Vlaamse overheid

Agentschap voor Overheidspersoneel

SECTORCOMITE XVIII
VLAAMSE GEMEENSCHAP EN VLAAMS GEWEST

protocol nr. 330.1057

PROTOCOL HOUDENDE DE CONCLUSIES VAN DE ONDERHANDELINGEN VAN 18 NOVEMBER 2013 EN 17 FEBRUARI 2014 DIE GEVOERD WERDEN IN HET SECTORCOMITE XVIII VLAAMSE GEMEENSCHAP EN VLAAMS GEWEST

Over

Ontwerp van omzendbrief : Integer omgaan met ICT-middelen

door de afvaardiging van de overheid, samengesteld uit:

vaste leden

1. de heer Kris Peeters, minister-president van de Vlaamse Regering en Vlaams minister van Economie, Buitenlands Beleid, Landbouw en Plattelandsbeleid, voorzitter;

2. de heer Geert Bourgeois, Vlaamse minister van Bestuurszaken, Binnenlands Bestuur, Inburgering, Toerisme en Vlaamse Rand;

3. de heer Philippe Muyters, Vlaams minister van Financiën, Begroting, Werk, Ruimtelijke Ordening en Sport;

enerzijds,

en de afvaardigingen van de drie representatieve vakbonden:

- de Algemene Centrale der Openbare Diensten, vertegenwoordigd door:

  de heren Jan Van Wesemael
  Chris Moortgat

- de Federatie van de Christelijke Syndicaten der Openbare Diensten die onder meer de ACV-Openbare Diensten en de ACV-Transport en Communicatie groepeert, vertegenwoordigd door:

  mevrouw Nathalie Hiel

- het Vrij Syndicaat van het Openbaar Ambt, vertegenwoordigd door:

  de heren Jos Mermans
  Francis Van Lindt

anderzijds,

Werd een eenparig akkoord afgesloten over bijgaand ontwerp van omzendbrief : Integer omgaan met ICT-middelen.

Bijgaand document maakt integraal deel uit van dit protocol.

Brussel, 21-02-2014

DE AFVAARDIGING VAN DE REPRESENTATIEVE VAKORGANISATIES:

Voor de Algemene Centrale der Openbare Diensten

Jan Van Wesemael

Voor de Federatie van de Christelijke Syndicaten der Openbare Diensten

Nathalie Huel

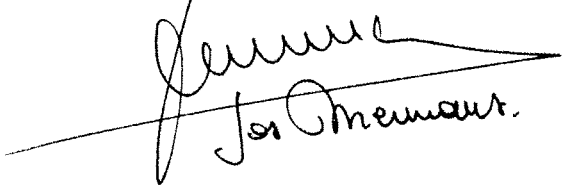
DE AFVAARDIGING VAN DE OVERHEID

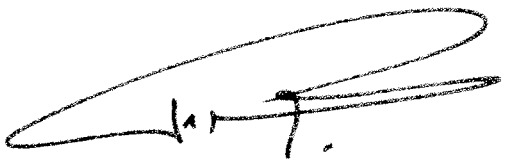
De Voorzitter,

Kris Peeters
minister-president van de Vlaamse Regering
en
Vlaams minister van Economie, Buitenlands Beleid, Landbouw en Plattelandsbeleid

Geert Bourgeois
Vlaams minister van Bestuurszaken, Binnenlands Bestuur, Inburgering, Toerisme en Vlaamse Rand

Voor het Vrij Syndicaat van het
Openbaar Ambt





Philippe Muyters
Vlaams minister van Financiën,
Begroting, Werk, Ruimtelijke Ordening,
en Sport

Omzendbrief BZ 2014

Omzendbrief ICT-code

Aan de personeelsleden van de entiteiten zonder rechtspersoonlijkheid (departementen en IVA's zonder rechtspersoonlijkheid)

Viceminister-president van de Vlaamse Regering en Vlaams minister van Bestuurszaken, Binnenlands Bestuur, Inburgering, Toerisme en Vlaamse Rand

Arenbergstraat 7, 1000 Brussel
Tel. 02 552 69 00 - Fax 02 552 69 01
kabinet.bourgeois@vlaanderen.be

Datum:

Betreft: Integer omgaan met ICT-middelen

Deze omzendbrief vervangt omzendbrief ICT/2004/02.

1. Inleiding

1.1 Waarom deze ICT-code?

De goede werking van de Vlaamse overheid is sterk afhankelijk van de vlotte en doeltreffende werking van de Informatie en Communicatie Technologie (ICT) en de manier waarop personeelsleden ermee omgaan. Daarom is het raadzaam om naast de algemene afspraken die in de *deontologische code* zijn opgenomen, ook af te spreken 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 de Vlaamse overheid 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.

Veel entiteiten hebben al een entiteitsspecifieke ICT-code of een entiteitsspecifiek reglement. Die specifieke codes en reglementen kunnen blijven gelden op voorwaarde dat ze niet in strijd zijn met de algemene afspraken van deze ICT-code. Als dat nodig is, maken entiteiten een specifieke aanvullende code.

Deze code is ontstaan naar aanleiding van volgende behoeften. U vindt ze verder uiteengezet in deze omzendbrief.

- De behoefte aan een **geactualiseerde ICT-code**: deze code heft de omzendbrief ICT/2004/02 op. De ICT-code van 2004 is verouderd door de vele technische ontwikkelingen op gebied van ICT. Daarnaast spelen ook maatschappelijke ontwikkelingen een rol bij de veroudering van de ICT-code van 2004, bijvoorbeeld de opkomst van de sociale media.

