

**Bijlage bij het arbeidsreglement
van gemeente en OCMW Waasmunster**

ICT-policy

Inhoudsopgave

1.	Inleiding	4
	Waarom deze ICT-code?	4
	Voor wie is de ICT-code bestemd?	4
	Wat zijn ICT-middelen?	4
2.	Hoe omgaan met ICT-middelen?	5
	Zorgvuldig gebruik van ICT-middelen	5
	Verboden gebruik	5
	Voorbeeldrol leidinggevende	6
3.	Veiligheid	6
	Cybercriminaliteit	6
	Cyberaanvallen en de gevolgen ervan	6
	Hoe cyberaanvallen voorkomen?	7
	Melden wanneer het toch misgaat	8
	Zorgvuldig omspringen met wachtwoorden en toegangscode	8
	Beheer van ICT-middelen	8
	Openbaarheid van bestuur versus vertrouwelijke informatie	8
	Beheer en opslag van informatie	9
	Cloudbestuur	10
	Beheer van hard- en software	10
	Telewerken	10
	Incidenten melden	11
4.	Communicatie	11
	Behoorlijk e-mailgebruik	11
	Gebruik en beheer van e-mail	11
	Privégebruik van e-mail	12
	Behoorlijk internetgebruik	12
	Sociale media	13
	Intellectuele eigendomsrechten	13
5.	Controlemiddelen	13
	Preventie	13
	Recht om te controleren	14
	Wat kan worden gecontroleerd?	14
	Doel van de controle	14
	Hoe kan worden gecontroleerd?	15
	Een permanente algemene controle	15
	Een occasionele algemene controle	15
	Een individuele controle	16

	Toegang tot e-mail en/of bestanden bij afwezigheid.....	17
6.	Maatregelen bij ongeoorloofd gebruik	18
7.	Maatregelen bij uitdiensttreding	19
8.	Functionaris voor gegevensbescherming.....	20

1. Inleiding

Waarom deze ICT-code?

De goede werking van de organisatie is sterk afhankelijk van de vlotte en doeltreffende werking van de Informatie en Communicatie Technologie (ICT) en de manier waarop de gebruikers ermee omgaan. Daarom worden naast de algemene afspraken die in het arbeidsreglement en de deontologische code zijn opgenomen, ook afspraken gemaakt over hoe de gebruikers dienen om te gaan met ICT.

Deze code is ontstaan naar aanleiding van volgende behoeften:

- Een **zorgvuldig en duurzaam gebruik van ICT-middelen**: het gebruik van ICT-middelen moet worden beperkt tot de toegelaten doeleinden, en dat op een zorgvuldige en vooruitziende wijze. Daarnaast is ook een duurzaam beheer van deze middelen belangrijk. Bij het omgaan met ICT-middelen speelt de leidinggevende een belangrijke voorbeeldrol (zie hoofdstuk 2).
- Het belang van het adequaat **beveiligen en beschermen** van ICT-middelen. Daarbij is het nodig om afspraken te maken over o.a. de omgang met wachtwoorden, cloudgebruik, telewerk en het beheer van informatie/hard- en software. De beveiliging van ICT-middelen tegen cybercriminaliteit is ook een belangrijk aandachtspunt (zie hoofdstuk 3).
- De behoefte aan afspraken rond een **veilig gebruik van communicatiemedia** zoals internet en e-mail. Daarnaast bestaat er een behoefte aan een etquette **om respectvol en correct te communiceren**. Ook een correct gebruik van sociale media hoort daarbij (zie hoofdstuk 4).
- **Preventie van misbruik en controle op gebruik van ICT-middelen**: de maatregelen op dat vlak vloeien voort uit de toepassing van telecom- en privacywetgeving en de beslissingen en aanbevelingen van de Gegevensbeschermingsautoriteit. Dit omvat enerzijds de controlemaatregelen die de organisatie kan toepassen ten aanzien van het onregelmatig gebruik van ICT-middelen (zie hoofdstuk **Fout! Verwijzingsbron niet gevonden.** en 5), en anderzijds de afspraken en maatregelen om de continuïteit van de dienstverlening te verzekeren (zie hoofdstuk 5.6 en 7).

Voor wie is de ICT-code bestemd?

De ICT-code geldt voor alle personeelsleden, mandatarissen en externen die toegang hebben tot de ICT-middelen van de organisatie (in deze ICT-code 'gebruikers' genoemd).

Met externen wordt eenieder bedoeld die geen personeelslid is van de organisatie (of in die hoedanigheid werkt). Te denken valt aan bv. stagiairs, jobstudenten, vrijwilligers, ingehuurde (project)medewerkers voor zover e.e.a. niet gedekt wordt door contractuele bepalingen.

Wat zijn ICT-middelen?

De organisatie biedt haar gebruikers een aantal ICT-middelen voor de uitoefening van hun taken.

De ICT-middelen kunnen opgesplitst worden in:

- ICT-systemen (hardware en software);
- Informatie op ICT-systemen.

Hardware en software zijn bijvoorbeeld:

- e-mail, internet- en intranetfaciliteiten;

- programmatuur en applicaties;
- netwerkinfrastructuur;
- computers, laptops, tablets;
- printers, multifunctionals;
- USB-sticks en externe harde schijven;
- telefoons, gsm's, smartphones;
- opslagmedia (bijvoorbeeld op een server), cloudinfrastructuur, ...

De informatie op de ICT-systemen behoort ook tot de ICT-middelen. De afspraken over het beheer van die informatie vind je in het hoofdstuk over Veiligheid (zie hoofdstuk 3).

De ICT-middelen die ter beschikking zijn gesteld, blijven eigendom van de organisatie.

2. Hoe omgaan met ICT-middelen?

Zorgvuldig gebruik van ICT-middelen

De gebruiker hanteert de ICT-middelen als een **voorzigtig en zorgvuldig** persoon.

- '**Voorzigtig**' betekent dat je de nadelige gevolgen van je handelen redelijk probeert in te schatten, dat je er met andere woorden op probeert te anticiperen.
- '**Zorgvuldig**' houdt in dat je die nadelige gevolgen probeert te voorkomen door gepaste voorzorgsmaatregelen te nemen.

Gebruikers moeten handelen op een manier die de integriteit en veiligheid van de ICT-middelen verzekert. De gebruiker neemt de nodige **veiligheidsmaatregelen** om **schade** aan de ICT-middelen te **voorkomen**, zowel binnen de organisatie als daarbuiten. Deze maatregelen worden beschreven in deze ICT-policy.

Daarnaast ben je bereid **verantwoordelijkheid** af te leggen over het gebruik van ICT-middelen. Deze middelen dienen om het algemeen belang na te streven, dus je gebruikt de middelen met het oog op zuinigheid, efficiëntie en effectiviteit.

