GEBRUIK VAN E-MAIL, INTRANET EN INTERNET BIJ VDAB

1. Inleiding

E-mail, intranet en internet zijn middelen die VDAB aanbiedt aan zowel haar eigen personeelsleden. (hierna vermeldt als personeelsleden), als aan werknemers van andere organisaties en cursisten, die middels een samenwerkingsovereenkomst gebruik mogen maken van de VDAB infrastructuur (hierna vermeld als externen).

Deze voorschriften resulteren uit de wetgeving ter zake en de noodzaak om de informatica-infrastructuur optimaal te laten functioneren voor elkeen binnen VDAB.

Wanneer deze communicatiemiddelen door externen worden gebruikt, is het VDAB lijnmanagement, dat aan deze externen daarvoor de toelating heeft gegeven, ook verantwoordelijk voor de naleving van deze regels door hen.

2. Algemeen kader

E-mailen en surfen met de middelen die VDAB ter beschikking heeft gesteld, is in principe alleen toegestaan voor de uitvoering van de opgelegde taken. Krachtens de deontologische code (omzendbrief AZ/MIN/98/4 van 1 september 1998) moeten de personeelsleden zich tijdens de diensturen volledig aan hun job wijden en mogen zij geen ongeoorloofd gebruik maken van uitrusting of materiaal van de VDAB voor privédoeleinden.
Ongeoorloofd gebruik is ruimer dan illegaal gebruik en omvat onder meer ook het gebruik van e-mail en internet voor private commerciële doeleinden of een gebruik dat de infrastructuur te zwaar zou belasten.
Het feit dat uw e-mailadres uw persoonlijke naam bevat, doet daaraan geen afbreuk. Dit neemt niet weg dat VDAB aanvaardt dat u bij de uitoefening van uw arbeidstaak en opdrachten recht hebt op respect voor uw persoonlijke levenssfeer en dat u in beperkte mate privécontacten mag onderhouden met collega's en met derden buiten de onderneming[1].

Het lijnmanagement kan, om eventueel ongeoorloofd gebruik van deze communicatiemiddelen tegen te gaan, steeds inhoudelijke controles laten uitvoeren, zoals :

- een globaal overzicht (per organisatorische entiteit) van de gedurende een bepaalde periode bezochte websites alsook de frequentie en het volume van de doorgezonden informatie, zonder daarbij het individueel gebruik vrij te geven; bij een gegrond vermoeden van ongeoorloofd gebruik van het internet, kan bovendien worden nagegaan wie bepaalde websites bezoekt

- een overzicht van de afzender, geadresseerde en grootte van de gedurende een bepaalde periode verzonden e-mailberichten zoals deze na de overbrenging op de server kunnen worden afgelezen; de kennisname van de inhoud van een

[1] Zie in dit verband het Advies uit eigen beweging (nr. 10/2000) van de Commissie voor Bescherming van de Persoonlijke Levenssfeer, betreffende het toezicht door de werkgever op het gebruik van het informaticasysteem op de werkplaats uitgebracht op 3 april 2000

emailbericht is niet toegestaan (tenzij binnen de perken van wetgeving inzake de bescherming van de persoonlijke levenssfeer en van het telecommunicatiegeheim).

De voor IT bevoegde dienst kan omwille van de goede werking van het informaticasysteem steeds technische controles (laten) uitvoeren, zoals:

- het isoleren of tegenhouden van verdachte berichten, zoals kettingmails en extreem omvangrijke e-mails die een congestie of vertraging van het netwerk kunnen teweegbrengen, alsook e-mails die besmet zijn met een computervirus.

