Gezien om gevoegd te worden bij het besluit van de gemeenteraad van 26 oktober 2021 betreffende 'Goedkeuring van het ontwerp van de ICT-gedragscode, als bijlage bij het arbeidsreglement voor gemeente- en ocmw-personeel'.

ICT-Code
lokaal bestuur Maarkedal

Bijlage bij het arbeidsreglement.

maarkedal
moet je beleven

Inhoudsopgave

1 Inleiding

1.1 Waarom deze ICT-code?

De goede werking van het bestuur is sterk afhankelijk van de vlotte en doeltreffende werking van de Informatie en Communicatie Technologie (Dienst ICT) en de manier waarop personeelsleden ermee omgaan. Daarom worden naast de algemene afspraken die in de deontologische code zijn opgenomen, ook afspraken gemaakt vanuit welke waarden en normen het personeel omgaat met ICT en welk gedrag daaraan voldoet.

Deze code voor ICT biedt een **algemeen kader met waarden en principes** die de personeelsleden van het bestuur moeten respecteren bij het dagelijks gebruik van ICT. Hoewel de meeste mensen ICT dadelijk in verband brengen met technische aspecten, brengt deze code vooral de sociale en morele aspecten van ICT onder de aandacht.

Deze code is ontstaan naar aanleiding van volgende behoeften:
- Een **zorgvuldig en duurzaam beheer van ICT-middelen**:
  naast het zorgvuldig en vooruitziend hanteren van ICT-middelen is een duurzaam beheer van deze middelen van groot belang. Bij het omgaan met ICT-middelen speelt de leidinggevende een belangrijke voorbeeldrol.
- Het belang van het **beveiligen en beschermen** van bedrijfsinformatie en persoonsgegevens die niet vallen onder de openbaarheid van bestuur. De beveiliging van ICT-middelen tegen virussen en internetcriminaliteit is ook een belangrijk aandachtspunt (*zie hoofdstuk 3*).
- De behoefte aan een etiquette **voor respectvol communiceren**: de kern van de etiquette bestaat erin dat rekening wordt gehouden met de gevoelens van anderen en met de gebruiken in een organisatie, in alle situaties waarin mensen met elkaar omgaan. Door sociale media ontdekken personeelsleden nieuwe mogelijkheden en toepassingen van communiceren, maar dat houdt ook nieuwe risico's in (*zie hoofdstuk 4*).
- **Preventie van misbruik en controle van gebruik van ICT**: de maatregelen op dat vlak vloeien voort uit de teksten en aanbevelingen van de Gegevensbeschermingsautoriteit met betrekking tot cybersurveillance , en omvatten onder meer de controlemaatregelen die de werkgever kan toepassen ten aanzien van het gebruik van ICT-middelen (*zie hoofdstuk 5 en 6*).

1.2 Voor wie is de ICT-code bestemd?

De code geldt voor alle personeelsleden, mandatarissen en externen die toegang hebben tot de elektronische communicatiemiddelen van lokaal bestuur Maarkedal.

Met externen wordt eenieder bedoeld die geen personeelslid is van lokaal bestuur Maarkedal (of in die hoedanigheid werkt). Te denken valt aan bv. stagiairs, medewerkers van APB's, VZW's, ingehuurde (project) medewerkers voor zover e.e.a. niet gedekt wordt door contractuele bepalingen.

1.3 Wat zijn ICT-middelen?

Het bestuur biedt haar personeelsleden en bepaalde externen van andere organisaties die bij lokaal bestuur Maarkedal een opdracht uitvoeren een aantal informatie-, communicatie- en technologiemiddelen 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 en internetfaciliteiten;
- programmatuur en applicaties;
- computers, laptops, tablets;
- printers;
- USB-sticks;

- telefoons, gsm's, smartphones;
- opslagmedia (bijvoorbeeld op een server), …

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*).

2 Hoe omgaan met ICT-middelen?

2.1 Zorgvuldig beheer van ICT-middelen

Met de ICT-middelen die gebruikt worden tijdens het werk ga je om als een **goede huisvader**. Concreet betekent "zorgvuldig beheer van ICT-middelen" onder meer het volgende:

- Gebruik de ICT-middelen:
  - in overeenstemming met de doelstellingen;
  - niet voor commerciële doeleinden;
  - niet voor discriminatie, pesten, stalking, spamming, …
  - met respect voor de wettelijke bepalingen over het auteursrecht (*zie hoofdstuk 4.5*) en de privacy;
  - niet voor illegale praktijken;
  - kostenbewust. Voor het gebruik van door de dienst verstrekte toestellen zoals gsm's, tablets en smartphones leef je de gemaakte afspraken na;
- Spring zorgvuldig om met je wachtwoorden (*zie hoofdstuk 3.1*).
- De meeste softwareproducten zijn gelicentieerd. Voor het installeren van nieuwe software, neem je contact op met de verantwoordelijke binnen je dienst, of met de ICT servicedesk..
- Uiteraard houd je je afzijdig van discriminatie, pesten, stalking, spamming, …
- Bezoek geen sites die zich tegen de grondbeginselen van de democratie en de rechtstaat keren, die kwetsend of beledigend zijn, die in strijd zijn met de goede zeden of die een gevaar voor verslaving vormen;
- Beveilig de informatie die je zelf door middel van ICT gebruikt en deel de informatie met anderen volgens de afspraken die gelden in je dienst.
- Neem niet deel aan activiteiten die de beveiliging van de informatie kunnen schaden, zoals het versturen van kettingbrieven, virussen, valse virusmeldingen, spamberichten. Wees voorzichtig met het openen van bijlagen.
  Bij vermoeden van spamberichten, phishing (berichten met doel onrechtmatig informatie te verkrijgen) waarschuw dan de ICT servicedesk.
- Neem geen ICT-middelen mee naar huis tenzij dit absoluut noodzakelijk is voor de uitvoering van je functie.

2.2 Voorbeeldrol leidinggevende

Als leidinggevende heb je een **faciliterende rol en een voorbeeldrol** op het vlak van het gebruik van ICT.
- Je denkt zorgvuldig na over de meest gepaste ICT-middelen en over de toegangspolitiek tot systemen die in je dienst wordt gevoerd.
- Je zorgt ervoor dat je personeelsleden 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 je personeelsleden.
- 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 en vragen over informatieveiligheid waar jij als eindgebruiker zelf iets aan kan doen, en geeft de daartoe na te volgen richtlijnen.

