

ICT - gebruikscode

1. Terminologie

- ICT-middelen: de apparatuur (computers, vaste en mobiele telefoons, faxmachines, modems, ...) de netwerken en de programma's en toepassingen (weg, elektronische post, databanken, nez) die het mogelijk maken digitale gegevens te raadplegen, bewerken, opslaan en verzenden.
- Programmatuur: alle software die door x werd aangekocht, gehuurd of die voor x werd ontwikkeld.
- Bestanden: alle informatie in digitale vorm zoals bijvoorbeeld e-mails, websites, tekstbestanden, tekeningen of foto's.

2. Algemeen

2.1. Doelstelling van deze Gebruikscode

De ICT infrastructuur van x biedt de mogelijkheid om een goede interne en externe communicatie en efficiëntie te verzekeren. Deze omgangscode biedt een aantal regels die door gebruiker moeten worden opgevolgd, zodat de ICT infrastructuur optimaal benut wordt en de goede werking van het netwerk gewaarborgd wordt.

2.2. Toegang en paswoord

Elke gebruiker krijgt een mail-adres en toegang tot het netwerk. Het paswoord is strikt persoonlijk. Misbruiken (door anderen) vallen onder uw verantwoordelijkheid.

2.3. Softwarepakketten, hardware

Het beheer van PV-netwerk is zeer complex en bepaalde taken op uw PC zijn centraal en automatisch gestuurd. Daarom worden alle hardware en softwareprogramma's uitsluitend met goedkeuring van de systeembeheerder geïnstalleerd.

2.4. Verantwoordelijkheid

Alle hard- en software is eigendom van x.

Elke gebruiker behandelt de hem toevertrouwde apparatuur als een goede huisvader en neemt de richtlijnen van de systeembeheerder in acht.

Iedere gebruiker is verantwoordelijk en aansprakelijk voor de ICT middelen die hem of haar werden verschaft en voor alles wat onder zijn/haar gebruikersidentificatie en paswoord gebeurt.

2.5. Gebruik

In principe kunnen de ICT-middelen enkel worden gebruikt voor het uitvoeren van taken binnen x door de werknemer van x.

Abnormale kosten door persoonlijk of ongeoorloofd gebruik (vb. telefoongesprekken naar het buitenland of schade aan apparatuur door persoonlijk gebruik) kunnen op de gebruiker verhaald worden.

De gebruiker is verplicht ernstige inbreuken en kwetsbaarheden te melden .

3. E-mail gebruik

Een e-mail heeft dezelfde juridische waarde als een fax.

Het e-mail adres dat door x ter beschikking wordt gesteld mag in principe enkel voor professionele doeleinden worden gebruikt (intern en extern).

Occasioneel gebruik voor privé-doeleinden wordt toegestaan, maar mag nooit strijdig zijn met x-belangen, de goede zeden, de goede samenwerking tussen collega's, racismewetgeving, enz.

Persoonlijke e-mail van een ander adres mag niet geconsulteerd worden in x (via webpagina's of via ophalen van een mailbox).

Iedereen leest dagelijks zijn/haar e-mail (internet en intranet). Bij lange afwezigheid wordt machtiging gegeven aan een collega om de dringende mails te verwerken.

De optie geadresseerde in Blindcopy (waarbij andere niet zien dat deze persoon een Copy kreeg), is voor gewoon gebruik verboden.

Teveel mail ontvangen is belastend voor het netwerk. Vermijd ook daarom nieuwsgroepen, kettingbrieven, chatrooms, jokes, e.a.

Open geen verdachte mails van ongekende afzenders. Open nooit attachments van verdachte mails. Bij verdachte omstandigheden, vermijdt u een connectie met het netwerk en verwittigt u onmiddellijk de systeembeheerder.

Bij het versturen van e-mail door de gebruiker dient steeds een disclaimer te worden aangehecht. Deze disclaimer wordt door de systeembeheerder geïnstalleerd.

4. Opslag van gegevens

Alle bestanden moeten worden bewaard op het centrale netwerk. Respecteer de richtlijnen voor bestandsstructuur en naamgeving.

Op de eigen pc mogen geen dossiers worden gearhiveerd.

