal activa	16.134.513,89	Totaal passiva	16.134.513,89

De resultatenrekening bevat de volgende cijfers:

Exploitatieresultaat (nadelig)	- 1.726.221,21
Over te dragen uitzonderlijk resultaat (batig)	33.334,81

8	2023_ZR_00050	Nieuwe huurovereenkomst oefenhal Weelde - Goedkeuring GOEDGEKEURD
----------	----------------------	--

Beschrijving

Aanleiding en context

Het gebruik van een oefenhal op Weelde Depot met een oppervlakte van 5000m² is een meerwaarde voor het opleiden en trainen van zowel het operationeel personeel als de rekruten in eigen streek. Niet als vervanging van de provinciale school, Campus Vesta maar zeker als aanvullende opleiding/oefen locatie.

In het zonecollege van 02/12/2020 werd het gebruik van hal 13 op Weelde Depot voor het geven van aanvullende opleidingen en als oefenhal goedgekeurd.

Argumentatie

De gemeente Ravels bezorgde een nieuwe huurovereenkomst voor hal 13 op Weelde Depot. De huurovereenkomst gaat in vanaf 1 februari 2023.

De zaken die veranderd zijn ten opzichte van het vorige contract zijn de volgende:

- Artikel 4 - De huurprijs: deze bedraagt voortaan 2750 EUR (ex. btw) per maand.

- Artikel 3 - De duur van het contract: deze is vanaf nu 3 jaar, welke telkens in samenspraak verlengbaar is. Daarnaast kan het contract door beide partijen worden opgezegd ten minsten 6 maanden vooraf (in plaats van de 3 in het vorige).
- Artikel 13 - Veranderingen aan het gehuurde goed: de volgende zin werd toegevoegd: ' De verhuurder behoudt zich het recht voor op gedurende de huurperiode op de loods zonnepanelen aan te leggen'

Financiële informatie

Visum: Visum verleend

Motivering

ok

Financiële informatie

MJP000243 -- Huur en huurlasten oefenhal Weelde -- Initieel budget: € 40.000,00 -- Beschikbaar: € 30.633,82 -- Huur Oefenhal Depot Weelde /H/2023/35119/126-01/71. De huur wordt betaald aan het begin van elk kwartaal. Voor het eerste kwartaal werd reeds 7.890,18 euro betaald (op basis van het vorige contract)

Totale huurprijs voor 2023: 33.000 euro

Besluit

Artikel 1

De zoneraad keurt de nieuwe huurovereenkomst voor hal 13 op Weelde Depot goed.

Artikel 2

De zoneraad vraagt de gemeente Ravels om werk te maken van het oplossen van de mankementen die werden doorgegeven.

9	2023_ZR_00051	Omzendbrief Federale dotaties 2023 voor de brandweer, definitieve bedragen - Kennisneming KENNIS GENOMEN
---	---------------	---

Beschrijving

Aanleiding en context

Het is belangrijk dat de hulpverleningszones over adequate middelen beschikken om hun wettelijke opdrachten te vervullen om zo de veiligheid en de bescherming van de bevolking te verzekeren. Met de omzendbrief van 3 januari 2023 gaf Minister van Binnenlandse Zaken meer toelichting bij de verdeling van de extra 18 miljoen euro federale dotatie voor de hulpverleningszones voor 2023.

Argumentatie

Met de omzendbrief van 21 februari 2023 geeft Minister van Binnenlandse Zaken meer toelichting bij de jaarlijkse structurele verhoging van de federale dotaties voor de hulpverleningszones.

In 2021 en 2022 werden de federale dotaties met respectievelijk 25 miljoen euro en meer dan 8 miljoen euro verhoogd. Deze verhogingen zijn nu structureel opgenomen in de federale dotaties aan de hulpverleningszones.

Voor 2023 wordt opnieuw een structurele verhoging voorzien. Vooropgesteld was 2 miljoen euro. Door een lineaire besparing voor de jaren 2022 tot 2024 toe te passen op alle federale kredieten zal de uiteindelijke verhoging van de federale dotaties aan de hulpverleningszones 300.000 euro bedragen. Voor de hulpverleningszone Taxandria betekent dit een verhoging van 4.520 euro.