Eén van de grootste risico's is het onzorgvuldig omgaan met het eigen gebruikerswachtwoord. Daarnaast is internetcriminaliteit een steeds toenemend risico. Verder geven we algemene richtlijnen rond

vertrouwelijkheid/openbaarheid van informatie en rond cloud-gebruik; raadpleeg voor specifieke vragen hieromtrent zo nodig de ICT-dienst of de functionaris voor gegevensbescherming, wiens contactgegevens onderaan dit document staan.

Iedere gebruiker is verantwoordelijk om informatieveiligheidsincidenten te melden. Aan het eind van dit hoofdstuk leggen we uit wat informatieveiligheidsincidenten zijn en waar deze gemeld moeten worden.

3.1 Zorgvuldig omspringen met wachtwoorden

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 **persoonlijk aansprakelijk** voor alle handelingen die worden uitgevoerd met hun eigen gebruikersnaam en wachtwoord.
Om deze aansprakelijkheid te waarborgen gelden voor het gebruik van wachtwoorden de volgende, strikt na te leven richtlijnen:

- Deel je wachtwoord nooit mee aan anderen (lijnmanagement, collega's, …); 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 aan te loggen met het account van je collega's. Voor het verzekeren van de continuïteit van de dienstverlening worden door lokaal bestuur Maarkedal veilige oplossingen voorzien, zoals het werken met een beveiligde gedeelde schijf**;**
- Elk personeelslid is verantwoordelijk voor veiligheid, en de leidinggevenden hebben bovendien een voorbeeldrol. **Een leidinggevende zal dus nooit vragen naar de wachtwoorden van de medewerkers; ook de ICT-dienstverlening zal nooit om je wachtwoord vragen;**
- Ook vraag je zelf nooit naar het wachtwoord van anderen;
- Wanneer om het even wie binnen het bestuur naar je wachtwoord vraagt, wijs je dat verzoek af met verwijzing naar deze ICT-code;

Ben je je wachtwoord vergeten, neem dan contact op met de ICT-dienst om een nieuw wachtwoord te verkrijgen.
Gebruik een **sterk wachtwoord**. Dit is een wachtwoord dat aan de volgende regels voldoet :

Aandachtspunten:

De volgende regels worden afgedwongen:
- Het wachtwoord bevat minstens 12 tekens;
- Het wachtwoord dient elke 6 maanden veranderd te worden;
- De 4 voorgaande wachtwoorden kunnen niet hergebruikt worden;
- Na 4 keer ingeven van een foutief wachtwoord wordt de gebruikersnaam een half uur geblokkeerd.

3.2 Malware (virussen) en internetcriminaliteit

Malware is de verzamelnaam voor alle 'kwaadaardige software' ('malicious software') zoals virussen, spyware, cryptolockers, enzovoort.
De mogelijke doelen van malware zijn:
- Informatie stelen (van de gebruiker of diens systeem);
- de werking van de systemen te ontregelen door gegevens/programma's te verminken of versleutelen;
- het geïnfecteerde systeem als aanvalswapen in te zetten richting andere systemen.

De verspreiding van malware gebeurt nog vaak via e-mail, ofwel als bijlage ofwel als link naar iets wat je kunt downloaden met de browser, zoals een 'gratis' programma. Het is mede daarom dat de gebruiker niet zelf (niet gekende) programmatuur kan installeren. De besmetting van de computer (tablet, smartphone) gebeurt wanneer je de bijlage opent of wanneer je op de link klikt. Klik daarom niet op links in "verdachte" mails en open niet de bijlagen die erbij zitten.

I**nternetcriminaliteit** bestaat in vele vormen en neemt steeds toe. Het is belangrijk om waakzaam te zijn tegen gerichte aanvallen zoals internetfraude en “phishing”. “Phishing” is een vorm van oplichting waarbij men hengelt naar persoonlijke informatie zoals bv. creditcardnummer, wachtwoord en accountgegevens. Soms nemen criminelen ook persoonlijk contact op met de gebruiker, per e-mail of per telefoon, en proberen ze de gebruiker over te halen om bepaalde handelingen uit te voeren (‘social engineering’).

Om zich tegen deze zaken te beschermen heeft het bestuur elke computer voorzien van anti-virussoftware.
Het is strikt verboden deze software uit te schakelen of wijzigingen aan te brengen in de huidige instellingen.
Indien de ICT-dienst merkt dat je deze anti-virussoftware uitgeschakeld hebt, kan hij je de toegang tot het netwerk onmiddellijk ontzeggen om de integriteit van het netwerk te beschermen. Vanaf dat de anti-virussoftware weer actief gemaakt is door de ICT-dienst, wordt je toegang tot het netwerk hersteld.
Volgende richtlijnen zijn van toepassing om te voorkomen dat jij of het bestuur het slachtoffer wordt van internetcriminaliteit:

- Het zelf installeren van software via e-mail, CD-roms, diskettes en/of de internettoegang op de eigen computer of ieder ander onderdeel van het netwerk is **kan enkel mits toelating van de ICT-dienst**. Indien er toch programma’s moeten worden geïnstalleerd, dan gebeurt dit uitsluitend door de ICT-dienst. Laat ook de veiligheidsmaatregelen op je computer intact (firewall, antivirus software enzovoort).
- Vertrouw nooit blindelings afzendergegevens in e-mailberichten. Neem bij twijfel langs een ander kanaal (bv. telefonisch) contact op met de afzender om de authenticiteit van het bericht te controleren.
- Denk na over de context van het bericht: “Is het logisch, te verwachten, of normaal, dat ik een bericht met deze inhoud ontvang van deze persoon of organisatie?”..
- Soms bevatten malware- en phishing mails heldere aanwijzingen dat er iets niet in orde is. **Het ontbreken van zulke aanwijzingen is echter geen *garantie* dat de mail authentiek en betrouwbaar is.** Aanwijzingen zijn onder andere spelfouten, slecht geformuleerde zinnen, het ontbreken van informatie die men in de mail zou verwachten of juist de vermelding van overtollige informatie, tegenstrijdigheden of feitelijke onjuistheden in het verhaal, de aankondiging dat je e-mail of je toegang tot online bankieren (enz.), zal worden gedeactiveerd als je niet doet wat de mail van je vraagt.
- Open geen verdachte e-mails en beantwoord ze vooral niet. **Open zeker niet de bijlage en klik niet op de links die erin staan**.. Heb je toch het bericht of de bijlage geopend of op een link in het bericht geklikt, dan neem je direct contact op met de ICT-dienst.
- Wees alert als iemand die je niet kent contact met je opneemt (per e-mail of per telefoon). Geloof niet zomaar alles wat men je vertelt en wees op je hoede als men je probeert over te halen om bepaalde handelingen (met name op je computer, smartphone, etc., of in verband met betalingen) uit te voeren;
- Wees extra op je hoede wanneer men je om **persoonlijke-, bedrijfs- of andere informatie** vraagt (ongeacht of dit per mail, per telefoon, op een webpagina of langs andere weg gebeurt); controleer of de afzender en zijn bericht legitiem zijn en ga bij twijfel niet op het verzoek in;
- Vermoed of constateer je dat je computer door malware is getroffen of dat je benaderd bent als onderdeel van een aanval, **neem dan onmiddellijk contact op met de ICT-dienst en je leidinggevende.**
- Het is verboden om via e-mail binnenkomende “virusmeldingen” naar alle personeelsleden door te sturen. Een door jou ontvangen virusmelding stuur je enkel door naar de ICT-dienst.
- Vaak wordt in dergelijke “virusmeldingen” aangeraden om bepaalde, zogenaamd schadelijke bestanden van je computer te verwijderen. Dit is strikt verboden. Neem bij twijfel omtrent virusmeldingen contact op met de ICT-dienst.

3.3 Beheer van informatie

3.3.1 Openbaarheid van bestuur versus vertrouwelijke informatie

Het bestuur 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 persoonsinformatie; andere gegevens van burgers;
- belangen van het bestuur bijvoorbeeld het geheim van beraadslagingen van organisaties die politieke beslissingen nemen, informatie over een interne audit;

- belangen binnen gerechtelijke procedures, bijvoorbeeld informatie m.b.t. gerechtelijke procedures of strafrechtelijke feiten waarbij het bestuur 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 van informatie waarover je beschikt en je verspreidt de 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.

Transport van vertrouwelijke gegevens (door bijvoorbeeld je laptop of een USB-stick mee te nemen) beperk je tot situaties waarin dat strikt noodzakelijk is voor de uitvoering van je werk. Je bent je in een dergelijke situatie steeds bewust van het risico van verlies of diefstal en gebruikt een van de speciale versleutelde USB-sticks die je bij de ICT-dienst kan verkrijgen / versleutelt de gegevens.

3.3.2 Verantwoordelijkheid beheer 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 beheerders van de ICT-opslagmogelijkheden en jezelf.

- De beheerders garanderen dat onbevoegden geen toegang hebben tot de systemen door het gebruik van firewalls, door een wachtwoordenbeleid, en toegangsbeheer.
- Je bent zelf verantwoordelijk voor de juiste en meest veilige opslag van je bestanden en voor je eigen wachtwoord. Dat wil zeggen dat je:
  - Werk gerelateerde bestanden opslaat in het gemeenschappelijk klassement op de netwerkschijf, in de juiste map. 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 harde schijf ervan. Het is niet de bedoeling om in documenten te gaan snuffelen waar je niets mee te maken hebt ook al zou dat mogelijk zijn;
  - je computer vergrendelt telkens als je je computer alleen laat. Dit kan door middel van de volgende toetsencombinaties:

3.3.3 Opslag van informatie

Over de **opslag van informatie** gelden de volgende afspraken:

- Sla geen bestanden op met commercieel karakter of voor privé-nevenwerkzaamheden.
- Persoonlijke bestanden kunnen lokaal of op de voorbehouden persoonlijke map op de server opgeslagen worden.
- Bewaar geen bestanden die:
  - obsceen of beledigend zijn;
  - in strijd zijn met de openbare orde;
  - in strijd zijn met de goede zeden;
  - het privéleven van iemand aantasten;
  - discriminerend, racistisch, seksistisch of xenofobisch zijn of die tot een dergelijk gedrag aanzetten;
  - onwettige informatie bevatten, zoals hacking software;
  - een inbreuk zijn op de auteursrechten, zoals bij muziekbestanden, films of software die je op een illegale manier verkregen hebt.

Het illegaal downloaden van bestanden is niet toegestaan. Indien langs andere weg verkregen, mag je dergelijke bestanden niet opslaan of verder verspreiden.

Van alle gebruikers wordt gevraagd om bewust om te springen met de schijfruimte van de bestandsservers. Maak er een gewoonte van om overbodige bestanden regelmatig te wissen.
Persoonlijke bestanden plaats je in een aparte map die je duidelijk als "Persoonlijk" aanduidt.

3.4 Incidenten melden

"Informatieveiligheidsincidenten" (kortweg "incidenten") zijn gebeurtenissen die de informatieveiligheid kunnen bedreigen. Iedereen is verplicht om dergelijke incidenten bij de juiste perso(o)n(en) te melden.

Onder informatieveiligheidsincidenten verstaan we onder meer:

A. Acute inbreuken op de veiligheid van de informatiesystemen:
   - Je constateert of vermoedt dat je computer, tablet of smartphone besmet is met 'malware'. **Wanneer je een besmetting constateert of vermoedt, schakel dan meteen – nog voordat je het incident meldt – de computer uit of haal hem weg uit het netwerk (door de netwerkkabel uit te trekken of de wifi op de computer uit te schakelen);**
   - je bent slachtoffer geworden van 'phishing';
   - je constateert of vermoedt dat je wachtwoord gekraakt is. **Bij een dergelijk vermoeden vervang je, nog vóór het incident te melden, zelf direct je wachtwoord;**
   - je constateert het ongeoorloofde gebruik, door om het even wie, van logische toegangen tot informatiesystemen, met name het gebruik van een account & wachtwoord door (een) andere dan de bevoegde gebruiker(s).
     Bij deze incidenten neem je onmiddellijk contact op met de dienst ICT.