- 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. Een degelijk beheer van ICT-middelen blijft niet binnen de grenzen van de werkomgeving, maar geldt ook bij het plaatsonafhankelijk werken (*zie punt 2 hieronder*).

- 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 punt 3 hieronder*).

- 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 punt 4 hieronder*).

- **Preventie van misbruik en controle van gebruik van ICT**: de maatregelen op dat vlak vloeien voort uit de teksten en aanbevelingen van de *Privacycommissie* met betrekking tot cybersurveillance (*zie punt 5 en 6 hieronder*).

1.2 Voor wie is de ICT-code bestemd?

De code geldt voor de entiteiten zonder rechtspersoonlijkheid (departementen en IVA's zonder rechtspersoonlijkheid).

1.3 Wat zijn ICT-middelen?

De Vlaamse overheid biedt haar personeelsleden en bepaalde werknemers van andere organisaties die bij de Vlaamse overheid 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;
- computers, laptops, tablets;
- printers;
- USB-sticks;
- telefoons,gsm's, smartphones;
- opslagmedia (bijvoorbeeld een server) ...

De **informatie op de ICT-systemen** behoort ook tot de ICT-middelen. De afspraken over het beheer van die informatie vindt u in het hoofdstuk over veiligheid (*zie punt 3.4 hieronder).*

2. Hoe omgaan met ICT-middelen?

2.1 Zorgvuldig beheer van ICT-middelen

Met de ICT-middelen die gebruikt worden tijdens het werk gaat u om als een **goede huisvader**. Dat principe houdt in dat u zich gedraagt als een **vooruitziend** en **zorgvuldig** persoon.

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

Daarnaast bent u bereid **verantwoording** af te leggen over het gebruik van middelen. De middelen dienen om het algemeen belang na te streven, dus u gebruikt de middelen met het oog op zuinigheid, efficiëntie en effectiviteit.

Hier gelden de specifieke afspraken voor het omgaan met ICT-instrumenten vanuit de ***deontologische code.***

- Gebruik ICT-middelen in overeenstemming met de doelstellingen.
- Gebruik ICT-middelen niet voor commerciële doeleinden.
- Gebruik de middelen niet voor discriminatie, pesten, stalking, spamming ...
- Gebruik de middelen op een wettelijke manier met respect voor het *auteursrecht* (*zie punt 4.6 hieronder*) en de privacy.
- Op de meeste softwareproducten rusten auteursrechten. Voor het installeren van nieuwe software, neemt u contact op met uw ICT-contactpunt of met de servicedesk.
- Ga kostenbewust om met ICT-middelen. Voor toestellen zoals gsm's, tablets en smartphones houdt u zich aan de gemaakte afspraken bij uw entiteit.
- Occasioneel gebruik van de middelen voor privédoeleinden is alleen mogelijk als dat de uitvoering van uw taken en uw productiviteit en die van uw collega's niet in het gedrang brengt. Voor bepaalde middelen is privégebruik toegestaan als sociaal voordeel.
- Blijf beleefd en professioneel in uw online communicatie, voer geen verhitte discussies en pas op met cynisme en sarcasme. Geschreven berichten komen soms anders over dan bedoeld.
- 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.
- Verstuur geen kettingbrieven, virussen of valse virusmeldingen. Als u een virus of valse virusmelding ontvangt, waarschuw dan de *servicedesk* (tel. 02/5539000, *servicedesk@vlaanderen.be*) en het virusmeldpunt (*antivirus@vlaanderen.be*).
- Als u spamberichten in uw mailbox ontvangt, kunt u de mails als bijlage doorsturen naar: *antispam@vlaanderen.be*.
- Spring voorzichtig om met uw wachtwoorden (*zie punt 3.2 hieronder*).
- Beveilig de informatie die u zelf door middel van ICT gebruikt en deel de informatie met anderen volgens de afspraken die gelden in uw entiteit.

2.2 Duurzaam beheer van ICT-middelen

Artikel 57, 1°, van het decreet van 21 december 2007 houdende bepalingen tot begeleiding van de begroting 2008 (Belgisch Staatsblad, 31 december 2007) zorgt ervoor dat de Vlaamse Regering lichamelijke roerende goederen, bijvoorbeeld ICT-middelen, die eigendom zijn van haar diensten en niet meer gebruikt worden, kan **schenken** aan:

- onderwijsinstellingen;
- verenigingen zonder winstoogmerk;
- stichtingen.

De diensten van de Vlaamse Regering beschikken immers vaak over een voorraad aan roerende goederen die buiten gebruik zijn gesteld, maar toch nog nuttig kunnen zijn.

De Vlaamse Regering heeft de voorwaarden van het afstaan van goederen niet door middel van een reglementair uitvoeringsbesluit bepaald. Wel kan elke bevoegde Vlaamse minister beslissen om de goederen die tot zijn beleidsdomein behoren, te schenken onder de voorwaarden die hij zelf vastlegt.

Voor het schenken van ICT-middelen wordt er aandacht besteed aan het **professioneel verwijderen van de data** die de ICT-middelen bevatten. Op 25 april 2003 keurde de Vlaamse Regering het *"ICT-veiligheidsbeleid voor de beleidsdomeinen van de Vlaamse overheid"* goed. Daarin staat dat de beheerder er voor moet zorgen dat zowel de gegevens, als de instellingen van alle onderdelen van informatiesystemen die data bevatten, onherstelbaar verwijderd worden.