	Initieel bedrag	Na indexatie omzendbrief /01/2023	Verhoging	Na indexatie omzendbrief 21/02/2023	Totale verhoging 2023
Basisdotatie 2023	705.971,70	776.185,20	+70.213,50	776.185,20	+70.213,50
Bijkomende dotatie 2023	2.571.114,76	2.820.609,13	+249.494,37	2.825.129,81	+254.015,05
Totale federale dotatie 2023	3.277.086,46	3.596.794,33	+319.707,87	3.601.315,01	+324.228,55

De omzendbrief met de toelichting en de bedragen is terug te vinden als bijlage. Dit zijn de definitieve bedragen.

Regelgeving: bevoegdheid

Wet van 15 mei 2007 betreffende de civiele veiligheid

Besluit

Artikel 1

De zoneraad neemt kennis van de omzendbrief van de Minister van Binnenlandse Zaken waarin zij toelichting geeft bij de structurele verhoging van de federale dotaties voor de hulpverleningszones.

Artikel 2

De zoneraad neemt kennis van de definitieve bedragen voor 2023 voor de hulpverleningszone Taxandria.

10	2023_ZR_00052	Vastlegging voor opleidingen op Campus Vesta - Goedkeuring GOEDGEKEURD
----	---------------	--

Beschrijving

Aanleiding en context

Het VTO Jaaractieplan bevat een zonaal programma waarin o.a. voortgezette opleidingen zijn vastgelegd.

Argumentatie

Voor het basiskader worden in 2023 voorzien:

- AT3311 Redden van dieren (6 uur)
- AT3411 Hybride en elektrische voertuigen (6 uur)
- + 2 opleidingen uit keuze programma
- AT2211 Industriële brandbestrijding (6 uur)
- AT1311 Tcell (6 uur)
- AT 1311 Hoogbouw (6 uur)
- AT7511 Scenario IGS (6 uur)

- AT5611 Scenario THV (6 uur)
- + 2 jaarlijks PPMO (2 uur)

Bovenstaande resulteert in 24 uur opleiding en 26 uur opleiding voor de mensen die PPMO moeten volgen.

Voor het middenkader worden in 2023 voorzien:

- 2 X EVO-0014 VMD (12 uur)
- AT3311 Redden van dieren (6 uur)
- AT3411 Hybride en elektrische vtg (6 uur) + een opleiding uit keuze programma
- AT2211 Industriële brandbestrijding (6 uur)
- AT7511 Scenario IGS (6 uur)
- AT5611 Scenario THV (6 uur)
- + 2 jaarlijks PPMO (2 uur)

Bovenstaande resulteert in 30 uur opleiding en 32 uur opleiding voor de mensen die PPMO moeten volgen.

Om al deze voortgezette opleidingen uit het zonaal programma te kunnen laten doorgaan worden er dit jaar in totaal zo'n 200 opleidingen ingericht. Een exacte hoeveelheid opleidingen, en dus ook kosten, kan op voorhand niet bepaald worden want is afhankelijk van het aantal deelnemers in de geplande sessies.

In plaats van voor elke opleiding een aparte bestelbon op te maken is het een administratieve vereenvoudiging om voor deze opleidingen een vastlegging voor Campus Vesta te doen van 140.000 euro van het VTO budget 351/123/17.

Regelgeving: bevoegdheid

Wet van 15 mei 2007 betreffende de civiele veiligheid

Financiële informatie

Visum: Visum verleend

Motivering

ok

Financiële informatie

Het totale budget op deze code bedraagt voor 2023 een bedrag van 385.000 euro. Op 15 maart is nog 324.300 euro beschikbaar.

Besluit

Artikel 1

De zoneraad gaat akkoord om voor de opleidingen opgesomd in de argumentatie van dit bundel een vastlegging voor Campus Vesta te doen van 140.000 euro van het VTO budget 351/123/17 in het kader van administratieve vereenvoudiging.

29 maart 2023 10:26 - De voorzitter opent de besloten zitting

29 maart 2023 10:40 - De voorzitter sluit de zitting

secretaris
Pascale Van Bael



Voorzitter
Frank Wilrycx