Concreet betekent 'zorgvuldig gebruik van ICT-middelen' dat je de ICT-middelen gebruikt in overeenstemming met de doelstellingen waarvoor ze verstrekt zijn, op een kostenbewuste wijze en in overeenstemming met alle afspraken die in deze ICT-code worden vastgelegd.

Verboden gebruik

Het is gebruikers verboden om de ICT-middelen te gebruiken voor de volgende (niet limitatief opgesomde) doeleinden:

- Elk gebruik dat wettelijk verboden is, zoals:
 - Het binnenbreken in enig netwerk of systeem (bv. hacking). De gebruiker mag op geen enkele wijze de normale werking van netwerken of systemen verstoren, zowel intern als extern. Dit verbod omvat ook het af luisteren van netwerkverkeer.
 - Het gebruik van de ICT-middelen voor oplichting of fraude (bv. phishing of identiteitsfraude).
 - Het gebruik van de ICT-middelen dat zich tegen de grondbeginselen van de democratie en de rechtsstaat keert (bv. het bezoeken van websites voor doeleinden van racisme, terrorisme, ...).
 - Het inbreuk maken op de bescherming van de persoonlijke levenssfeer van natuurlijke personen (privacybescherming).

- Het inbreuk maken op de intellectuele eigendomsrechten (bv. auteursrechten op foto's en teksten).
- Elk gebruik dat obscene of in strijd met de openbare orde of goede zeden is (bv. het bezoeken van websites met pornografische of anderszins schokkende beelden).
- Elk gebruik dat kwetsend of beledigend is (bv. discriminerend, xenofob of seksistisch gedrag).
- Het gebruik met het oog op verslavingsgevoelige activiteiten, in het bijzonder gok- en kansspelen.
- Het gebruik voor commerciële doeleinden of privé-nevenwerkzaamheden.
- Elk gebruik dat het imago, de morele of economische belangen van de organisatie kan schaden.
- Het verspreiden van vertrouwelijke informatie naar derden die niet gerechtigd zijn om deze informatie te ontvangen of gebruiken.

Voorbeeldrol leidinggevende

Als leidinggevende heb je een **faciliterende rol en een voorbeeldrol** op het vlak van ICT-gebruik. Betrek bij de volgende punten ook de functionaris voor gegevensbescherming als adviseur indien nodig.

- Je denkt zorgvuldig na over de meest gepaste ICT-middelen en over de toegangspolitiek tot systemen die binnen je dienst of afdeling wordt gevoerd.
- Je zorgt ervoor dat de gebruikers binnen je dienst of afdeling de geschikte vorming volgen om de ICT-systemen op een passende manier te gebruiken.
- Je bespreekt mogelijke risico's van het gebruik van ICT met de gebruikers binnen je dienst of afdeling.
- Je hebt de verantwoordelijkheid om problemen rond ICT-gebruik aan te pakken of aan te kaarten.

3. Veiligheid

Dit hoofdstuk bespreekt enkele veel voorkomende risico's inzake informatieveiligheid waar jij als gebruiker mee geconfronteerd kan worden, en formuleert afspraken die nageleefd moeten worden om dergelijke risico's te minimaliseren.

Cybercriminaliteit

Cyberaanvallen en de gevolgen ervan

Internet- of cybercriminaliteit is een groeiend fenomeen en bestaat in vele vormen. Het motief van cybercriminelen is veelal financieel gewin. Daarvoor moeten ze eerst in de ICT-systemen van de organisatie geraken. Dat doen ze vooral door middel van de volgende tactieken:

- Wachtwoorden van gebruikers bemachtigen via phishing. Dit is een vorm van oplichting waarbij men hengelt naar persoonlijke informatie (zoals bv. creditcardnummer, wachtwoord en accountgegevens) om die te misbruiken. Je krijgt dan meestal een mail met een link naar een website waar je je login moet ingeven. Men doet bijvoorbeeld of er een belangrijk document voor je klaarstaat, of dat een bank- of ander account zal worden afgesloten tenzij je inlogt. Wanneer je je login ingeeft, gebruikt de aanvaller die om in je echte account in te loggen.
- Wachtwoorden van gebruikers bemachtigen via het raden van wachtwoorden. Te korte, evidente of eenvoudige wachtwoorden kunnen binnen enkele seconden geautomatiseerd geraden worden.
- Kwaadaardige software ('malware') op de ICT-systemen proberen activeren via gebruikers. In dit geval ontvang je bijvoorbeeld een mail met een bijlage die je moet

openen. De bijlage bevat software die de aanvaller in staat stelt de ICT-systemen van de organisatie binnen te dringen, of die zelfstandig schade aan de ICT-systemen en data veroorzaakt. De malware is veelal gecamoufleerd (bv. als een pdf of een zip-bestand). Wanneer je de bijlage opent wordt de malware actief.

- Zwakke plekken in de technische beveiliging proberen uitbuiten. Zwakke plekken in de beveiliging van ICT-systemen zijn een continu gegeven. Er worden regelmatig nieuwe zwakheden gevonden, waarna softwareleveranciers snel updates voorzien die het probleem verhelpen. De dienst ICT staat er voor in om deze updates steeds snel te installeren.

Van zodra de aanvaller erin geslaagd is de ICT-systemen binnen te dringen, kan de aanvaller de cyberaanval voortzetten. Verschillende scenario's zijn mogelijk, zoals:

- Ransomware: de bestanden van de organisatie worden door malware versleuteld en zijn dan onbruikbaar. De organisatie moet de aanvaller betalen om de bestanden te kunnen ontsleutelen.
- Diefstal van gegevens, gevolgd door afpersing: bij de inbraak in de systemen wordt data gestolen en de aanvaller dreigt deze op internet te plaatsen. De organisatie moet betalen om de data niet online te publiceren. Dit scenario gebeurt vaak in combinatie met ransomware.
- Inbraak in en misbruik van mailboxen: de aanvaller heeft een login van een medewerker bemachtigd (door phishing of via het raden van een te gemakkelijk wachtwoord) en gebruikt diens mailbox om phishingmails uit naam van de organisatie te verspreiden.

Steevast leiden cyberaanvallen tot veel tijdverlies voor de dienst ICT en alle andere diensten, omdat er moeilijker gewerkt kan worden en dienst ICT de systemen moet herstellen. Het herstel verloopt meestal stapsgewijs: het kan dagen tot weken duren voor alles terug in orde is. De minder zichtbare gevolgen kunnen zelfs maanden aanslepen. Meestal moeten er vanwege de omvang en complexiteit van de herstelwerken ook gespecialiseerde derden worden ingeschakeld, wat erg kostelijk is. Er ontstaan bovendien aanzienlijke risico's voor de bescherming van de (persoons)gegevens die op de ICT-systemen aanwezig zijn. Ook het imago en de reputatie van de organisatie kan worden aangetast wanneer een cyberaanval zich voordoet.

Hoe cyberaanvallen voorkomen?