In het kader van de *gemeenschappelijke ICT-dienstverlening* kunnen de *aangesloten entiteiten* gebruik maken van een te betalen aanbod voor de afvoer van informaticamateriaal en voor de opruiming van harde schijven.

2.3 Groene ICT

Er zijn een heleboel dingen die u kunt doen om **groener om te springen met technologie en grondstoffen**, en de druk op ons milieu te verlichten.

- Zet uw computer, beeldscherm en printer uit als u naar huis gaat.
- Zet uw computer, beeldscherm en printer in slaapstand tijdens uw lunch en vergaderingen vanaf 15 minuten. Bent u meer dan een uur weg, zet de computer dan uit.
- Stel het energiebeheer van uw computer in om energie-efficiënt te werken. Voor computers die met het raamcontract ICT van de Vlaamse overheid aangekocht werden, is dit sinds 1 april 2010 de standaardinstelling.
- Gebruik geen schermbeveiliging.

2.4 Voorbeeldrol leidinggevende

Als leidinggevende heeft u een **faciliterende rol en een voorbeeldrol** op het vlak van het gebruik van ICT.

- U denkt zorgvuldig na over de meest gepaste ICT-middelen en de toegangspolitiek tot systemen die in uw entiteit wordt gevoerd.
- U zorgt ervoor dat uw personeelsleden de geschikte vorming volgen om de ICT-systemen op een passende manier te gebruiken.
- U bespreekt mogelijke risico's van het gebruik van ICT met uw personeelsleden.

- U volgt de kosten en het gebruik van ICT op aan de hand van de toegestane rapportering. (*zie punt 6 hieronder*)
- U hebt de verantwoordelijkheid om problemen rond ICT-gebruik aan te pakken of aan te kaarten.

2.5 Telewerken / tijds- en plaatsonafhankelijk werken

Door de toename van het tijds- en plaatsonafhankelijk werken en de moderne informaticamogelijkheden zijn de **grenzen tussen privé en werk vaak minder duidelijk.** Als u documenten en materiaal mee op verplaatsing neemt (bv. naar huis), treft u de nodige maatregelen om die informatie te beschermen, zowel thuis als onderweg. Respecteer de bestaande afspraken die zijn opgenomen in de *omzendbrief rond telewerk*, zowel de algemene afspraken als de afspraken binnen uw entiteit.

3. Veiligheid

3.1 ICT-veiligheidsbeleid

Gebruik ICT-middelen met zorg en beveilig zowel de toestellen, de toepassingen als de informatie die u bewaart op die middelen. Het *ICT-veiligheidsbeleid* van de Vlaamse overheid bevat de minimale veiligheidsvereisten. Elke entiteit is vrij om hogere eisen te stellen aan haar **ICT-veiligheidsbeleid**.

Als uw laptop, tablet of smartphone **gestolen** wordt, moet u dat onmiddellijk aan de *helpdesk* melden. Entiteiten die een beroep doen op de *gemeenschappelijke ICT-dienstverlening*, kunnen contact opnemen met het telefoonnummer 02 553 90 00, intern 39000. ICT'ers zullen dan het nodige doen om te voorkomen dat iemand op onterechte wijze toegang verkrijgt tot de werkomgeving van de Vlaamse overheid.

In de onderstaande gevallen moet u onmiddellijk contact opnemen met de ***helpdesk***:
- uw wachtwoord is gekraakt;
- er staat een virus op uw computer;
- u bent het slachtoffer geworden van *internetfraude* (= phishing).

Schakel ook meteen uw computer uit of haal hem weg uit het netwerk (door de netwerkkabel uit te trekken of wifi uit te schakelen).

Wanneer personeelsleden beschikken over fysieke maatregelen om hun ICT-middelen te beveiligen, moeten zij die ook gebruiken.

Meer informatie over ICT-veiligheid vindt u op de desbetreffende website.

3.2 Zorgvuldig omspringen met wachtwoorden

Gebruikers zijn **persoonlijk aansprakelijk** voor alle handelingen die worden uitgevoerd met hun eigen gebruikersidentificatie/wachtwoord.

Deel daarom nooit een wachtwoord mee aan anderen (lijnmanagement, collega's,...) en scherm het wachtwoord af van onrechtmatig gebruik: **wachtwoorden zijn persoonlijk en vertrouwelijk**. Log dus ook niet aan met het account van uw collega's. En schrijf een wachtwoord nooit op.

Elk personeelslid is verantwoordelijk voor veiligheid, en het lijnmanagement heeft bovendien een voorbeeldrol. **Het lijnmanagement zal dus niet vragen naar de paswoorden van de medewerkers.** Voor het verzekeren van de continuïteit van de dienstverlening adviseert het lijnmanagement veilige oplossingen te gebruiken zoals bijvoorbeeld het werken met een beveiligde gedeelde schijf of document managementsysteem.
Ook **de ICT-dienstverlening zal niet vragen naar de paswoorden van de medewerkers.**

Gebruik een sterk wachtwoord. Een sterk wachtwoord bevat minimaal acht karakters en bestaat uit kleine letters, hoofdletters, cijfers en/of speciale tekens (bijvoorbeeld -,_,*). Meer informatie over het *veilig gebruik van wachtwoorden* vindt u op het ICT-extranet.

Op de website vindt u meer *richtlijnen met betrekking tot het wachtwoordenbeleid en de toegangscontrole*.