Indien ongeoorloofd gebruik van deze communicatiemiddelen is vastgesteld, kan het lijnmanagement optreden tegen eigen personeelsleden met alle gepaste middelen die krachtens het Vlaams personeelsstatuut gelden. Voor externen, zal in zulk geval het lijnmanagement van betrokkene hiervan worden ingelicht.
Uiteraard mogen er geen laakbare handelingen worden gesteld door de personeelsleden of externen. Zo is verspreiden van discriminerende boodschappen (van welke aard ook zoals racistische en seksistische boodschappen) via e-mail, nieuwsgroepen, intranet, internet en dergelijke, niet geoorloofd. Het lijnmanagement kan krachtens het Vlaams personeelsstatuut de auteur van zulke boodschappen steeds een tuchtstraf opleggen aan eigen personeelsleden. We wensen er de aandacht op te vestigen dat de auteur van racistische boodschappen bovendien strafrechtelijk kan worden vervolgd op grond van de wet van 30 juli 1981.
De VDAB is niet verantwoordelijk voor misdrijven die door de personeelsleden of externen tijdens de uitoefening van hun taken worden gesteld.
Daarnaast moeten ook andere rechtsregels gerespecteerd worden, zoals de wetgeving op het auteursrecht.

3. Richtlijnen voor het e-mailgebruik

Virussen, hoaxen[2]

Als er twijfel bestaat over de herkomst van een mail of het vermoeden dat er een virus- of hoaxrisico bestaat, open dan de mail niet, en zeker niet de bijlagen, maar neem contact op met de helpdesk.

Kettingmail

Doe niet mee aan het verspreiden van om het even welke vorm van kettingmail.

Naam

E-mailadressen zijn strikt persoonlijk. Fraude met e-mailadressen is verboden.

Wachtwoorden

Elke mailbox is beveiligd met een wachtwoord. Hiervoor gelden de algemene regels voor wachtwoorden binnen de VDAB

- Gebruik geen triviale wachtwoorden.
- De laatste drie gebruikte wachtwoorden mogen niet opnieuw gebruikt worden.
- Verzeker de vertrouwelijkheid van uw wachtwoord. Verander uw wachtwoord als u vermoedt dat de vertrouwelijkheid niet langer verzekerd is.
- Gebruik nooit de naam en het wachtwoord van een andere persoon.

[2] Een hoax is een viruswaarschuwing waarachter in feite geen echt virus verscholen zit

Inkomende externe e-mail
Abonnementen op via mail verspreide elektronische magazines (E-zines) kan alleen voor wat professioneel relevant is.

Versturen van vertrouwelijke informatie
Houd er rekening mee dat e-mail zich niet zo goed leent tot vertrouwelijke communicatie. Een kleine manipulatiefout kan ervoor zorgen dat een bericht ongewenst bij de verkeerde personen terechtkomt.

Nieuwsgroepen
De personeelsleden en externen zijn individueel verantwoordelijk voor de inhoud van de berichten die zij verspreiden via de gemodereerde nieuwsgroepen.

4. Richtlijnen voor intranet- en internetgebruik

Aansluiting op het net

- Alle aansluitingen op het internet worden uitgevoerd via het VDAB Intranet en de Internet Service Providers (ISP). Dit geldt zowel voor de pc's die rechtstreeks op het SIP-netwerk of het cursistennetwerk aangesloten zijn als deze die op een afstand via een publiek net aangesloten zijn (vast of via inbellen). Hieruit volgt dat voor deze pc's een rechtstreekse aansluiting via modem naar een ISP uitgesloten is. Een dergelijke rechtstreekse aansluiting kan bij wijze van uitzondering enkel worden toegestaan voor pc's die nooit op het SIP-netwerk aangesloten worden.
- Om een aansluiting mogelijk te maken krijgt de persoon toegang tot het internet via zijn naam en een paswoord. De internettoegang kan niet gedelegeerd worden. Het lijnmanagement kan ook steeds toegang tot internet beperken tot bepaalde websites.
  • Buiten de info bestemd voor de VDAB-produktie (cfr. Onderrichtingen) mag er niets verspreid worden zonder toelating van de leidende ambtenaren van de centrale diensten.
- Betalende en/of expliciete internet-sites mogen niet geraadpleegd worden.
- Beluisteren van radioprogramma's, muziek, videobroadcasts zijn te belastend voor de internetlijnen en dus ook niet toegelaten.

5. Contactpersonen voor meer inlichtingen:

1. Security (mail: security@vdab.be)