Leef de volgende afspraken na om te voorkomen dat jij of de organisatie het slachtoffer wordt van internetcriminaliteit:

- De organisatie voorziet alle systemen van veiligheidsmaatregelen (bv. anti-malware software). Gebruikers moeten deze maatregelen te allen tijde intact laten. Het is strikt verboden de veiligheidsmaatregelen uit te schakelen of wijzigingen aan te brengen in de huidige instellingen. Indien de ICT-dienst merkt dat je deze maatregelen uitgeschakeld of gewijzigd hebt, kan men je de toegang tot het netwerk onmiddellijk ontzeggen om de integriteit van het netwerk te beschermen.
- Wees alert voor phishing en mails die malware verspreiden. Klik niet zomaar op links en open niet zomaar bijlages bij e-mails. Wees ook op je hoede voor valse SMS'en en telefoontjes. Verstrek niet zomaar persoonlijke-, bedrijfs- of andere informatie (ongeacht het kanaal waarlangs dit gevraagd wordt). Controleer altijd of de afzender, het bericht of de webpagina betrouwbaar zijn en ga bij twijfel niet op het verzoek in.
- Het is verboden om via e-mail binnenkomende (valse of echte) virusmeldingen naar alle gebruikers door te sturen. Als je vragen hebt over zo'n mail, raadpleeg dan de dienst ICT. Ook het versturen van kettingbrieven of spamberichten is verboden.
- Gebruikers mogen zelf geen software installeren (zie hoofdstuk 3).
- Hou je aan de binnen de organisatie geldende regels voor wachtwoorden en toegangscode's (zie hoofdstuk 3).

Melden wanneer het toch misgaat

Vermoed of constateer je dat je computer door malware is getroffen of dat je benaderd bent als onderdeel van een cyberaanval (bv. door middel van phishing), meld dit dan overeenkomstig de incidenten- en datalekkenprocedure binnen de organisatie. Elke gebruiker dient zich op de hoogte te stellen van deze procedure.

Zorgvuldig omspringen met wachtwoorden en toegangscode

Aan iedere individuele gebruiker wordt een persoonlijke gebruikersnaam en wachtwoord gegeven. Aan deze identificatiegegevens zijn je toegangsrechten in het netwerk en binnen de gebruikte software gekoppeld.

Juist daarom zijn wachtwoorden **persoonlijk** en **vertrouwelijk** en zijn gebruikers **individueel verantwoordelijk** voor alle handelingen die worden uitgevoerd met hun eigen gebruikersnaam en wachtwoord.

Om deze verantwoordelijkheid te waarborgen gelden voor het gebruik van wachtwoorden de volgende, strikt na te leven afspraken:

- Deel je wachtwoord nooit mee aan anderen (lijnmanagement, collega's, ...). **Een leidinggevende zal nooit vragen naar je wachtwoorden, en ook de ICT-dienst zal nooit om je wachtwoord vragen.** Vraag zelf nooit naar het wachtwoord van anderen. Wanneer om het even wie binnen of buiten de organisatie naar je wachtwoord vraagt, wijs je dat verzoek af met verwijzing naar deze ICT-code;
- Scherm het wachtwoord af van onrechtmatig gebruik: let op dat niemand meekijkt als je je wachtwoord intypt en schrijf het wachtwoord ook nergens op;
- Het is niet toegestaan om in te loggen met het account van je collega's. Voor het verzekeren van de continuïteit van de dienstverlening worden door de organisatie veilige oplossingen voorzien, zoals het werken met een beveiligd gemeenschappelijk opslagsysteem;
- Elke gebruiker is verantwoordelijk voor de veiligheid van de eigen wachtwoorden, en de leidinggevendenden hebben bovendien een voorbeeldrol;
- Elke gebruiker hanteert verschillende wachtwoorden voor professionele doeleinden enerzijds en privédoeleinden anderzijds. Voor de aanmaak van privé-accounts wordt het professioneel e-mailadres niet gebruikt.

Ben je je wachtwoord vergeten, neem dan contact op met de ICT-dienst om een nieuw wachtwoord in te stellen.

Wachtwoorden moeten voldoen aan bepaalde regels. Deze worden op niveau van het besturingssysteem afgedwongen via de systeeminstellingen.

Door de toegenomen cyberdreigingen wordt er naast de toegangsbeveiliging door middel van wachtwoorden ook ingezet op een extra beveiligingslaag, met name multifactorauthenticatie of MFA. Dat houdt concreet in dat je bovenop je wachtwoord over een extra element (factor) moet beschikken om toegang te krijgen tot het interne netwerk. Alle gebruikers zijn verplicht om het MFA-beleid van de organisatie toe te passen en na te leven. De bovenstaande afspraken voor wachtwoorden moeten naar analogie worden toegepast op deze bijkomende factor.

Beheer van ICT-middelen

Openbaarheid van bestuur versus vertrouwelijke informatie

De organisatie beschikt over een grote hoeveelheid aan informatie. Veel van die informatie stellen we ter beschikking van de burger in het kader van de openbaarheid van bestuur.

Daarnaast is een groot deel van de informatie **vertrouwelijk**, omdat de belangen van de betrokkenen worden geschaad bij openbaarmaking van de informatie:

- belangen van natuurlijke personen, bijvoorbeeld gegevens die onder het medische geheim vallen, tuchtdossiers, dossiers met persoonsgebonden informatie van burgers;
- belangen van de organisatie, bijvoorbeeld het geheim van beraadslagingen van politieke organen, informatie over een interne audit;
- belangen binnen gerechtelijke procedures, bijvoorbeeld informatie m.b.t. gerechtelijke procedures of strafrechtelijke feiten waarbij de organisatie betrokken partij is;
- zaken van maatschappelijk belang, bijvoorbeeld informatie die invloed kan hebben op de openbare orde en veiligheid of informatie die een economisch, financieel of commercieel belang kan schaden.

Je denkt na over het soort informatie waarover je beschikt en je verspreidt die informatie alleen als je er zeker van bent dat het niet over vertrouwelijke gegevens gaat. Bij twijfel neemt je steeds contact op met je leidinggevende.

Beheer en opslag van informatie

Voor een papieren document is het vaak gemakkelijk om zelf de vertrouwelijkheid te garanderen. Je kunt het document zelf op **een veilige plaats** wegbergen. Voor elektronische bestanden geldt er een **gedeelde verantwoordelijkheid** tussen de ICT-beheerders en jezelf.