3.3 Malware (virussen) en internetcriminaliteit

Malware is de verzamelnaam voor alle 'kwaadaardige software' (*'Malicious Software'*) zoals virussen, Trojaanse paarden, spyware, enzovoort.

De verspreiding van malware gebeurt nog vaak via e-mail, ofwel als bijlage ofwel als link naar iets wat u kunt downloaden met de browser, zoals een 'gratis' programma.
De bedreiging van **internetcriminaliteit** bestaat in vele vormen en neemt steeds toe. Het is belangrijk waakzaam te zijn tegen gerichte aanvallen zoals internetfraude of phishing, een vorm van oplichting waarbij men hengelt naar persoonlijke informatie zoals uw 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 te overhalen om bepaalde handelingen uit te voeren (*'social engineering'*).

Hieronder vindt u adviezen om te voorkomen dat u het slachtoffer wordt van internetcriminaliteit.

- Laat de veiligheidsmaatregelen op uw computer intact (firewall, antivirus software enzovoort).
- Vertrouw nooit blindelings afzendergegevens in e-mailberichten.
- Denk na over de context van het bericht: 'Klopt het dat ik dit bericht ontvang van deze organisatie?'.
- Open geen verdachte e-mails en beantwoord ze vooral niet. Open zeker niet de bijlage en bezoek ook niet de links die erin staan. Bij twijfel, kunt u het best (telefonisch) contact opnemen met de afzender van het bericht.
- Wees alert als iemand die u niet kent, contact met u opneemt (per e-mail of per telefoon). Geloof niet zomaar alles wat men u vertelt en wees op uw hoede als men u probeert te overhalen om een handeling uit te voeren.
- Vermoedt u dat uw computer door malware is getroffen of dat men u heeft proberen te benaderen als onderdeel van een aanval, neem dan onmiddellijk contact op met de servicedesk en het virusmeldpunt (*antivirus@vlaanderen.be*).

Meer antivirusinformatie vindt u op de website.

3.4 Beheer van informatie

3.4.1 Openbaarheid van bestuur versus vertrouwelijke informatie

De Vlaamse overheid beschikt over een schat 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;
- belangen van de Vlaamse overheid, bijvoorbeeld het geheim van beraadslagingen van instanties die politieke beslissingen nemen, informatie over een interne audit;
- belangen binnen gerechtelijke procedures, bijvoorbeeld informatie m.b.t. gerechtelijke procedures of strafrechtelijke feiten waarbij de Vlaamse overheid 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.

U denkt na over het soort van informatie waarover u beschikt en u verspreidt de informatie alleen als u er zeker van bent dat het niet over vertrouwelijke gegevens gaat. Bij twijfel neemt u onmiddellijk contact op met uw leidinggevende.

De verspreiding of verwerking van bepaalde persoonsgegevens mag enkel met een aangifte of een machtiging van de Privacycommissie (*www.privacycommission.be/nl*).

Transport van vertrouwelijke gegevens (door bijvoorbeeld uw laptop of een USB-stick mee te nemen) beperkt u tot situaties waarin dat strikt noodzakelijk is voor de uitvoering van uw werk. U bent zich in een dergelijke situatie steeds bewust van het risico en encrypteert de gegevens.

Verantwoordelijkheid beheer van informatie

Voor een papieren document is het vaak gemakkelijk om zelf de vertrouwelijkheid te garanderen. U 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 uzelf.

- De beheerders garanderen dat onbevoegden geen toegang hebben tot onze systemen door het gebruik van firewalls, door een wachtwoordenbeleid of toegangsbeheer ...
- Uzelf bent verantwoordelijk voor de juiste en meest veilige opslag van uw bestanden en voor uw eigen wachtwoord. Dat wil zeggen dat u:
    - werkgerelateerde bestanden opslaat in het gemeenschappelijk klassement in de juiste map. Zo kunt u informatie delen met uw collega's en is er geen verlies van informatie mogelijk, aangezien van alles een back-up word gemaakt. Het is niet de bedoeling om in andere mappen en documenten te gaan snuffelen waar u niets mee te maken heeft;
    - uw computer vergrendelt met een wachtwoord als u uw computer alleen laat (Ctrl - alt - delete → deze computer vergrendelen/ lock computer).

De gedeelde verantwoordelijkheid geldt als er een contract is met de beheerders. Een contract op maat is vaak niet mogelijk bij **cloud toepassingen**. Cloud computing is het langs het internet op aanvraag beschikbaar stellen van hardware, software en gegevens en kan zeer snel worden aangeleverd of vrijgegeven. De cloud staat voor het internet dat

met al de computers die erop aangesloten zijn een soort 'wolk van computers vormt'. Bij cloud computing draaien de computerprogramma's niet op de computer van de gebruiker, maar op (een of meer) machines in die cloud. De gebruiker is geen eigenaar van de gebruikte hardware, software en gegevens en is niet verantwoordelijk voor het onderhoud ervan.

Als u informatie op een cloud platform zet (linkedIn, Facebook, Dropbox, Yammer, Google Docs,...) dan bent u onderworpen aan de voorwaarden van dat platform. Dat u bedrijfsinformatie op een cloudtoepassing zet waar ze is afgeschermd met een login en wachtwoord, betekent nog niet noodzakelijk dat die informatie daar veilig staat.

Bij cloud toepassingen gelden de volgende afspraken.

