Regels voor het gebruik van ICT-apparatuur door contractanten

Art. 1
Dit document is van toepassing op de personen aan wie, in het kader van de uitvoering van een contract van aanneming van diensten of van werken tussen (i) Electrabel of een andere onderneming van de Groep ENGIE (hierna "de Klant" genoemd) en (ii) een contractant (hierna “Contractant” genoemd), apparatuur voor Informatie- en Communicatietechnologie (hierna "ICT-apparatuur" genoemd) is toevertrouwd door de Klant. Deze personen worden hierna "Gebruikers" genoemd.

De Contractant heeft de verantwoordelijkheid, t.o.v. deKlant, om alle verplichtingen weerhouden in dit document te laten respecteren door de medewerkers van de Contractant. Hij engageert zich om aan zijn medewerkers dit document toe te lichten vóór zij gebruik maken van TIC materiaal en vraagt hen de richtlijnen van dit document te respecteren.

Art. 2
De ICT-apparatuur mag uitsluitend worden gebruikt met geïnstalleerde officiële software en hardware (ontwikkeld voor de Klant, onder licentie gekocht of gehuurd).

Elke installatie van een programma dat geen deel uitmaakt van het standaardpakket dat is geïnstalleerd op de door de Klant ter beschikking gestelde ICT-apparatuur (pc, pda, enz.) moet uitdrukkelijk worden aangevraagd bij de Information Security Manager (ISM) van de Klant.

Art. 3
Elke Gebruiker moet de nodige maatregelen nemen om te voorkomen dat de door de Klant ter beschikking gestelde ICT-apparatuur wordt gestolen. De Klant is verantwoordelijk voor de beveiliging van de apparatuur.

Art. 4
De Gebruiker moet de apparatuur gebruiken als een goede huisvader en het gebruik van de apparatuur mag de goede werking van het bedrijf van de Klant niet in gevaar brengen, noch schade toebrengen aan het imago en de reputatie van de Klant ten opzichte van derden.

Art. 5
De Klant kent een wachtwoord en een User ID toe aan elke Gebruiker. Het wachtwoord moet worden gevormd volgens de regels die zijn vastgelegd in het "Beleid inzake wachtwoorden", dat kan worden geraadpleegd op het intranet van de Klant.

Art. 6
Via de User ID kan de Gebruiker duidelijk worden geïdentificeerd door de computersystemen.

Het wachtwoord is persoonlijk en mag niet worden meegedeeld aan andere personen.

Art. 7
Elke Gebruiker die toegang heeft tot het computersysteem van de Klant, ongeacht de vorm ervan, is verantwoordelijk voor het gebruik dat hij maakt van dit systeem.

Art. 8
Wanneer de Gebruiker e-mails verzendt, moet hij elk bericht systematisch als volgt ondertekenen in naam van zijn werkgever/organisatie:

Voornaam en naam van de Gebruiker
Naam van de werkgever/organisatie van de Gebruiker, contractant van Klant

Bv:
Jan Dupont
Bullax nv, contractant van Electrabel

De Gebruiker mag geen e-mails verzenden in naam van een andere Gebruiker, behalve wanneer hij hiervoor de uitdrukkelijke toestemming van deze laatste heeft gekregen.

Het is formeel verboden om het wachtwoord en de User ID van een andere Gebruiker te gebruiken.

Het is verboden om af te wijken van deze regels zonder de voorafgaande schriftelijke toestemming van de bevoegde Information Security Manager (ISM) van de Klant.

Art. 9
De computerapplicaties mogen niet voor lange tijd onbewaakt worden gelaten zonder dat de toegang tot de applicaties is beveiligd (Control-Alt-Delete/Lock Computer).

Art. 10
De e-mails die binnen het bedrijf van de Klant worden verzonden, zijn vertrouwelijk en mogen niet worden doorgestuurd ("geforward") naar adressen buiten het bedrijf van de Klant of naar andere Gebruikers, behalve als deze informatie moet worden meegedeeld voor doeleinden die kaderen in de dienstverlening en de geadresseerde kan worden beschouwd als een gemachtigd persoon. Elke e-mail die vertrouwelijke informatie bevat, moet als vertrouwelijk worden gemarkeerd.

Het per e-mail verzenden van zeer vertrouwelijke berichten moet worden vermeden, behalve indien toereikende veiligheidsmaatregelen zijn genomen.

Art. 11
Inkomende e-mails worden systematisch gecontroleerd op de aanwezigheid van virussen. Elk bericht dat een virus bevat, wordt automatisch verwijderd. De verzender en de geadresseerde worden hiervan op de hoogte gebracht met een specifieke kennisgeving.

Art. 12
Onder aan de e-mails die naar adressen buiten het bedrijf van de Klant worden verzonden, moet een "disclaimer" worden toegevoegd. Deze disclaimer wordt automatisch toegevoegd aan alle uitgaande e-mails.

Art. 13
De Gebruiker mag geen e-mails automatisch laten doorsturen naar zijn privéadres (door activering van de functie "Inkomende berichten automatisch doorsturen"), ook niet in periodes van afwezigheid (vakantie, bijvoorbeeld). In dat laatste geval is het aangeraden dat hij gebruik maakt van een "Out of Office"-bericht, waarin hij de naam vermeldt van de medewerker van de Contractant die eventueel zijn taken tijdelijk overneemt tijdens zijn afwezigheid.