- De beheerders zorgen ervoor dat onbevoegden geen toegang hebben tot de systemen, door het implementeren van technische maatregelen zoals firewalls, wachtwoordbeleid en toegangsbeheer.
- Je bent echter zelf verantwoordelijk voor de juiste en meest veilige opslag van je bestanden. Dat wil zeggen dat je:
 - werkgerelateerde bestanden opslaat in het gemeenschappelijk opslagsysteem (netwerkschijf). Zo kun je informatie delen met je collega's en is er geen verlies van informatie mogelijk, aangezien van alles een back-up wordt gemaakt. Bij vervanging van je computer zal geen rekening worden gehouden met eventueel aanwezige bestanden op de lokale harde schijf ervan;
 - geen werkgerelateerde software of informatie zonder toestemming overzet op private apparatuur;
 - fysiek transport van vertrouwelijke informatie beperkt tot situaties waarin dat strikt noodzakelijk is voor de uitvoering van je werk. Wees je in een dergelijke situatie steeds bewust van het risico op verlies of diefstal.
 - persoonlijke bestanden opslaat onder op je persoonlijke OneDrive;
 - bewust omspringt met de beschikbare opslagruimte: verwijder regelmatig overbodige bestanden, bewaar bestanden slechts op één plaats;
 - je computer vergrendelt telkens als je je computer alleen laat, of deze uitschakelt indien je voor langere tijd afwezig zult zijn. Je computer vergrendelen kan door middel van de volgende toetsencombinaties:



of



(ctrl-alt-delete → deze computer vergrendelen / lock computer, of de 'Windows-toets + L' combinatie);

- Iedereen speelt een belangrijke rol in het vermijden van ongeoorloofde toegang tot gevoelige informatie. Dit geldt zowel voor de toegangen tot de ICT-systemen en toepassingen als voor de fysieke toegang tot lokalen of documenten. Iedereen brengt daarom clean desk in de praktijk door:

- enkel documenten die dezelfde dag nodig zijn op de bureau te laten liggen. Bij een afspraak met een externe mogen in principe nooit persoonsgegevens van anderen zichtbaar zijn.
- de ruimte af te sluiten wanneer men deze (tijdelijk) verlaat. In het geval van een open landschapsbureau controleert men of er geen vertrouwelijke informatie aanwezig is die onbewaakt wordt achtergelaten en kan worden ingekeken door onbevoegden. De computer wordt vergrendeld (zie hoger voor toetsencombinatie).
- op het einde van de werkdag de ruimte op te ruimen en de deur en ramen te sluiten.

Cloudgebruik

Cloud computing is ICT-dienstverlening via het internet, bijvoorbeeld het aanbieden van (gratis) opslagruimte of programmatuur (bv. Microsoft 365, Dropbox, Google Docs, WeTransfer, maar ook platformen zoals LinkedIn, Facebook, ...).

Om in een cloudomgeving veilig en verantwoord te kunnen handelen, gelden de volgende afspraken:

- Gebruikers mogen geen werkgerelateerde informatie opslaan in andere cloudomgevingen dan deze waarvoor de organisatie een contract heeft afgesloten (bv. de Microsoft 365 omgeving, Onedrive). Het is niet toegelaten om op eigen initiatief andere cloudomgevingen te gebruiken (Dropbox, Google Drive, enzovoort).
- Zorg ervoor dat je het overzicht behoudt over welke informatie waar staat.
- Vermijd het breder delen van informatie dan strikt noodzakelijk is.

Beheer van hard- en software

Om veiligheidsredenen hebben de gebruikers **geen lokale beheerdersrechten** op hun toestellen. Het is niet toegelaten om door middel van technische handelingen alsnog te proberen beheerdersrechten te verwerven.

Alle hard- en software die nodig is om de taken naar behoren te kunnen uitvoeren wordt door de organisatie ter beschikking gesteld. De gebruiker mag zelf geen bijkomende hard- of software installeren. Ongeoorloofde installaties kunnen immers nadelige gevolgen hebben voor de organisatie en voor de individuele gebruiker.

Indien er alsnog bijkomende hard- of software nodig is voor het uitvoeren van een taak, richt de gebruiker hiervoor een aanvraag aan de dienst ICT. Deze handelt de aanvraag verder af.

Indien blijkt dat bepaalde hard- of software werd geïnstalleerd zonder voorafgaandelijke toelating van de dienst ICT, dan kan de ICT-dienst deze hard- of software terug verwijderen.

Het gebruik van privétoestellen is verboden in het interne netwerk. Privétoestellen mogen enkel op het publieke netwerk gebruikt worden. Dit netwerk is beschikbaar via Wi-Fi-toegang of indien gewenst bekabeld. Een bekabelde toegang moet vooraf aangevraagd worden bij de dienst ICT.

Telewerken

Door de toename van telewerk en van de mogelijkheden die ICT biedt, zijn de grenzen tussen privé en werk vaak minder duidelijk. Als je documenten en ICT-middelen meeneemt op verplaatsing (bv. naar huis), tref je zowel thuis als onderweg de nodige maatregelen om die documenten en ICT-middelen te beschermen tegen verlies, ongeoorloofde inzage of ongeoorloofde wijziging. Respecteer daarom de volgende algemene afspraken:

- Neem enkel de noodzakelijke documenten en ICT-middelen mee op verplaatsing.
- Laat de documenten en ICT-middelen niet onbeheerd achter.

- Vergrendel je werktoestellen wanneer je die niet gebruikt.
- Spring zorgvuldig om met je wachtwoorden en toegangscode (bv. bij het intypen op publieke plaatsen).
- Zorg ervoor dat je thuisnetwerk beveiligd is met een sterk wachtwoord.
- Maak geen verbinding met openbare Wi-Fi netwerken.
- Gebruik de door de organisatie voorziene beveiligde verbinding om veilig toegang te krijgen tot het organisatienetwerk (Avingu).
- Blijf waakzaam voor malware (virussen, spyware, ...) en internetcriminaliteit (phishing, social engineering, ...).
- Bewaar werkdocumenten steeds in het gemeenschappelijk opslagsysteem (netwerkschijf) van de organisatie, zodat deze meteen ook in de back-up worden meegenomen en hou geen lokale kopieën bij.
- Vermijd papieren versies van dossiers, tenzij strikt noodzakelijk.
- Berg papieren documenten op in een afgesloten lade of kast.
- Vernietig vertrouwelijke documenten op een correcte wijze indien de bewaring ervan niet langer vereist is.
- Gebruik beter geen privétoestellen voor werkgerelateerde zaken: je privétoestellen zijn (mogelijk) minder beschermd dan je werktoestellen. Gevoelige informatie hoort daarom niet thuis op privétoestellen.
- Het ambts- en/of beroepsgeheim en de discretieplicht gelden ook tegenover je huisgenoten.

Incidenten melden

Als organisatie gaan we niet alleen aan de slag met heel wat gegevens, we zijn ook verantwoordelijk voor de beveiliging ervan. Wanneer er zich incidenten voordoen op het vlak van informatieveiligheid, dan moeten we deze registreren en opvolgen. Elke gebruiker is verplicht om dergelijke incidenten of datalekken te melden bij de juiste perso(o)n(en). Bij wie je concreet moet melden en wat de juiste stappen zijn, kan je terugvinden in het goedgekeurde beleid rond incidenten en datalekken.