- Weeg goed af of het nodig is of een meerwaarde heeft om data op te slaan op het desbetreffend cloud platform. Een applicatie die de Vlaamse overheid aanbiedt, verdient steeds voorkeur.
- Sla alleen niet-vertrouwelijke en niet-kritische data voor de organisatie op in de cloudtoepassing, gelet op de beperkte zekerheid rond beveiliging. Bij voorkeur worden deze data geëncrypteerd. Sla geen persoonsgegevens op.
- Zorg ervoor dat u het overzicht behoudt over welke informatie waar staat.
- Vertrouw niet alleen op een cloud platform voor de beschikbaarheid van data (cloud diensten komen en gaan, passen hun voorwaarden en financiering of kostprijs aan en zijn meestal niet aansprakelijk als de dienst een paar uur of enkele dagen niet beschikbaar is).

3.4.2 Opslag van informatie

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

- Sla geen bestanden op met commercieel karakter of voor privé-nevenwerkzaamheden.
- Bewaar geen bestanden die:
    - obsceen of beledigend zijn;
    - in strijd zijn met de openbare orde;
    - in strijd zijn met de goede zeden;
    - het privé-leven van iemand aantasten;
    - discriminerend, racistisch of xenofobisch zijn of die tot een dergelijk gedrag aanzetten;
    - onwettige informatie bevatten, zoals hacking software;
    - een inbreuk zijn op de auteurswet zoals muziekbestanden, films, software die u op een illegale manier verkregen hebt.

Het **illegaal downloaden** van bestanden is niet toegestaan. U mag dergelijke bestanden ook niet opslaan of verder verspreiden.

4. Communicatie

4.1 Hoe communiceren?

Als basisregel geldt '**respectvol communiceren**', zowel bij interne als externe communicatie.

In deze rubriek vindt u meer informatie over wat dat concreet betekent voor het communiceren met:
- telecommunicatie;
- e-mail;
- extranet en internet;
- sociale media.

Daarbij respecteert u de wet op het auteursrecht van 1994 (*zie punt 4.6 hieronder*).

4.2 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 Vlaamse overheid, blijft de telefoon een belangrijk contactmiddel. Een **goede bereikbaarheid en een correcte dienstverlening** blijven dan ook noodzakelijk.

Richtlijnen en informatie over verschillende initiatieven ter verbetering van de telefonische dienstverlening vindt u op de website.

Een overzicht van de gsm-belprofielen van het ministerie van de Vlaamse gemeenschap vindt u eveneens op de website. De kosten in het buitenland kunnen sterk verschillen van bij ons, onderzoek de beste manier van communiceren voor u vertrekt.

4.3 Behoorlijk e-mail gebruik

E-mail is een **populair, effectief en efficiënt** communicatiemiddel binnen de Vlaamse overheid. Toch horen we onszelf en anderen ook klagen over de toename van e-mails en over het verkeerde en soms storende gebruik ervan. Het volgen van onderstaande richtlijnen garandeert dat e-mail een goed hulpmiddel is en blijft voor ons werk.

4.3.1 Gebruik en het beheer van e-mail

Hieronder vindt u adviezen voor een efficiënt gebruik van e-mail.

- Geef steeds een duidelijke omschrijving in de onderwerpregel van het e-mailbericht. De onderwerpregel vat uw 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 relevant dat alle geadresseerden bij de zaak worden betrokken. Stuur uw antwoord of bedenkingen in dat geval alleen naar de oorspronkelijke afzender.
- Maak, alleen voor dringende berichten, gebruik van de mailbox-functie 'prioriteit hoog'. De lezer van uw e-mail weet dan dat die e-mail dringend behandeld moet worden.
- Verkies persoonlijk contact boven e-mail. Zeker als de collega voor wie u een vraag hebt dichtbij zit, kunt u hem of haar beter rechtstreeks aanspreken.
- Gebruik e-mail nooit voor een op een 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. Maak maximaal gebruik van document management systemen, zodat u links kunt doorsturen in plaats van bijlagen.

Hieronder vindt u ook enkele afspraken voor het beheer van **interactieve generieke e-mailadressen** (geen generieke e-mailadressen die gebruikt worden als distributielijst bijvoorbeeld voor het versturen van nieuwsbrieven). Er bestaan immers heel wat dergelijke generieke e-mailadressen die e-mail versturen én ontvangen. De kwaliteit ervan wat de frequentie waarmee ze gelezen worden, de degelijkheid van antwoorden enzovoort betreft, loopt erg uiteen.

- Bij het aanmaken van generieke e-mailadressen moet er grondig worden nagegaan of het zinvol is een generiek adres te creëren. De naam van het generieke e-mailadres kunt u het best ook even aftoetsen met Taaladvies.
- Een generiek e-mailadres wordt minstens elke dag eenmaal geopend. Als dat nodig is, wordt de mailbox frequenter geopend.
- Alle e-mails worden beantwoord, ofwel meteen, 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 de generieke mailbox worden nooit anoniem verstuurd en geven altijd ook een telefoonnummer op, bij voorkeur het algemene nummer van een teamsecretariaat of afdeling.

Het lijnmanagement raadt de personeelsleden aan een privé-account te gebruiken voor persoonlijke e-mails (bijvoorbeeld via Hotmail, Gmail ...) om werk en privémailverkeer volledig van elkaar te scheiden. Als dat niet mogelijk of gewenst is, adviseert het lijnmanagement om alle verzonden en ontvangen persoonlijke e-mails te bewaren in een aparte map, waarvan de naam begint met 'Persoonlijk', bij voorkeur aangevuld met de naam van de betrokken werknemer. Als medewerkers persoonlijke e-mails versturen met het werkmailadres, kunnen die e-mails gecontroleerd worden (permanente algemene controles, occasionele algemene controles en individuele controles). De 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 controles.