B. Diefstal of verlies van ICT-middelen:
   - verlies of diefstal van elektronische gegevensdragers waarop persoonsgegevens zijn opgeslagen zoals USB-stick, dienstlaptop of tablet, maar ook je smartphone (hierop staat immers je contactenlijst). **Personeelsleden die beschikken over fysieke maatregelen om hun ICT-middelen te beveiligen, moeten die ook gebruiken (bijvoorbeeld een laptop-kabelslot of een afsluitbare kast waar de laptop bij afwezigheid in opgeborgen wordt).**

     Bij deze incidenten neem je onmiddellijk contact op met de dienst ICT.

C. Overige incidenten:
   - verlies of de diefstal van papieren documenten waarin persoonsgegevens vermeld staan (archiefstukken, brieven, …);
   - ongeoorloofde toegang door derden tot ruimten waar persoonsgegevens bewaard worden (archief, serverruimte, …);
   - inzage door onbevoegden in papieren of elektronische documenten waarin persoonsgegevens staan;
   - het op enigerlei andere wijze toegang krijgen door onbevoegden tot vertrouwelijke informatie van het bestuur;
   - iedere situatie of omstandigheid die de integriteit, beschikbaarheid of vertrouwelijkheid van de binnen lokaal bestuur Maarkedal gebruikte informatie kan schaden;
   - Ook (het vermoeden van) een inbreuk op de privacywetgeving, de wet op het rijksregister of enige andere de privacy betreffende wet moet steeds gemeld worden.

     Bij deze incidenten neem je onmiddellijk contact op met de algemeen directeur.

4 Communicatie

Als basisregel geldt '**respectvol communiceren**', zowel bij interne als externe communicatie. Indien je twijfelt kun je steeds advies vragen bij de dienst communicatie, zij helpen je graag verder.

4.1 Behoorlijk telecommunicatie gebruik

Onder telecommunicatiegebruik valt het gebruik van gsm, smartphone, telefoon, fax, enzovoort. Hoewel het gebruik van andere communicatiemiddelen (bijvoorbeeld e-mail, internet) groeit binnen de samenleving, blijft de telefoon een belangrijk contactmiddel. Een **goede bereikbaarheid en een correcte dienstverlening** blijven dan ook noodzakelijk.

4.2 Behoorlijk e-mailgebruik

E-mail is een **populair, effectief en efficiënt** communicatiemiddel binnen het bestuur met onmiskenbare voor- en nadelen. Het volgen van onderstaande richtlijnen garandeert dat e-mail een goed hulpmiddel is en blijft voor ons werk.

4.2.1 Gebruik en beheer van e-mail

Hieronder vind je een aantal richtlijnen voor een efficiënt gebruik van e-mail:

- Elk personeelslid moet minstens iedere **werk**dag zijn/haar post opvolgen, behoudens bij afwezigheid t.g.v. het bijwonen van een studiedag en andere dienstprestaties op verplaatsing;
- Geef steeds een duidelijke omschrijving in de onderwerp regel van het e-mailbericht. De onderwerp regel vat je bericht samen zoals een krantenkop.
- Wees zuinig met 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.
- 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.
- Met de mailbox-functie 'prioriteit hoog' laat je de lezer van je e-mail weten dat die e-mail dringend behandeld moet worden. Gebruik de functie daarom alleen voor dringende berichten.
- Verkies persoonlijk contact boven e-mail. Zeker als de collega voor wie je een vraag hebt dichtbij zit, kun je hem of haar beter rechtstreeks aanspreken.
- Gebruik e-mail nooit voor één op één gesprekken, discussies, meningsverschillen of emotioneel geladen boodschappen. Gebruik de telefoon voor dringende of complexe vragen.
- Beperk de bijlagen zowel wat het aantal als de grootte ervan betreft, en definieer steeds duidelijk hun inhoud. Verstuur bestanden met (gevoelige) persoonsgegevens zo veel mogelijk als een gecomprimeerd bestand (via 7-Zip) met een wachtwoord door. Voor meer informatie daarover kan je bij de ICT-dienst terecht;
- Het gebruik van e-mail voor commerciële of illegale doeleinden is verboden;
- Ruim regelmatig je mailbox op door oude of overbodige berichten te verwijderen. Die zorgen namelijk voor een onnodige belasting van de opslagschijven op de servers. Maak ook de map "verwijderde items" regelmatig leeg;
- Maak gebruik van vakantieboodschappen (*in ieder geval* wanneer je meer dan 3 opeenvolgende werkdagen afwezig zal zijn). Geef daarin aan vanaf wanneer mails niet meer en weer wel worden gelezen en bij wie de correspondent in de tussentijd terecht kan (eventueel voor welke thema's) en vermeld de contactgegevens van die persoon of personen, of een generiek e-mailadres. Bijvoorbeeld:

  Beste,

  Ik ben met vakantie van […] tot en met […] en kan je bericht niet lezen. Je e-mail wordt niet automatisch doorgestuurd, maar gaat niet verloren. Voor dringende zaken kun je mijn collega […] contacteren op het nummer […] of via e-mail op […]. Ik beantwoord je e-mail vanaf […]

  Met vriendelijke groet,
  […]

Hieronder vind je enkele afspraken voor het beheer van **dienst e-mailadressen**. Er bestaan immers heel wat dergelijke generieke postbussen die e-mails versturen én ontvangen.

- Een dienst e-mailadres wordt minstens elke dag eenmaal geopend. Als dat nodig is, wordt de postbus frequenter geopend.
- Alle e-mails worden behandeld binnen de 5 werkdagen, ofwel door meteen het antwoord op de gestelde vraag te geven, ofwel met een boodschap dat de vraag werd ontvangen en wordt behandeld door de persoon in cc. Mensen beschouwen e-mail als een snel medium, dus verwachten ze een snelle reactie.
- E-mails vanuit een dienstpostbus worden nooit anoniem verstuurd, maar uit naam van de behandelend ambtenaar. Indien je ook een telefoonnummer meegeeft, bij voorkeur het algemene nummer van een teamsecretariaat of afdeling.

4.2.2 Privé gebruik van e-mail

Personeelsleden gebruiken bij voorkeur een privé-account voor persoonlijke e-mails (bijvoorbeeld via Hotmail, Gmail, Telenet, …) om werk en privémailverkeer van elkaar te scheiden. Let hierbij op: je persoonlijke mail-account wordt niet door de systemen van lokaal bestuur Maarkedal gescand – het gevaar is dat je op die manier de systemen compromitteert. Het is niet toegestaan om voor de uitvoering van de werkopdrachten gebruik te maken van een privaat e-mail account. Alle officiële elektronische correspondentie dient te verlopen via het door de werkgever daartoe verstrekte e-mail adres.