5. Internetgebruik

Het internet mag enkel gebruikt worden voor professionele doeleinden. Het gebruik dat indruist tegen de essentie van deze gebruikscodes of tegen de aanvullende instructies van de Secretaris zijn verboden, zoals:

- het verspreiden of downloaden van gegevens in strijd met de auteursrechten
- het rondsturen van berichten die als een aantasting van iemands mendelijke waardigheid kunnen beschouwd worden, zoals berichten die kunnen ervaren worden als racistisch, discriminerend op basis van geslacht, seksuele geaardheid, godsdienst, afkomst, handicap, ... of die sexueel intimiderend zijn;
- het consulteren van erotische of pornografische sites, zelfs wanneer het gaat om wettelijk toegelaten publicaties;

- het doorsturen, downloaden van bestanden die het netwerk nodeloos belasten (meer dan 10 Mb, radio of telefoon over internet,...), tenzij dit met voorafgaande uitdrukkelijke toestemming van de systeembeheerder;
- de deelname aan kettingsbrieven, chatrooms, newsgroups, ... ongeacht het onderwerp waarover zij handelen.

Het gebruik van het internet mag in ieder geval nooit strijdig zijn met x belangen, de goede zeden, racismewetgeving, enz.

6. Toezicht en controle

* De systeembeheerder voert dagelijks de nodige controles uit op een niet-geïndividualiseerde wijze om de goede werking van het netwerk te waarborgen (overbelasting, veiligheid). De procedure daartoe ligt ter inzage bij de systeembeheerder.

* Indien de systeembeheerder bij deze dagelijkse controle vaststelt:

- dat een gebruiker bewust of onbewust de veiligheid of de goede werking van het systeem in het gedrang brengt;
- of dat er ongeoorloofde feiten, feiten strijdig met de goede zeden of feiten die de waardigheid van een andere persoon schenden (incl. ernstige pesterijen), voorkomen ;
- of dat de veiligheid en/of de goede technische werking van het geheel van de IT-netwerksystemen van x, met inbegrip van de controle op de kosten die ermee gepaard gaan alsook de fysieke bescherming van de installaties;

mag de systeembeheerder deze gebruiker zonder enige formaliteit identificeren en contacteren om de problemen te verhelpen.

* Indien de systeembeheerder bij deze dagelijkse controle vaststelt dat een gebruiker de regels van x of de e-policy niet naleeft (vb. overmatig gebruik van e-mail voor persoonlijke doeleinden) of de technologie niet ter goeder trouw aanwendt, moet de systeembeheerder alle gebruikers op de hoogte brengen van een onregelmatigheid en van het feit dat een individualisering zal plaats hebben wanneer een nieuwe onregelmatigheid wordt vastgesteld.

De systeembeheerder mag de activiteit van de geïndividualiseerde gebruiker, indien noodzakelijk en na verwittiging, ook verder opvolgen.

Bij vaststelling van ernstige inbreuken op de ICT-gebruikscodes is de systeembeheerder gehouden de Secretaris hiervan op de hoogte te brengen.

De gebruiker die bij de toepassing van de individualisering verantwoordelijk wordt gesteld voor een onregelmatigheid bij het gebruik van de elektronische on-line communicatiemiddelen, wordt uitgenodigd voor een gesprek vóór iedere beslissing of evaluatie die hem individueel kan raken; deze procedure op tegenspraak zal de gebruiker in staat stellen het gebruik van de hem ter beschikking gestelde elektronische on-line communicatiemiddelen te rechtvaardigen. De gebruiker kan zich desgewenst laten bijstaan door een raadsman.

7. VERTROUWENSPERSOON

Voor vragen over de gebruikscodes, klachten in verband met het gebruik, pesterijen of ander storend gedrag kan je terecht bij de systeembeheerder, de heer/mevrouw.....

Ondertekening van de gebruikscode

Ik heb een exemplaar ontvangen van de "ICT-gebruikscode x" en ik het er uitgebreid kennis van genomen.

Hierbij geef ik de toestemming dat niet alleen de elektronische communicatiegegevens, maar ook de inhoud ervan mogen worden geopend bij een individualisatie.

Ik verklaar mij volledig akkoord met de inhoud ervan.

Naam,

Datum en handtekening, voorafgegaan door de mededeling 'voor akkoord'.