4.3.2 Inhoud van e-mail

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

- Pas eerst en vooral tijdens de uitoefening van uw functie dezelfde basisprincipes toe voor e-mailberichten als bij de gewone briefwisseling of bij een telefoongesprek: communiceer correct en vermeld uw naam en contactgegevens.
- Gebruik enkel uw login en paswoord om e-mails te verzenden.
- Gebruik geen andere handtekening dan de uwe.
- Verstuur neutrale berichten, dus geen berichten met een commercieel, politiek en/of religieus karakter.
- 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.
- Houd er rekening mee dat 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.
- Verstuur geen kettingbrieven, echte of valse virusberichten of verhitte reacties. Meld een virus aan de juiste instanties. Als u twijfelt over de herkomst van een mail of als u vermoedt dat er een virusrisico bestaat, open dan de mail niet, en zeker niet de bijlagen, maar neem contact op met de *helpdesk*.
- Respecteer de wet op het auteursrecht van 1994 (*zie punt 4.6 hieronder*).
- Houd het kort. E-mail is bedoeld voor snelle informatie-uitwisseling, begin daarom uw e-mail meteen met de conclusie of actie.
- Ruim regelmatig uw mailbox op door oude of overbodige berichten te verwijderen. Die zorgen voor een onnodige belasting van de opslagschijven op de servers. Maak de map 'verwijderde items' regelmatig leeg.
- Stuur geen 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.
- Maak gebruik van *vakantieboodschappen*. 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, personen of generiek e-mailadres.

4.3.3 E-mail filtering

Conform de huidige afspraken van het generieke *ICT-veiligheidsbeleid*, blijft het e-mailverkeer gefilterd op virussen en spam.

De filterregels worden bepaald door het college van ambtenaren-generaal (CAG). De *gemeenschappelijke ICT- dienstverlener* zal samen met het overlegorgaan over informatieveiligheid periodiek de filterregels evalueren en noodzakelijke wijzigingen aanbevelen aan het CAG.

4.4 Behoorlijk extranet- en internetgebruik

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

De Vlaamse overheid verwacht van haar medewerkers de discipline en verantwoordelijkheid om het internet correct en efficiënt als werkinstrument te gebruiken. Luisteren naar de radio of tv-kijken met live streaming neemt bijvoorbeeld veel bandbreedte in. Dat vertraagt het netwerk en heeft dus gevolgen voor het werk van collega's. Zorg daarom voor een redelijk, professioneel en zinvol gebruik van het internet tijdens het werk (*zie punt 4.54.5 hieronder*).

Bij de Vlaamse overheid is **beperkt privégebruik** van het internet toegestaan onder bepaalde voorwaarden:
- voor zover het is toegestaan binnen de eigen entiteit;
- als het de uitvoering van uw taken en uw productiviteit en die van uw collega's niet in het gedrang brengt. (zie ook *deontologische code*)

Het is echter niet toegestaan om bepaalde sites te bezoeken en bestanden voor privédoeleinden te downloaden.

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

Als preventiemiddel kan het lijnmanagement de **toegang tot bepaalde internetsites blokkeren**. De Vlaamse overheid verwacht immers van haar werknemers dat ze internet als werkinstrument gebruiken. Ook belasten bepaalde sites het netwerk (*zie punt 5 hieronder*).

In sommige situaties kunt u zelf informatie op internet of extranet plaatsen. Als u 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 het Vlaams *personeelsstatuut* (VPS) en de *deontologische code.*

Daarnaast respecteert u de wet op het auteursrecht van 1994 (*zie punt 4.6 hieronder4.6 hieronder*).

4.5 Sociale media

Bij de Vlaamse overheid 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 personeelsleden van de Vlaamse overheid gebruiken sociale media en dat geeft heel veel mogelijkheden:
- u kunt er kennis mee delen;
- u kunt uw professionele ideeën toetsen aan de realiteit;
- u kunt in contact komen met andere medewerkers, experts in uw vakgebied, burgers, enzovoort.

Tegelijk brengt dat ook een paar **risico's** mee: hoe scheidt u werk en privé? Hoe let u op uw rol als ambtenaar? Die risico's kunnen zowel voor uzelf als voor de organisatie gevolgen hebben. Dus 'bezint eer ge begint!'

Het is belangrijk dat u ook op sociale media de richtlijnen van *de deontologische code* in acht neemt, verantwoordelijk en loyaal bent en duidelijk maakt of u in eigen naam spreekt of vanuit de organisatie. Deelname aan sociale media is waarschijnlijk niet uw volledige taakinhoud. Vergeet de rest van uw werk niet en gebruik sociale media tijdens de werkuren alleen voor uw werk.

Binnen de Vlaams overheid is er een *handreiking sociale media* tot stand gekomen dankzij co-creatie. De **handreiking** bestaat vooral uit een verzameling richtlijnen over hoe u als individuele medewerker verstandig sociale media kunt gebruiken. De handreiking hangt samen met een *visienota sociale media,* die net als de handreiking positief is geadviseerd door het CAG. Bovendien sluit de handreiking aan bij *de deontologische code* van de Vlaamse overheid.