Als je met je werk-e-mail account persoonlijke mails ontvangt en verzendt, is het aangeraden om alle persoonlijke verzonden en ontvangen e-mails te verplaatsen naar een aparte mailfolder , waarvan de naam begint met 'Privé', bij voorkeur aangevuld met de naam van het betrokken personeelslid. Via het werkmailadres verstuurde en ontvangen e-mails die niet in die map staan (maar bv nog in de inbox of in de folder "verzonden berichten"), zijn onderworpen aan de gangbare controles (*zie hoofdstuk 6*).

Deze aanbeveling is een preventiemiddel om controles en het opsporen van misbruiken te vermijden en de schending van het privéleven van de medewerker zoveel mogelijk te beperken bij die controles.

4.2.3 Inhoud van e-mail

Over de inhoud van de e-mails gelden volgende afspraken:

- Pas eerst en vooral tijdens de uitoefening van je functie dezelfde basisprincipes toe voor e-mailberichten als bij de gewone briefwisseling of bij een telefoongesprek: communiceer correct en vermeld je naam en contactgegevens.
- Gebruik enkel je eigen login en wachtwoord om e-mails te verzenden.
- Gebruik geen andere handtekening dan de jouwe.
- Verstuur neutrale berichten, dus geen berichten met een commercieel, politiek en/of religieus karakter; binnen nieuwsgroepen of op andere publieke fora kunnen nooit standpunten van lokaal bestuur Maarkedal worden meegedeeld, tenzij met toestemming van lokaal bestuur Maarkedal;
- Verstuur geen berichten die:
  - obsceen of beledigend zijn;
  - in strijd zijn met de openbare orde;
  - in strijd zijn met de goede zeden;
  - het privéleven van iemand aantasten;
  - discriminerend of xenofobisch zijn of tot een dergelijk gedrag aanzetten;
  - onjuiste informatie (zoals kettingbrieven) of malware bevatten, indien je een dergelijke mail ontvangt contacteer je de ICT-servicedesk.
- 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. Zet geadresseerden die elkaars gegevens niet mogen kennen in bcc.
- Respecteer de auteursrechten (*zie hoofdstuk 4.6*).
- Stuur geen e-mails automatisch door naar een eigen externe mailbox (bijvoorbeeld Hotmail, Gmail, Telenet, …). De veiligheid van de berichten bij die aanbieders kan immers niet gegarandeerd worden.
- Wees je er van bewust dat e-mail geen wettelijk karakter heeft en derhalve niet bindend is tenzij er een geavanceerde elektronische handtekening (met speciaal certificaat en footprint) aan gekoppeld is. Er is namelijk "een geheel van elektronische gegevens dat aan een bepaalde persoon kan worden toegeschreven en dat het behoud van de integriteit van het document aantoont" vereist om dezelfde juridische waarde te hebben als een handgeschreven handtekening. De tendens is evenwel, dat in de praktijk e-mail steeds vaker als bewijsmiddel gezien wordt.
  Binnen het bestuur geldt daarom een standaard juridische disclaimer voor alle externe mails. De e-mail handtekening wordt automatisch aangemaakt en mag niet gewijzigd worden. De juridische disclaimer zit mee vervat in de e-mail handtekening als een URL naar de website.

4.2.4 E-mail filtering

Het bestuur filtert het (officiële) e-mailverkeer op virussen en spam, en hoewel dit het risico van spam-mail en/of virussen vermindert, blijft de mogelijkheid aanwezig.

4.3 Behoorlijk intranet- en internetgebruik

De meeste collega's hebben toegang tot het intranet en het internet. Dat biedt de mogelijkheid om veel nuttige informatie voor het werk op te zoeken.

Het bestuur verwacht van haar medewerkers de discipline en verantwoordelijkheid om het internet correct en efficiënt als werkinstrument te gebruiken. Online luisteren naar de radio of tv-kijken met live-streaming, bijvoorbeeld, neemt veel bandbreedte in. Dat vertraagt het netwerk en heeft dus gevolgen voor het werk van collega's. Ook het veelvuldig bezoeken van andere soorten sites kan het netwerk belasten. Zorg daarom voor een redelijk, professioneel en zinvol gebruik van het internet tijdens het werk.

Bij het bestuur is **beperkt privégebruik** 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 bepaalde sites te bezoeken en bestanden voor privédoeleinden te downloaden.

Het is niet toegestaan sites te bezoeken die:
- zich tegen de grondbeginselen van de democratie en de rechtstaat keren, zoals sites die in verband staan met racisme, terrorisme, discriminatie, …;
- anderen kunnen kwetsen of beledigen, zoals sites met racistische of seksistische onderwerpen, pornografisch materiaal, schokkende foto's, …;
- een gevaar voor verslaving vormen zoals goksites en pornografische sites.

Evenmin zijn toegelaten (niet-limitatieve opsomming):
- Deelnemen aan chatrooms en dergelijke, ongeacht het onderwerp waarover zij handelen.
- Het downloaden en installeren van programma's zonder expliciete toelating van de ICT-Dienst;
- Het gebruik van internet voor illegale of commerciële doeleinden
- Het binnen breken in systemen van lokaal bestuur Maarkedal zelf of in enig ander netwerk of site. Het personeel mag op geen enkele wijze tussenkomen in de normale werking van het netwerk van het bestuur, noch van enig ander netwerk.

Als preventiemiddel kan de **toegang tot bepaalde internetsites geblokkeerd worden** (*zie hoofdstuk 5*).

In sommige situaties kan je zelf informatie op internet of intranet plaatsen. Als je die middelen gebruikt om zelf te communiceren, volg dan de algemene richtlijnen die van toepassing zijn op overheidscommunicatie en de regels rond spreekrecht, spreekplicht en zwijgplicht uit de deontologische code. Daarnaast respecteer je de auteursrechten (*zie hoofdstuk 4.6*).

4.4 Sociale media

Het gebruik van sociale media brengt veel mogelijkheden met zich mee. Tegelijk brengt het ook een paar **risico's** 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 het bestuur gevolgen hebben. Dit betekent dat de voor- en eventuele 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 mogelijke 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 het bestuur. Gebruik sociale media tijdens de werkuren alleen voor je werk.