4. Communicatie

In deze rubriek vind je meer informatie over het gebruik van:

- e-mail;
- internet en intranet;
- sociale media;
- materiaal dat beschermd is door intellectuele eigendomsrechten.

Behoorlijk e-mailgebruik

E-mail is een **populair, effectief en efficiënt** communicatiemiddel binnen de organisatie, met onmiskenbare voor- en nadelen. Het volgen van onderstaande richtlijnen zorgt ervoor dat e-mail een goed hulpmiddel is en blijft voor het uitvoeren van je taken.

Gebruik en beheer van e-mail

Hieronder vind je een aantal afspraken voor een efficiënt en informatieveilig gebruik van e-mail:

- Beperk het gebruik van CC: stuur het bericht uitsluitend naar personen die echt op de hoogte moeten zijn of die expliciet om een kopie van het bericht hebben gevraagd.
- Zet geadresseerden die elkaars gegevens niet mogen of moeten kennen in BCC.

- Vermijd het gebruik van 'allen beantwoorden'. Vaak is het niet nodig dat alle geadresseerden bij de zaak worden betrokken. Stuur je antwoord of bedenkingen alleen terug naar hen voor wie dit direct relevant is.
- Houd er rekening mee dat een e-mail zich niet zo goed leent voor vertrouwelijke communicatie. Een kleine fout kan ervoor zorgen dat een bericht ongewenst bij de verkeerde personen terechtkomt. Bovendien worden e-mails (en de bijlagen) standaard onversleuteld verstuurd.
- Beperk de bijlagen bij e-mails, zowel wat het aantal als de grootte ervan betreft, en definieer steeds duidelijk hun inhoud. Maak maximaal gebruik van het gemeenschappelijk opslagsysteem, zodat je de link met de bestandslocatie kunt doorsturen in de plaats van bijlagen. Soms kan een te groot bestand door middel van een compressieprogramma aanzienlijk gecomprimeerd worden. Voor meer informatie daarover kan je bij de ICT-dienst terecht.
- Stuur geen verdachte mails (phishingmails, mails met verdachte bijlages, ...) door naar collega's. Indien je een dergelijke mail ontvangt, contacteer dan de ICT-servicedesk.
- Ruim regelmatig je mailbox op door oude of overbodige berichten te verwijderen. Die zorgen namelijk voor een onnodige belasting van de opslagruimte. Maak ook de map 'verwijderde items' regelmatig leeg.
- Stuur geen werkgerelateerde e-mails door (noch automatisch, noch manueel) naar een eigen externe mailbox (bijvoorbeeld Hotmail, Gmail, Telenet, ...). De veiligheid en vertrouwelijkheid van de berichten bij die aanbieders kan immers niet gegarandeerd worden.
- Binnen de organisatie geldt een standaard model van e-mailhandtekening met een juridische disclaimer. Deze mag niet gewijzigd worden en wordt verplicht aan elke mail toegevoegd die aan externen gericht is.
- Maak gebruik van afwezigheidsboodschappen wanneer je voor een langere periode afwezig zal zijn. Geef daarin aan vanaf wanneer e-mails niet meer en weer wel worden gelezen en bij wie de afzender in de tussentijd terecht kan (eventueel voor welke thema's) en vermeld de contactgegevens van die persoon of personen, of een generiek e-mailadres.

Privégebruik van e-mail

Gebruikers moeten een private e-mailaccount hanteren voor niet-werkgerelateerde e-mails om werkgerelateerde en privémail van elkaar te scheiden. Let hierbij op: je private e-mailaccount wordt niet door de systemen van de organisatie gescand – het gevaar bestaat dat je op die manier de systemen compromitteert. Het is niet toegestaan om voor de uitvoering van de werkopdrachten gebruik te maken van een private e-mailaccount. Alle officiële elektronische correspondentie dient te verlopen via het door de organisatie verstrekte e-mailadres.

Behoorlijk internetgebruik

De meeste gebruikers hebben toegang tot het internet. Dat biedt de mogelijkheid om veel nuttige informatie voor het werk op te zoeken.

De organisatie verwacht van haar gebruikers de discipline en verantwoordelijkheid om het internet correct en efficiënt als werkinstrument te gebruiken. Zorg voor een redelijk, professioneel en zinvol gebruik van het internet tijdens het werk.

Binnen de organisatie is **beperkt niet-werkgerelateerd gebruik** van het internet toegestaan onder bepaalde voorwaarden:

- voor zover het is toegestaan binnen de eigen dienst;
- als het de uitvoering van je taken en je productiviteit en die van je collega's niet in het gedrang brengt;

Het is echter niet toegestaan om het intranet of internet te gebruiken op een manier die valt onder een verboden gebruik (zie infra).

Als preventiemiddel kan de **toegang tot bepaalde internetsites geblokkeerd worden**.

Sociale media

Binnen de organisatie wordt een brede definitie van sociale media gehanteerd. Het gaat om interactieve internettoepassingen die een multimediale dialoog tussen gebruikers van het medium mogelijk maken. Cruciaal daarbij is dat de gebruiker niet alleen consumeert, maar ook gemakkelijk zelf inhoud aan het medium kan toevoegen. Het gaat dus om tweerichtingsverkeer.

Veel gebruikers binnen de organisatie zijn actief op sociale media en dat geeft heel veel mogelijkheden:

- je kunt er kennis mee delen;
- je kunt je professionele ideeën toetsen aan de realiteit;
- je kunt in contact komen met andere medewerkers, experts in je vakgebied, burgers, enzovoort.

Tegelijk brengt dat ook een paar **risico's** met zich mee, bijvoorbeeld ten aanzien van een adequate scheiding van werk en privé, of ten aanzien van je rol als ambtenaar wanneer je publiek uitspraken doet. Die risico's kunnen zowel voor jezelf als voor de organisatie gevolgen hebben. Dit betekent dat de voor- en nadelen van het gebruik van sociale media vooraf goed moeten worden afgewogen. Deze afweging moet ervoor zorgen dat je bewust start met zulk gebruik en dat je daarbij ook daadwerkelijk rekening houdt met de voor- en nadelen.

Het is belangrijk dat je ook op sociale media de richtlijnen van de deontologische code in acht neemt, verantwoordelijk en loyaal bent en duidelijk maakt of je in eigen naam spreekt of vanuit de organisatie. Gebruik sociale media tijdens de werkuren alleen voor werkgerelateerde doeleinden of binnen de grenzen van een beperkt niet-werkgerelateerd gebruik (zoals beschreven in deze ICT-code).

Intellectuele eigendomsrechten

Voor het gebruik van materiaal en informatie geldt het wettelijk kader inzake de intellectuele eigendomsrechten. Dat betekent onder meer dat je alleen teksten of afbeeldingen van derden mag verspreiden en gebruiken wanneer de rechthebbende(n) daarvoor toestemming hebben gegeven of daarvan op een andere manier wettig gebruik kan worden gemaakt.