4.6 Auteursrechten

4.6.1 Gebruik van materiaal en informatie door een werknemer

Voor het gebruik van materiaal en informatie geldt de *wet van 30/06/1994 betreffende het auteursrecht en de naburige rechten*. Dat betekent onder meer dat u alleen teksten of afbeeldingen van derden mag verspreiden en gebruiken met de **toestemming van de oorspronkelijke auteur**. Daarbij moeten personeelsleden zowel de auteursrechten van derden als die van de Vlaamse overheid respecteren.

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

Op de website vindt u meer concrete informatie over
- de rechten als gebruiker van een werk en wat verboden is;
- intellectuele eigendom.

4.6.2 Productie van materiaal/informatie door werknemer

Overeenkomstig het *Vlaamse personeelsstatuut* (VPS) dragen personeelsleden alle **vermogensrechten aan de Vlaamse overheid** over op de werken die bij de uitoefening van hun functie tot stand zijn gebracht en waarvan ze de (mede)auteur zijn.
Het gaat daarbij om de auteursrechten op:
- computerprogramma's;
- alle andere werken die personeelsleden voor de uitvoering van hun functie tot stand brengen.

Dat wil zeggen dat de auteursrechten op werken die niet bij de uitoefening van het ambt tot stand worden gebracht in principe aan het personeelslid blijven toebehoren.

5. Preventiemiddelen van de werkgever

Het lijnmanagement treedt eerst en vooral preventief op om:
- controles en het opsporen van misbruiken te vermijden;
- de schending van het privéleven van de medewerker zoveel mogelijk te beperken bij controles.

Het lijnmanagement neemt de volgende preventieve maatregelen.

- Het lijnmanagement kan de toegang tot bepaalde sites blokkeren. De Vlaamse overheid verwacht immers van haar werknemers dat ze internet als werkinstrument gebruiken. Het veelvuldig bezoeken van bepaalde sites kan bovendien het netwerk belasten. Op de website vindt u meer informatie over het *beheer van het internetverkeer* (Die informatie geldt alleen voor de entiteiten die gebruik maken van de gemeenschappelijke ICT-dienstverlener).
- Het lijnmanagement raadt de personeelsleden van de Vlaamse overheid aan een privé-account te gebruiken (*zie punt 4.3.1*).
- Alle werkgerelateerde bestanden worden bij voorkeur bewaard op opslagmedia die toegankelijk zijn voor de hiërarchische chef en de collega's. Persoonlijke bestanden op die opslagmedia worden duidelijk als 'Persoonlijk' aangeduid.
- Bij een geplande langdurige afwezigheid worden afspraken gemaakt over:
    - het doorsturen van e-mails;

  - het plaatsen van afwezigheidsboodschappen in e-mailaccounts;
  - het plaatsen van werkgerelateerde 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. 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.

6. Controlemiddelen van de werkgever

6.1 Recht om te controleren

Het lijnmanagement heeft het **recht om het internet- en e-mailgebruik** van de medewerkers te controleren. Daarbij moet het **recht op een privéleven** van de personeelsleden gerespecteerd 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**: de controle en 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 werkgever op controle van werkmiddelen;
- het recht van de werknemer op zijn privéleven.

6.2 Wat kan worden gecontroleerd?

Het lijnmanagement kan controles doen van:
- het gebruik van e-mail;
- het gebruik van internet;
- het gebruik van andere professionele elektronische communicatiemiddelen zoals Skype;
- 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, documentmanagement-systemen enzovoort).

6.3 Doel van de controle

Controle van het lijnmanagement 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:
  - het kraken van computers, waaronder het op illegale manier kennis nemen van persoonsgegevens of vertrouwelijke medische bestanden;
  - het raadplegen van sites die

- zich tegen de grondbeginselen van de democratie en de rechtstaat keren, zoals sites die verband houden met racisme, terrorisme of discriminatie;
- anderen kunnen kwetsen of beledigen, zoals sites met racistische of seksistische onderwerpen, pornografisch materiaal of schokkende foto's;
- een gevaar voor verslaving vormen zoals goksites en pornografische sites;
- het privéleven van iemand aantasten.

(2) het beschermen van bepaalde informatie. De algemene regel bij de Vlaamse overheid is 'openbaarheid van bestuur'. Er zijn echter uitzonderingen op die regel, omdat bepaalde informatie niet geschikt is om algemeen gedeeld te worden. Een controle van de werkgever is mogelijk ter bescherming van die informatie als de belangen opgesomd in *artikel 13 en 14 van het decreet van 16 maart 2004 betreffende de openbaarheid van bestuur*, 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 de Vlaamse overheid. Daar hoort de controle op de bijbehorende kosten en de fysieke bescherming van de ICT-omgevingen (installaties) van de Vlaamse overheid bij;

(4) het te goeder trouw naleven van deze ICT-code en andere richtlijnen voor het gebruik van onlinetechnologieën;

(5) het verzekeren van de continuïteit van de dienstverlening bij overlijden, onvoorziene afwezigheid of vertrek van een werknemer.

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 het lijnmanagement 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.

i. 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.

Het lijnmanagement kan sommige IT-systemen controleren voor de veiligheid, de performantie en de goede technische werking. Daar hoort de controle op de bijbehorende kosten en de fysieke bescherming van de ICT-omgevingen (installaties) van de Vlaamse overheid bij (*derde doel bij punt 6.3 hierboven*).

ii. Een occasionele algemene controle

Een **occasionele algemene controle** is het verzamelen en de inzage door het lijnmanagement van algemene on-linecommunicatiegegevens die tijdens een beperkte periode werden gegenereerd en betrekking hebben op een groep van personeelsleden.