4.5 Auteursrechten

4.5.1 Gebruik van materiaal en informatie door het personeel

Voor het gebruik van materiaal en informatie gelden de bepalingen van het Wetboek van economisch recht zoals toegevoegd door de wet van 19 april 2014 ("Wet houdende invoeging van boek XI, "Intellectuele eigendom" in het Wetboek van economisch recht, en houdende invoeging van bepalingen eigen aan boek XI in de boeken I, XV en XVII van hetzelfde Wetboek"). Dat betekent onder meer dat je alleen teksten of afbeeldingen van derden mag verspreiden en gebruiken met de **toestemming van de oorspronkelijke auteur**.

Wees zorgvuldig bij het publiceren van informatie en publiceer geen onwettige informatie of informatie die schade kan berokkenen aan derden.

4.5.2 Productie van materiaal/informatie door het personeel

Personeelsleden dragen in principe alle vermogensrechten op de werken die ze uit hoofde van de uitoefening van hun functie (mee) tot stand (helpen) brengen aan het bestuur over.

De auteursrechten op werken die niet uit hoofde van de uitoefening van het ambt tot stand worden gebracht blijven in principe aan het personeelslid toebehoren.

5 Preventiemiddelen

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 medewerker zoveel mogelijk te beperken.

De volgende preventieve maatregelen kunnen, op aanwijzing van de algemeen directeur, genomen worden:
- De toegang tot bepaalde sites kan geblokkeerd worden. Het bestuur verwacht immers van haar personeelsleden dat ze internet als werkinstrument gebruiken. Het (veelvuldig) bezoeken van bepaalde sites kan bovendien het netwerk te veel belasten.
- Alle werk gerelateerde informatie wordt bewaard op media die toegankelijk zijn voor de leidinggevenden en collega's (en systeembeheer). Persoonlijke bestanden op die opslagmedia worden duidelijk als 'privé' aangeduid.
- Bij een geplande langdurige afwezigheid worden afspraken gemaakt over:
    - de afwezigheidsboodschap ten behoeve van de e-mail, en het doorsturen van vóór de afwezigheid ontvangen e-mails;
    - het plaatsen van werk gerelateerde bestanden op opslagmedia die door verschillende medewerkers worden gedeeld.
- Bij een onverwachte en mogelijke langdurige afwezigheid van een medewerker wordt er zo snel mogelijk gezorgd voor een afwezigheidsboodschap (waar dit niet meer mogelijk is door de medewerker zelf zal dit via de ICT-servicedesk gedaan worden). Zo zijn alle correspondenten van het afwezige personeelslid op de hoogte van diens afwezigheid en beschikken ze over de contactgegevens van andere medewerkers bij wie ze terecht kunnen.
- Het gebruik van dienst e-mailadressen (of dienstpostbussen) kan nuttig zijn om mogelijke afwezigheden, of niet beschikbaar zijn van medewerkers op te vangen.

6 Controlemiddelen

6.1 Recht om te controleren

Lokaal bestuur Maarkedal heeft het recht om een controle uit te oefenen op het internet- en e-mailgebruik van de medewerkers. Deze controle is niet beperkt tot de eigen medewerkers, maar betreft alle gebruikers van de netwerkdiensten van lokaal bestuur Maarkedal. De privacy van de gebruikers dient hierbij zoveel als mogelijk gerespecteerd te worden.

De controle moet 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 lokaal bestuur Maarkedal op controle van werkmiddelen;
- het recht van het personeelslid/de netwerkgebruiker op zijn privéleven.

6.2 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 Teams;
- De informatie en bestanden die werknemers publiceren op het extranet en internet;
- De informatie en bestanden die werknemers opslaan op verschillende opslagmedia (alle geïdentificeerde mappen op computers, servers, document management systemen enzovoort).

De controles betreffen niet het volgende:
- Informatie uit de privésfeer
- Toestellen die geen eigendom zijn van het bestuur indien deze geen werkgerelateerde informatie bevatten.

6.3 Doel van de controle

Controle is alleen mogelijk als een van de vijf 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. Dat zijn feiten als:
   a. het kraken van computers, waaronder het op illegale manier kennis nemen van persoonsgegevens of vertrouwelijke medische bestanden;
   b. het raadplegen van sites die:
      i. zich tegen de grondbeginselen van de democratie en de rechtstaat keren, zoals sites die verband houden met racisme, terrorisme of discriminatie;
      ii. anderen kunnen kwetsen of beledigen, zoals sites met racistische of seksistische onderwerpen, pornografisch materiaal of schokkende foto's;
      iii. een gevaar voor verslaving vormen zoals goksites en pornografische sites;
      iv. het privéleven van iemand aantasten.

(2) het beschermen van bepaalde informatie. De algemene regel bij het bestuur 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 werkgever ter bescherming van die informatie is mogelijk als de belangen opgesomd in het bestuursdecreet van 7 december 2018 worden geschaad. De werkgever 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 IT-systemen van het bestuur. Daarbij hoort de controle op de bijbehorende kosten en de fysieke bescherming van de ICT-omgevingen (installaties) van het bestuur;
(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;
(5) het verzekeren van de continuïteit van de dienstverlening bij overlijden, onvoorziene afwezigheid of vertrek van een personeelslid.

De gegevens die verzameld en verwerkt worden voor een controle met een van de vijf 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 bepaald personeelslid.

6.4 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.

6.4.1 Een permanente algemene controle

Een **permanente algemene controle** is het automatisch monitoren of bewaren van elektronische communicatiegegevens. Het gaat om niet-geïndividualiseerde gegevens; dat zijn gegevens die niet gelinkt worden aan een persoon.

Sommige IT-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 het bestuur (*derde doel bij hoofdstuk 6.3*).

6.4.2 Een occasionele algemene controle

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

De algemeen directeur kan voor de doelen 1 tot en met 4 (*zie hoofdstuk 6.3*) een occasionele algemene controle 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 personeelsleden die de sites hebben bezocht;
- het aantal en het volume van de uitgaande e-mails (niet de binnenkomende berichten), maar niet de identificatie van de betrokken personeelsleden 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.