Alle gebruikers hebben daarom de plicht om zich ervan te vergewissen dat het materiaal en de informatie waar ze gebruik van maken op een rechtsgeldige manier gebruikt kan worden.

5. Controlemiddelen

Preventie

De leidinggevenden treden eerst en vooral preventief op om:

- controles te *vermijden*;
- het opsporen van misbruiken te *vermijden*;
- bij eventuele controles de schending van het privéleven van de gebruiker zoveel mogelijk te beperken.

In het kader van deze doeleinden kan de organisatie preventieve maatregelen nemen, zoals het blokkeren van de toegang tot bepaalde internetsites of het werken met dienst e-mailadressen/dienstpostbussen. Daarnaast is het de verantwoordelijkheid van elke gebruiker om de noodzakelijke preventieve maatregelen te nemen die door deze ICT-code worden opgelegd.

Recht om te controleren

De organisatie heeft het recht om een controle uit te oefenen op het internet- en e-mailgebruik van de gebruikers. De privacy van de gebruikers zal hierbij zoveel als mogelijk gerespecteerd worden.

De controle zal getoetst worden aan:

- het finaliteitsbeginsel: een controle is alleen mogelijk voor het nastreven van gerechtvaardigde doelen;
- het transparantiebeginsel: er wordt open gecommuniceerd over de controles en de doelen en voorwaarden van de controles;
- het proportionaliteitsbeginsel: zowel het uitvoeren van een controle als het soort controle moeten in verhouding staan tot het doel van de controle.

Die drie beginselen hebben als doel het evenwicht te houden tussen:

- het recht van de organisatie op controle van werkmiddelen;
- het recht van de gebruiker op respect voor zijn privéleven.

Wat kan worden gecontroleerd?

De controles kunnen betreffen:

- Het gebruik van e-mail;
- Het gebruik van internet;
- Het gebruik van andere professionele elektronische communicatiemiddelen zoals Skype, MS Teams, ...;
- De informatie en bestanden die gebruikers publiceren op het intranet, extranet en internet;
- De informatie en bestanden die gebruikers raadplegen en opslaan op verschillende opslagmedia (alle geïdentificeerde mappen op computers, servers, document management systemen, enzovoort).

Doel van de controle

Controle is alleen mogelijk als een van de vier volgende doelen worden nagestreefd:

- (1) het voorkomen en vaststellen van ongeoorloofde feiten, lasterlijke feiten of feiten die strijdig zijn met de goede zeden of die de waardigheid van een andere persoon kunnen schaden. Daaronder vallen bijvoorbeeld:
 - Het binnenbreken in enig netwerk of systeem (bv. hacking).
 - Het gebruik van de ICT-middelen voor oplichting of fraude (bv. phishing of identiteitsfraude).
 - Het gebruik van de ICT-middelen dat zich tegen de grondbeginselen van de democratie en de rechtsstaat keert (bv. het bezoeken van websites voor doeleinden van racisme, terrorisme, ...).
 - Elk gebruik dat obscene of in strijd met de openbare orde of goede zeden is (bv. het bezoeken van websites met pornografische of anderszins schokkende beelden).

- Elk gebruik dat kwetsend of beledigend is (bv. discriminerend, xenofob of seksistisch gedrag).
 - Het inbreuk maken op de bescherming van de persoonlijke levenssfeer van natuurlijke personen (privacybescherming).
 - Het inbreuk maken op de intellectuele eigendomsrechten (bv. auteursrechten op foto's en teksten).
- (2) het beschermen van vertrouwelijke informatie. De algemene regel bij de organisatie is 'openbaarheid van bestuur'. Er zijn echter uitzonderingen op die regel, omdat bepaalde informatie niet geschikt is om algemeen gedeeld te worden. Een controle door de organisatie is mogelijk als de door de uitzonderingsgronden op de openbaarheid van bestuur beschermde belangen geschaad worden. De organisatie kan ook controle doen op de praktijken die in strijd zijn met die belangen;
- (3) het verzekeren van de veiligheid, de performantie of de goede technische werking van de ICT-systemen van de organisatie. Daarbij hoort de controle op de bijbehorende kosten en de fysieke bescherming van de ICT-omgevingen (installaties) van de organisatie;
- (4) het te goeder trouw naleven van deze ICT-code en andere richtlijnen voor het gebruik van onlinetechnologieën, zoals vermeld in het arbeidsreglement, de deontologische code, de arbeidsovereenkomst of enige andere reglementaire of contractuele bepaling;

De gegevens die verzameld en verwerkt worden voor een controle met een van de vier bovenstaande doelen, kunnen niet gebruikt worden voor een controle met andere doeleinden. Als een wettelijke bepaling dat toestaat of oplegt, kan de algemeen directeur de gegevens voor een ander doel gebruiken, inkijken en herleiden tot een bepaalde gebruiker.

Hoe kan worden gecontroleerd?

De manier waarop wordt gecontroleerd is afhankelijk van het doel van de controle. We onderscheiden daarin permanente en occasionele algemene controles, en individuele controles.

Een permanente algemene controle

Een **permanente algemene controle** is het automatisch monitoren of bewaren van elektronische online communicatiegegevens. Het gaat om niet-geïndividualiseerde gegevens (gegevens die niet gelinkt worden aan een persoon/gebruiker).

Sommige ICT-systemen kunnen worden gecontroleerd om hun veiligheid, performantie en goede technische werking te waarborgen. Daarbij hoort ook de controle op de bijbehorende kosten en de fysieke bescherming van de ICT-omgevingen (installaties) van de organisatie.

Een occasionele algemene controle

Een **occasionele algemene controle** is het verzamelen en de inzage van algemene elektronische online communicatiegegevens die tijdens een beperkte periode werden gegenereerd en betrekking hebben op een groep van gebruikers.

De algemeen directeur kan beslissen om voor de in hoofdstuk 5 genoemde doeleinden een occasionele algemene controle te doen. Bij een occasionele algemene controle worden de volgende zaken gecontroleerd:

- een lijst van de bezochte websites, de frequentie en het volume van de doorgezonden informatie, maar niet de identificatie van de betrokken gebruikers die de sites hebben bezocht;
- het aantal, het volume en het tijdstip van de uitgaande e-mails (niet de binnenkomende berichten), maar niet de identificatie van de betrokken gebruikers die ze hebben verstuurd.

Een occasionele algemene controle kan niet slaan op in het verleden ontstane gegevens en is beperkt tot de tijd die nodig is om eventuele misbruiken te voorkomen of vast te stellen.