Art. 14
De Gebruikers kunnen niet aansprakelijk worden gesteld voor de berichten die zij ontvangen, voor zover zij niet zelf om deze berichten hebben gevraagd. Indien een Gebruiker evenwel meermaals berichten die

strijdig zijn met de bepalingen van dit document verzendt aan dezelfde persoon, neemt de betreffende Gebruiker geëigende maatregelen om een einde te stellen aan de verzending van deze berichten (door erover te spreken met de auteur van de berichten of door de Information Security Manager van de Klant op de hoogte te brengen) of hij licht zijn werkgever in, die dan samen met de Klant moet onderzoeken welke gepaste maatregelen kunnen worden genomen.

Art. 15
De Klant heeft software geïnstalleerd die de inhoud filtert van de websites waar de Gebruikers toegang toe willen nemen. Met deze filter kan de toegang worden geblokkeerd tot websites waarvan de inhoud illegaal, beledigend of ongepast wordt geacht. Aldus heeft de Klant de toegang geblokkeerd tot alle websites die tot bepaalde categorieën behoren, zoals pornografie, naakt, kansspelen, MP3, chatten of instant messaging. Als een Gebruiker toegang probeert te nemen tot een van deze websites, krijgt hij een bericht dat meldt dat de toegang is geblokkeerd en dat vermeldt tot welke categorie de website behoort.

Elk probleem in verband met de internetfilter – met name als een Gebruiker om professionele redenen toch toegang moet krijgen tot een website – dient te worden gemeld aan de Information Security Manager van de Klant.

Art. 16
Het is verboden om:

- vertrouwelijke informatie over de Klant, over een of meer Gebruikers, over de medewerkers van de Klant, over de klanten van de Klant of over derden te verspreiden, behalve indien het verspreiden van deze informatie verantwoord is om professionele redenen;
- te proberen toegang te krijgen tot e-mails van andere Gebruikers of van derden met de bedoeling ze te lezen;
- teksten, beelden of geluidsbanden te lezen/bekijken/beluisteren, te verzenden of te bewaren die racistisch, erotisch, pornografisch, seksueel of obsceen van aard zijn of een vergelijkbare inhoud bevatten, ongeacht de bron van deze teksten, beelden of geluidsbanden (bijvoorbeeld usb-poort, cd, dvd, enz.).

Art. 17
Het is eveneens verboden om berichten te verzenden naar grote groepen (> 100 mensen) zonder de uitdrukkelijke voorafgaande schriftelijke toestemming van de Information Security Manager van de Klant.

Art. 18
Het verzenden en ontvangen van lange berichten wordt automatisch beperkt om elk risico met betrekking tot de beschikbaarheid van het netwerk te voorkomen. Alle bijlagen van meer dan 25 MB die samen met inkomende of uitgaande e-mails worden verzonden en alle inkomende berichten die bijlagen met uitvoerbare bestanden bevatten, worden verwijderd. Gebruikers die regelmatig berichten moeten kunnen verzenden of ontvangen die groter zijn dan de vastgestelde limiet, dienen contact op te nemen met de IS Service Desk van de Klant.

Art. 19
Streaming is niet toegestaan, behalve tijdens de dienstverlening. Videoconferenties zijn toegestaan, alsook het bekijken of beluisteren van werkgerelateerde informatie. Het is verboden om te luisteren naar radio-uitzendingen of te kijken naar video's die geen verband houden met de diensten die worden verleend via de ICT-apparatuur.

Art. 20

De controleprocedure is er in hoofdzaak op gericht de privacy van de Gebruikers van de ICT-apparatuur te doen respecteren en vooraf regels vast te leggen die de Klant in acht moet nemen wanneer hij de elektronische communicatie (internet en e-mail) wenst te controleren.

Bij alle controles die worden uitgevoerd dient rekening te worden gehouden met de volgende principes:

- **Doeleinden**: dit document geeft een volledig overzicht van de doeleinden waarvoor een controle kan worden uitgevoerd.
- **Proportionaliteit**: de controle en de omvang ervan moeten in alle gevallen gepast, relevant en afgemeten zijn. Ze moeten bovendien in proportie zijn tot het beoogde doel of de beoogde doeleinden en steeds tot het minimum worden beperkt.
- **Transparantie**: dit document wordt meegedeeld om de Gebruikers te informeren over de rechten en plichten van alle partijen.

Art. 21
Alle controles worden uitgevoerd door het IS-departement, onder de verantwoordelijkheid van de dienst Human Resources van de Klant of van de Chief Security Officer van de Klant.

Art. 22
Bij de vaststelling van een inbreuk op de bepalingen van dit document, zal de Klant aan de Contractant, werkgever van de Gebruiker, alle informatie omtrent de inbreuken kunnen verstrekken en aan de Contractant kunnen vragen de nodige correctieve acties te nemen en eventueel met onmiddellijke ingang het gebruik van het TIC materiaal kunnen stopzetten voor de betrokken Gebruiker.

Art. 23
Elke niet-naleving van de bepalingen van dit document door een Gebruiker kan bovendien worden beschouwd als een contractuele fout van de Contractant, werkgever van de Gebruiker, in het kader van de uitvoering van het aannemingscontract.

Art. 24
Elke Gebruiker die een storing in de werking van het computersysteem vaststelt, moet dit melden aan de IS Service Desk of, in geval van veiligheidsproblemen, aan de Information Security Manager (ISM) van de Klant.