6.4.3 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 en het volume ervan. Het gaat hier dus om gegevens *over* de communicatie, niet over de *inhoud* van de communicatie. Bij controle mag de werkgever

sowieso geen inzage nemen in de inhoud van privé e-mails van het personeelslid, maar er mag wel gecontroleerd worden op ongeoorloofd privé gebruik van het email account. De tijdstippen, frequentie en geadresseerden van de e-mails is meestal voldoende om ongeoorloofd gebruik te kunnen vaststellen. Ter bescherming van zowel werkgever als werknemer zal de controle van het e-mailgebruik dan ook gebeuren door de functionaris voor gegevensbescherming of interne vertrouwenspersoon, samen met de ICT-verantwoordelijke ("vier-ogen principe"). Zij zullen de gegevens over het mailgebruik van het personeelslid die voor de controle relevant zijn, aan de werkgever beschikbaar stellen. Zij dragen er daarbij zorg voor dat er geen privé-inhouden van e-mails van het personeelslid aan de werkgever gegeven worden.

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

- Uit een occasionele algemene controle blijkt dat een of meerdere personeelsleden 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 personeelsleden op een duidelijke en begrijpelijke wijze heeft ingelicht over het bestaan van een onregelmatigheid;
  - het personeel 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*.
- Uit een occasionele algemene controle blijkt dat een of meerdere personeelsleden uit de gecontroleerde groep zich **schuldig maken** aan (*zie doelen 1-3 bij hoofdstuk 6.3*):
  - ongeoorloofde feiten, lasterlijke feiten of feiten die strijdig zijn met de goede zeden of die de waardigheid van een andere persoon kunnen schaden;
  - het openbaar maken van vertrouwelijke informatie: bepaalde informatie mag immers niet algemeen gedeeld worden, namelijk als de belangen opgesomd in het bestuursdecreet van 7 december 2018 worden geschaad;
  - feiten die de veiligheid, de performantie of de goede technische werking van de IT-systemen van de het bestuur in het gedrang brengen of de kosten abnormaal hoog doen oplopen

  In die gevallen moet het betrokken personeelslid *niet vooraf worden gewaarschuwd*; dit is een *directe individualisering*.
- Er is een **gegrond vermoeden** dat een personeelslid zich schuldig maakt aan de feiten, vermeld in het vorige punt. In dat geval kan het lijnmanagement het internetgebruik en e-mailverkeer van dat personeelslid 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**. Het betrokken personeelslid hoeft niet op voorhand gewaarschuwd te worden; dit is een *directe individualisering*.
  Met 'gegrond vermoeden' wordt bedoeld dat er nog **andere feitelijke elementen** zijn die erop wijzen dat een bepaald personeelslid zich schuldig zou maken aan de feiten vermeld in het vorige punt (bijvoorbeeld in het geval het lijnmanagement vermoedt dat een medewerker 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 verantwoordelijkheid voor het gegrond vermoeden ligt bij de algemeen directeur en diensthoofden. Zij moeten in voorkomend geval voor de rechter kunnen bewijzen dat er zo'n gegrond vermoeden was.

- 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 artikel 222 Decreet Lokaal Bestuur. Artikel 223 Decreet Lokaal Bestuur bepaalt ook dat Audit Vlaanderen voor het uitoefenen 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 werk gerelateerd e-mailverkeer, werk gerelateerde bestanden en elektronische communicatiegegevens te onderzoeken**. Die onderzoeksmogelijkheid wordt niet beperkt

door het moment waarop de e-mails, bestanden of gegevens zijn ontstaan. Het betrokken personeelslid hoeft niet vooraf gewaarschuwd te worden; dit is een *directe individualisering*. 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.

- De wet van 4 augustus 1996 betreffende het welzijn van de werknemers bij de uitvoering van hun werk, verplicht de werkgever 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.

- Uit een permanente of occasionele controle blijkt dat een gebruiker van de elektronische middelen de **veiligheid, performantie en/of goede technische werking** van de IT-systemen in **het gedrang** brengt of de **kosten abnormaal hoog** doet oplopen. In dat geval kan nagegaan worden wie de gebruiker is met een directe individualisering.

De betrokken werknemer dient op de hoogte te worden gebracht van de controle en heeft het recht om hierbij aanwezig te zijn voor zover dit de objectiviteit van de controle niet in gedrang brengt.

6.5 Toegang tot e-mail en / of bestanden bij plotse, onverwachte langdurige of definitieve afwezigheid van een personeelslid

Allereerst is het de verantwoordelijkheid van ieder diensthoofd (ook in éénmansdiensten) om bij een geplande / voorziene (al dan niet definitieve) afwezigheid van zichzelf of een medewerker **voor een volledige overdracht van alle informatie, bestanden en e-mails te zorgen**: vóór het vertrek worden de werk gerelateerde bestanden en mailberichten overgedragen aan de juiste collega's, of op een plek gezet die voor lokaal bestuur Maarkedal toegankelijk is. Er worden afspraken gemaakt over de afwezigheidsboodschap voor e-mail (welke collega is aanspreekbaar voor wat; welke vragen moeten aan het algemene dienst-mailadres worden gericht). Alle persoonlijke (privé) bestanden en e-mails worden door het vertrekkende personeelslid hetzij gewist, hetzij opgeslagen in een map met de naam "Persoonlijk" (gevolgd door de eigen naam). Door deze maatregelen wordt voorkomen dat lokaal bestuur Maarkedal tijdens de geplande afwezigheid toegang moet nemen tot de persoonlijke mailbox van het personeelslid en wordt – wanneer toegang onverhoopt toch noodzakelijk blijkt – diens privacy maximaal beschermd.

Veel e-mails zijn juist wél voor een individueel personeelslid bedoeld (bijvoorbeeld mails in het kader van de opvolging van een dossier dat door het personeelslid behandeld wordt). **Om de continuïteit te garanderen, is het de verantwoordelijkheid van het diensthoofd om bij een onvoorziene afwezigheid van een personeelslid (bv. ziekte) van meer dan twee opeenvolgende werkdagen, aan de ICT-dienst te melden dat er een afwezigheidsbericht moet worden ingesteld op het mailadres van de afwezige collega***.* Het diensthoofd geeft aan de ICT-dienst de tekst van het bericht door; minimaal staan daarin de gegevens zoals vermeld onder titel 4.3.1 ("Gebruik en het beheer van e-mail", onderdeel 'vakantieboodschappen').