Een individuele controle

Bij een **individuele controle** wordt gecontroleerd:

- wie welke websites heeft bezocht, wanneer en voor hoe lang;
- wie bepaalde e-mails heeft verzonden, de geadresseerden, het volume en de frequentie ervan. Het gaat hier dus om gegevens *over* de communicatie, niet over de *inhoud* van de communicatie. Bij controle mag de organisatie sowieso geen inzage nemen in de inhoud van niet-werkgerelateerde e-mails van de gebruiker, maar er mag wel gecontroleerd worden op eventueel ongeoorloofd niet-werkgerelateerd gebruik van het e-mailaccount. De tijdstippen, frequentie en geadresseerden van de e-mails zijn meestal voldoende om ongeoorloofd gebruik te kunnen vaststellen. Ter bescherming van zowel de organisatie als de gebruiker zal de controle van het e-mailgebruik dan ook gebeuren door de functionaris voor gegevensbescherming of interne vertrouwenspersoon, samen met de ICT-dienst ('vier-ogen principe'). Zij zullen de gegevens over het mailgebruik van het gebruiker die voor de controle relevant zijn, aan de organisatie beschikbaar stellen. Zij dragen er daarbij zorg voor dat er geen privé-inhouden van e-mails van het gebruiker doorgegeven worden.

Een individuele controle is toegestaan voor de volgende doelen en onder de volgende **voorwaarden**:

1. Uit een occasionele algemene controle blijkt dat een of meerdere gebruikers uit de gecontroleerde groep de ICT-middelen niet hebben gebruikt volgens de afspraken van deze ICT-code of andere richtlijnen voor het gebruik van online technologieën. De individuele controle kan in die situatie alleen gebeuren nadat de algemeen directeur (of zijn vertegenwoordiging):
 - de betrokken gebruikers op een duidelijke en begrijpelijke wijze heeft ingelicht over het bestaan van een onregelmatigheid;
 - de gebruikers op de hoogte heeft gebracht dat de elektronische online communicatiegegevens geïndividualiseerd zullen worden als opnieuw een dergelijke onregelmatigheid wordt vastgesteld

Dit is een *indirecte individualisering*.

2. In bepaalde andere gevallen moet de betrokken gebruiker *niet vooraf worden gewaarschuwd*, dit is een *directe individualisering*. Aanleidingen om over te gaan tot een directe individualisering kunnen zijn:
 - a. Uit een occasionele algemene controle blijkt dat een of meerdere gebruikers uit de gecontroleerde groep zich **schuldig maken** aan:
 - (1) ongeoorloofde feiten, lasterlijke feiten of feiten die strijdig zijn met de goede zeden of die de waardigheid van een andere persoon kunnen schaden;
 - (2) het openbaar maken van vertrouwelijke informatie: bepaalde informatie mag immers niet algemeen gedeeld worden, namelijk als de door de

uitzonderingsgronden op de openbaarheid van bestuur beschermde belangen geschaad worden;

(3) feiten die de veiligheid, de performantie of de goede technische werking van de ICT-systemen van de organisatie in het gedrang brengen of de kosten abnormaal hoog doen oplopen.

- b. Er is een **gegrond vermoeden** dat een gebruiker zich schuldig maakt aan de feiten, vermeld in het vorige punt. In dat geval kan het lijnmanagement het internetgebruik en e-mailverkeer van die gebruiker laten controleren. De algemeen directeur kan dat doen zonder zich te beroepen op gegevens die verzameld zijn in een eerder uitgevoerde occasionele algemene controle. Deze controle **is beperkt in de tijd** en kan **niet slaan op gegevens die in het verleden zijn ontstaan**.

Met 'gegrond vermoeden' wordt bedoeld dat er nog **andere feitelijke elementen** zijn die erop wijzen dat een bepaalde gebruiker zich schuldig zou maken aan de feiten vermeld in het vorige punt (bijvoorbeeld in het geval het lijnmanagement vermoedt dat een gebruiker bepaalde vertrouwelijke informatie heeft bezorgd aan een derde, kan dit vermoeden gebaseerd zijn op een gesprek met die derde of op daden van die derde waaruit blijkt dat deze over die vertrouwelijke informatie beschikt). De verantwoordingsplicht voor het gegrond vermoeden ligt bij de algemeen directeur en lijnmanagement.

- c. Er zijn **ernstige indicaties** van mogelijke **onregelmatigheden**. In dat geval kan **Audit Vlaanderen** een forensische audit (administratief onderzoek) instellen naar de aangelegenheid in kwestie. De bevoegdheid van Audit Vlaanderen op dat vlak is expliciet opgenomen in artikel 222 Decreet Lokaal Bestuur. Artikel 223 Decreet Lokaal Bestuur bepaalt ook dat Audit Vlaanderen voor het uitvoeren van zijn bevoegdheden toegang heeft tot alle informatie. Audit Vlaanderen is derhalve in het kader van de uitvoering van zijn forensische audits ook bevoegd om **alle werkgerelateerd e-mailverkeer, werkgerelateerde bestanden en elektronische communicatiegegevens te onderzoeken**. Die onderzoeksmogelijkheid wordt niet beperkt door het moment waarop de e-mails, bestanden of gegevens zijn ontstaan. Audit Vlaanderen kan dergelijke gegevens eveneens gebruiken in het kader van een detectieaudit, op voorwaarde dat wordt gewaakt over de vertrouwelijkheid van de onderzochte gegevens in de rapportering.
- d. De wet van 4 augustus 1996 betreffende het welzijn van de werknemers bij de uitvoering van hun werk, verplicht de organisatie tot een onderzoek bij feiten van geweld, pesterijen en ongewenst seksueel gedrag. De algemeen directeur is daarbij bevoegd om de verzamelde elektronische online communicatiegegevens te individualiseren. Het gaat daarbij zowel om de gegevens die werden verzameld bij een occasionele controle als de gegevens die werden verzameld bij de permanente controle. Met dat doel kunnen ook gegevens die in het verleden zijn ontstaan, worden geraadpleegd.

Toegang tot e-mail en/of bestanden bij afwezigheid

Naast een daadwerkelijke controle voor de in hoofdstuk 5 beschreven doeleinden, kunnen er zich situaties voordoen die een bedreiging vormen voor de continuïteit van de dienstverlening. Vooral afwezigheden (zowel voorzien/onvoorzien als tijdelijk/definitief) kunnen in dat verband een risico vormen. Het is dan ook belangrijk om correcte afspraken te maken, zowel om de continuïteit van de dienstverlening in dergelijke gevallen te verzekeren als de privacy van de gebruiker te waarborgen.

Allereerst moeten er door de gebruiker zelf preventieve maatregelen worden genomen om een continuïteitsrisico bij afwezigheden te voorkomen:

- Werkgerelateerde bestanden moeten worden opgeslagen in het gemeenschappelijk opslagsysteem en persoonlijke bestanden onder de map C:\privé of je persoonlijke OneDrive;
- Werkgerelateerde e-mails moeten worden opgeslagen bij het relevante dossier, overeenkomstig de richtlijnen van de leidinggevende;
- Voor niet-werkgerelateerde e-mails moet een private e-mailaccount worden gehanteerd;
- In geval van een voorziene afwezigheid, moet in de mailbox een afwezigheidsboodschap worden ingesteld;
- In geval van een voorziene afwezigheid, moeten de e-mails/dossiers die tijdens de afwezigheidsperiode opvolging vereisen worden overgedragen aan collega's.