Het lijnmanagement kan voor de doelen 1 tot en met 4 (*zie punt 6.3 hierboven*) 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.

iii. Een individuele controle

Bij een individuele controle controleert het lijnmanagement:
- wie, welke websites heeft bezocht, wanneer en voor hoe lang;
- wie bepaalde e-mails heeft verzonden, de geadresseerden en het volume ervan. Het lijnmanagement kan ook de verzonden werkgerelateerde e-mails lezen als ze de medewerkers aanbeveelt persoonlijke e-mails te verzenden via een privé account (Hotmail, Gmail ...). Het lijnmanagement gaat ervan uit dat alle e-mails verzonden met het account dat ter beschikking wordt gesteld door de Vlaamse overheid, werkgerelateerd zijn.

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 on-linetechnologieën. De individuele controle kan in die situatie alleen nadat het lijnmanagement:
  - 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 on-linecommunicatiegegevens geïndividualiseerd zullen worden als opnieuw een dergelijke onregelmatigheid wordt vastgesteld (= indirecte individualisering).

- Uit een occasionele algemene controle blijkt dat een of meerdere personeelsleden uit de gecontroleerde groep zich **schuldig maken** aan:
  - 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 artikelen 13 en 14 van het *decreet van 16 maart 2004 betreffende de openbaarheid van bestuur*, worden geschaad;
  - feiten die de veiligheid, de performantie of de goede technische werking van de IT-systemen van de Vlaamse overheid in het gedrang brengen (*zie doel 1-3 bij 6.3 hierboven*).

  In die gevallen moet het betrokken personeelslid niet vooraf worden gewaarschuwd (= directe individualisering).

- Het lijnmanagement heeft 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. Het lijnmanagement kan dat 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 (= directe individualisering). Met 'gegrond vermoeden' wordt bedoeld dat er nog andere **feitelijke elementen** (bijvoorbeeld pestmails) zijn die erop wijzen dat een bepaald personeelslid zich schuldig zou maken aan de feiten vermeld in het vorige punt. De verantwoordelijkheid dat er een gegrond vermoeden is, ligt bij de lijnmanagers. Zij moeten in voorkomend geval voor de rechter kunnen bewijzen dat er zo'n gegrond vermoeden was.

- Een personeelslid is **overleden of onvoorzien afwezig of heeft de dienst verlaten en kan niet worden bereikt**. In dat geval kan het lijnmanagement het werkgerelateerde e-mailverkeer en de werkgerelateerde bestanden op de opslagmedia van het betrokken personeelslid raadplegen. Het doel daarvan is de **continuïteit van de dienstverlening te garanderen.** Als het lijnmanagement de medewerkers verplicht persoonlijke e-mails te verzenden via een privé account (Hotmail, Gmail ...), dan mag het ervan uitgaan dat alle e-mails verzonden met het account dat ter beschikking wordt gesteld, werkgerelateerd zijn. Als een dergelijke verplichting niet bestaat, kan het e-mailaccount en de opslagmedia van het afwezige personeelslid ook persoonlijke – niet-werkgerelateerde – berichten en informatie bevatten. Dan gebeurt het raadplegen via een veiligheidsadviseur of een medewerker belast met integriteitszorg. Die kan dan nagaan welke berichten en informatie werkgerelateerd zijn en dus mogen worden ingezien door de hiërarchische chef en welke persoonlijke zijn.

- *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**. Het lijnmanagement 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.

- 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 34 van *het kaderdecreet bestuurlijk beleid* van 18 juli 2003. Datzelfde artikel 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 werkgerelateerde e-mailverkeer, werkgerelateerde bestanden en elektronische communicatiegegevens te onderzoeken**. Die onderzoeks- mogelijkheid wordt niet beperkt door het moment waarop de e-mails, bestanden of gegevens zijn ontstaan. Het betrokken personeelslid hoeft niet vooraf gewaarschuwd te worden (= 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.

- 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 het lijnmanagement nagaan wie de gebruiker is met een directe individualisering.

7. Maatregelen bij ongeoorloofd gebruik

Als een ongeoorloofd gebruik van de communicatiemiddelen is vastgesteld, kan het lijnmanagement **optreden met alle gepaste middelen** die volgens het *Vlaams personeelsstatuut* gelden. Een tuchtstraf kan alleen worden opgelegd nadat het personeelslid werd gehoord en de kans kreeg het gebruik van de ICT-middelen te rechtvaardigen.

Op *http://www.bestuurszaken.be/BVR_Deel01-T1T2* vindt u het toepassingsgebied van het VPS. Het tuchtsysteem in het VPS gelden alleen voor statutaire medewerkers van de Vlaamse overheid. Voor contractuele medewerkers gelden het private arbeidsrecht, de rechten en plichten en sancties die leidinggevenden kunnen opnemen in het arbeidsreglement.

Als het lijnmanagement of een externe dienstverlener bij een occasionele of permanente controle onwettige activiteiten effectief vaststelt of onwettige informatie ontdekt, dan zal het lijnmanagement dat melden 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 kinderpornografisch materiaal of het bezit ervan enzovoort.
Onwettige informatie is bijvoorbeeld hacking software.

De bestraffing van misdrijven tegen de vertrouwelijkheid, integriteit en beschikbaarheid van informatiesystemen vindt u in het *Strafwetboek van 8 juni 1967*.

Geert BOURGEOIS
Viceminister-president van de Vlaamse Regering en Vlaams minister van Bestuurszaken, Binnenlands Bestuur, Inburgering, Toerisme en Vlaamse Rand