Werk gerelateerde e-mails aan het persoonlijke e-mailadres van het personeelslid, die ontvangen zijn tussen het begin van een ongeplande afwezigheid en het instellen van het afwezigheidsbericht, vallen tussen wal en schip maar kunnen voor de continuïteit belangrijke informatie bevatten. Omdat men niet kan voorkomen dat tijdens de afwezigheid ook private e-mails ontvangen zijn (die dan niet door het personeelslid naar de map "Persoonlijk" verplaatst zijn, conform titel 4.3.2), mag lokaal bestuur Maarkedal niet zonder meer inzage in de mailbox nemen wanneer er naar werk gerelateerde e-mails uit die (korte) periode gevraagd wordt.

Dit zal eerder bij uitzondering gebeuren. Lokaal bestuur Maarkedal weegt in zo'n geval af of het voor de continuïteit van de dienstverlening noodzakelijk is om inzage te nemen in specifieke mails (*doel 5 onder titel 6.3*). Als dit vermoed wordt en de gegevens niet op een andere manier verkregen kunnen worden (bv. door ze opnieuw te laten toezenden) kan lokaal bestuur Maarkedal, mits gemotiveerd besluit en op advies van de

functionaris voor gegevensbescherming, met onderstaande procedure inzage verkrijgen in de voor de goede werking noodzakelijke e-mail berichten en/of bestanden.

De toegang tot de mailbox gebeurt door de functionaris voor gegevensbescherming of interne vertrouwens-persoon, samen met de ICT-dienst ("vier-ogen principe"). Zij zullen de e-mails uit de mailaccount van het personeelslid die met betrekking tot de continuïteit van de dienstverlening relevant zijn, aan de werkgever beschikbaar stellen. Zij dragen er daarbij zorg voor dat er geen privé-inhouden van e-mails van het personeelslid aan de werkgever gegeven worden.

Wat de bestanden op schijf betreft, geldt dat persoonlijke bestanden door personeelsleden moeten worden opgeslagen in een aparte map die duidelijk als "Persoonlijk" is aangeduid (*zie titel 3.3.3, "Opslag van informatie"*). De inhoud van alle andere mappen waartoe het personeelslid toegang heeft, wordt als werk gerelateerd beschouwd. Lokaal bestuur Maarkedal kan daarom zonder meer toegang nemen tot die andere mappen wanneer dit ten behoeve van de continuïteit noodzakelijk is.

Deze maatregelen kunnen pas genomen worden nadat men geprobeerd heeft contact op te nemen met betrokkene om hem in de mogelijkheid te stellen dit zelf te regelen.

7 Maatregelen bij ongeoorloofd gebruik

De werknemer die bij toepassing van de individualiseringsprocedure verantwoordelijk wordt gesteld voor een onregelmatigheid bij het gebruik van de elektronische online communicatiemiddelen, wordt uitgenodigd voor een gesprek vóór enige beslissing of evaluatie die hem individueel kan raken; deze procedure op tegenspraak zal de werknemer in staat stellen het gebruik van de hem ter beschikking gestelde elektronische onlinecommunicatiemiddelen te rechtvaardigen. De werknemer zal zich desgewenst door zijn raadsman naar keuze kunnen laten bijstaan.

Als een ongeoorloofd gebruik van de communicatiemiddelen definitief is vastgesteld, kan 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 het Decreet Lokaal Bestuur. Voor contractuele medewerkers gelden het private arbeidsrecht, en de rechten, plichten en sancties opgenomen in het arbeidsreglement.

Als de algemeen directeur (of zijn vertegenwoordiging) of een externe dienstverlener bij een occasionele of permanente controle onwettige activiteiten effectief vaststelt of onwettige informatie ontdekt, dan zal dit, via de algemeen directeur, gemeld worden aan de gerechtelijke autoriteiten. Bij twijfel is het de bedoeling dat Audit Vlaanderen op de hoogte wordt gebracht voor verder onderzoek.

Onwettige activiteiten zijn bijvoorbeeld gokactiviteiten, hacking, surfen naar sites met (kinder)pornografisch materiaal of het bezit ervan enzovoort. Onwettige informatie is bijvoorbeeld hacking-software.

De bestraffing van misdrijven tegen de vertrouwelijkheid, integriteit en beschikbaarheid van informatiesystemen is voorts ook geregeld in het Strafwetboek.

8 Maatregelen bij uitdiensttreding

Voor zowel het personeel als de mandatarissen geldt dat:
- alle toegangen naar informatiebronnen van het bestuur worden afgesloten
- alle persoonlijke informatie vooraf door het personeelslid moet verwijderd worden van de opslagbronnen van het bestuur;
- informatie niet wordt meegenomen, bewaard, opgeslagen op persoonlijke informatiedragers of overgedragen naar een andere werkgever.

- Om de continuïteit van de dienst te garanderen dient het personeelslid ten laatste op de laatste werkdag samen met de ICT-dienst alle voor de dienst relevante e-mails uit zijn of haar eigen mailbox hetzij te verplaatsen naar een afdelings-mailbox, hetzij door te sturen naar een collega van dezelfde dienst of naar degene die de functie overneemt.
- In principe dienen alle werk gerelateerde bestanden te zijn opgeslagen op opslagmedia die toegankelijk zijn voor de hiërarchische chef en de collega's. Ten laatste op de laatste werkdag verplaatst het personeelslid samen met de ICT-dienst alle werk gerelateerde bestanden die nog niet op een dergelijk opslagmedium staan, daarheen.
- Vanaf de dag na de uitdiensttreding kan de ICT-dienst alle persoonlijke bestanden en persoonlijke mailbox verwijderen zonder toestemming van het uittredend personeelslid
- Alle ICT-middelen die ter beschikking gesteld werden aan het personeelslid worden ten laatste op de laatste werkdag teruggegeven aan de hiërarchische chef of aan de ICT-dienst.

9 ICT-dienst

Voor ICT ondersteuning en vragen kan u terecht bij dienst ICT, Charlotte.DeMullier@maarkedal.be of Jasper.Billemont@maarkedal.be

10 Functionaris voor gegevensbescherming

Het bestuur doet beroep op de dienstverlening van de dienst eGov van de provincie Oost-Vlaanderen, die te bereiken is via informatieveiligheid@oost-vlaanderen.be.