De leidinggevenden zien erop toe dat deze preventieve maatregelen worden nageleefd.

Er kunnen zich echter ook situaties voordoen waarbij het niet mogelijk is om op voorhand voldoende preventieve maatregelen te nemen die de continuïteit verzekeren. Dit is voornamelijk het geval bij onvoorziene afwezigheden. In dergelijke gevallen geldt de onderstaande procedure:

- Aan de afwezige medewerker wordt toestemming gevraagd om door de ICT-dienst een afwezigheidsbericht in te stellen en/of bepaalde mailberichten in de mailbox van de medewerker op te zoeken.
- Indien de toestemming om toegang te krijgen tot de mailbox niet verkregen kan worden omdat de afwezige medewerker niet of niet tijdig bereikt kan worden, wordt aan de algemeen directeur gemotiveerd de toestemming gevraagd om toegang te krijgen tot de mailbox van de medewerker. De algemeen directeur zal hierbij zorgvuldig afwegen of het voor de continuïteit van de dienstverlening noodzakelijk is om inzage te nemen in specifieke mails met als belangrijkste criterium dat de gegevens niet op een andere manier tijdig verkregen kunnen worden (bv. door ze opnieuw te laten toezenden door de afzenders). Indien deze uitzonderingssituatie zich voordoet wordt de betrokken medewerker hiervan zo snel mogelijk schriftelijk op de hoogte gesteld.
- Het instellen van de afwezigheidsmelding en/of het consulteren van de mailbox van de afwezige medewerker gebeurt steeds volgens het 'vier-ogen-principe', concreet: minimaal een ICT-medewerker en een lid van het managementteam daartoe aangesteld door de algemeen directeur. Zij stellen de voor de continuïteit van de dienstverlening relevante e-mails uit de mailbox ter beschikking van de organisatie en dragen er daarbij zorg voor dat er geen privé-inhouden van e-mails doorgegeven worden.

Wat de opgeslagen bestanden betreft, geldt dat persoonlijke bestanden moeten worden opgeslagen onder de map C:\privé of de persoonlijke OneDrive. De inhoud van alle andere mappen wordt als werkgerelateerd beschouwd. De organisatie kan daarom zonder meer toegang nemen tot die mappen wanneer dit ten behoeve van de continuïteit noodzakelijk is.

6. Maatregelen bij ongeoorloofd gebruik

De gebruiker die bij toepassing van de individualiseringsprocedure verantwoordelijk wordt gesteld voor een onregelmatigheid bij het gebruik van de ICT-middelen, wordt uitgenodigd voor een gesprek vóór enige beslissing of evaluatie die hem individueel kan raken. Deze procedure op tegenspraak zal de gebruiker in staat stellen het gebruik van de hem ter

beschikking gestelde ICT-middelen te rechtvaardigen. De gebruiker zal zich desgewenst door zijn vakbondsafgevaardigde kunnen laten bijstaan.

Als een ongeoorloofd gebruik van de ICT-middelen definitief is vastgesteld, kan daartegen opgetreden worden met alle gepaste middelen die volgens de relevante wettelijke bepalingen en reglementen van toepassing zijn en volgens de geldende procedures.

Voor statutaire medewerkers geldt het tuchtsysteem zoals opgenomen in de rechtspositieregeling. Voor contractuele medewerkers gelden het private arbeidsrecht, en de rechten, plichten en sancties opgenomen in het arbeidsreglement.

Als bij een occasionele of permanente controle onwettige activiteiten effectief worden vastgesteld of onwettige informatie ontdekt, dan zal dit, via de algemeen directeur, gemeld worden aan de gerechtelijke autoriteiten en/of Audit Vlaanderen.

7. Maatregelen bij uitdiensttreding

Voor alle gebruikers gelden de volgende afspraken:

- Alle toegangen naar informatiebronnen van de organisatie worden afgesloten;
- Alle privémails en -bestanden moeten door de gebruiker vooraf verwijderd worden van de ICT-systemen van de organisatie. Vanaf de dag na de uitdiensttreding kan de organisatie alle privébestanden en het persoonlijke e-mailaccount verwijderen zonder toestemming van de gebruiker;
- Werkgerelateerde informatie mag niet worden meegenomen, bewaard of opgeslagen op persoonlijke informatiedragers, noch overgedragen naar een andere organisatie;
- In de mailbox van de gebruiker moet ten laatste op de laatste werkdag een afwezigheidsboodschap worden ingesteld, waarbij de afzender erop wordt gewezen dat de gebruiker de organisatie heeft verlaten, met vermelding van de contactgegevens waar de afzender terecht kan voor verdere opvolging. In geval van een onvoorzien vertrek meldt de leidinggevende van de gebruiker onverwijld aan de ICT-dienst dat er een dergelijk afwezigheidsbericht dient te worden ingesteld;
- Om de continuïteit van de dienstverlening te verzekeren dient de gebruiker ten laatste op de laatste werkdag alle voor de dienst relevante e-mails uit zijn of haar eigen mailbox hetzij te verplaatsen naar een dienstmailbox, hetzij door te sturen naar een collega van dezelfde dienst of naar degene die de functie overneemt. In geval van een onvoorzien vertrek geldt de procedure in infra beschreven;
- In principe dienen alle werkgerelateerde bestanden te zijn opgeslagen in het gemeenschappelijk opslagsysteem dat toegankelijk is voor de leidinggevende en/of de collega's. Ten laatste op de laatste werkdag verplaatst de gebruiker (eventueel samen met de ICT-dienst) alle werkgerelateerde bestanden die nog niet op een dergelijk opslagsysteem staan, daarheen;
- Vanaf de dag na de uitdiensttreding wordt het persoonlijke e-mailaccount van de gebruiker door de ICT-dienst geblokkeerd en niet meer gebruikt voor het verzenden van e-mails. De inhoud van de mailbox en het afwezigheidsbericht worden verwijderd binnen een termijn van uiterlijk 3 maanden;
- Alle ICT-middelen die eigendom zijn van de organisatie worden ten laatste op de laatste werkdag door de gebruiker teruggegeven aan de leidinggevende of aan de ICT-dienst;
- Accounts die aangemaakt werden bij 'derde partijen' op naam of met het e-mailadres van de gebruiker worden afgesloten en/of verwijderd bij het einde van de tewerkstelling.

De leidinggevendens zien erop toe dat deze maatregelen worden nageleefd.

8. Functionaris voor gegevensbescherming

De organisatie doet beroep op de dienstverlening van de dienst informatieveiligheid van POLIS (provincie Oost-Vlaanderen), die te bereiken is via informatieveiligheid.polis@oost-vlaanderen.be.