

**Collectieve arbeidsovereenkomst van de nv
ELECTRABEL van 1 juni 2007 met betrek-
king tot het gebruik van het TIC-Materiaal**

**Convention collective de travail de la s.a.
ELECTRABEL du 1^{er} juin 2007 relative à
l'utilisation du Matériel TIC**

Tussen enerzijds: Electrabel nv, vertegenwoordigd door Chan- tal Pont en Pierre Devillers; En anderzijds: ACV Elektriciteit en Gas, vertegenwoordigd door Chris Vanmol en ACV-CNE , verte- genwoordigd door Bruno Baudson; ABVV Gazelco, vertegenwoordigd door Jean-Claude Galler en Filip Baeckelandt; ACLVB, vertegenwoordigd door Valérie Vanhemelen.	Entre, d'une part ; Electrabel S A., représentée par Chantal Pont et Pierre Devillers ; Et, d'autre part ; La CSC gaz et électricité, représentée par Chris Vanmol et la CSC-CNE, représentée par Bruno Baudson ; La FGIB-Gazelco, représentée par Jean- Claude Galler et Filip Baeckelandt ; La CGSLB, représentée par Valérie Vanhe- melen.
Hoofdstuk 1. Inleiding	Chapitre 1. Introduction
Art. 1. Deze collectieve arbeidsovereenkomst (hier- na "CAO" genoemd) wordt afgesloten door Electrabel in toepassing van artikel 20 van de sectorale CAO van 30 november 2006 met betrekking tot het gebruik van Technologisch materiaal voor Informatie en Communicatie (hierna "TIC-Materiaal") en heeft tot doel, een gedragscode voor alle Gebruikers vast te leggen.	Art. 1. La présente convention collective de travail (ci-après « CCT ») est prise par Electrabel en application de l'article 20 de la CCT sectorielle du 30 novembre 2006 relative à l'utilisation du Matériel de technologie de l'Information et de la Communication (ci-après « Matériel TIC »). Elle a pour objet de déterminer la ligne de conduite pour tous les Utilisateurs.
Hoofdstuk 2. Toepassingsgebied	Chapitre 2. Champ d'application
Art. 2. Deze CAO is van toepassing op de werknemers die zijn aangeworven met een arbeidsovereenkomst.	Art. 2. La présente CCT est applicable aux travailleurs engagés sous contrat de travail.
Hoofdstuk 3. Eigendom van het TIC-Materiaal	Chapitre 3. Propriété du Matériel TIC
Art. 3. Het TIC-Materiaal mag uitsluitend worden gebruikt met officieel geïnstalleerde software en hardware (ontwikkeld voor de onderneming, aangekocht of gehuurd onder licentie). Elke installatie van een programma dat niet tot het standaardpakket behoort op het door Electrabel ter beschikking gestelde TIC-Materiaal (PC's, PDA's, enz.), moet uitdrukkelijk worden aangevraagd bij de Métier Information Security Manager (MISM). Art. 4. Elke Gebruiker moet de nodige voorzorgen	Art. 3. Le Matériel TIC ne peut tourner qu'avec des logiciels et matériels officiellement installés (développés pour l'entreprise, achetés ou loués sous licence). Toute installation d'un logiciel non standard sur du Matériel TIC fourni par Electrabel (PC, PDA, etc.) doit faire l'objet d'une demande expresse au Métier Information Security Manager (MISM). Art. 4. Chaque Utilisateur doit prendre les précau-

nemen ten einde te vermijden dat het TIC-materiaal, door de werkgever ter zijner beschikking gesteld, gestolen wordt. Deze laatste is verantwoordelijk voor de beveiligingsmiddelen van het informatica-materiaal.	tions nécessaires afin d'éviter le vol du matériel TIC mis à sa disposition par l'employeur. Ce dernier est responsable des moyens de protection du matériel informatique.
Hoofdstuk 4. Gebruik van het TIC-Materiaal voor Privé-doeleinden <i>Toepassing van artikel 7 van de sectorale CAO</i>	Chapitre 4. Usage à des Fins privées du Matériel TIC <i>Application de l'article 7 de la CCT sectorielle</i>
Art. 5. De beperking van het privégebruik van het TIC-Materiaal maakt deel uit van een algemene verplichting die uit de arbeidsovereenkomst voortvloeit, namelijk de verplichting om het werk met zorg, loyaliteit en nauwgezetheid uit te voeren, als een goede huisvader, met inachtneming van de regels inzake wellevendheid, de ethiek, de goede zeden.	Art. 5. La limitation de l'usage privé du Matériel TIC fait partie d'une obligation générale découlant du contrat de travail, à savoir l'obligation d'effectuer le travail avec soin, loyauté et précision, en bon père de famille, dans le respect du savoir-vivre, de l'éthique et des bonnes mœurs.
Art. 6. Het gebruik van het TIC-Materiaal voor Privé-doeleinden wordt aanvaard voor zover dit slechts bij uitzondering en in beperkte mate gebeurt en voor zover dit de goede gang van zaken in de onderneming en de correcte uitvoering van de taken van de Gebruiker niet belemmert. Het mag evenmin het imago en de reputatie van Electrabel tegenover derden schaden.	Art. 6. L'usage à des Fins privées du Matériel TIC est accepté pour autant que celui-ci reste exceptionnel, limité et qu'il n'entrave pas la bonne marche de l'entreprise et la bonne exécution du travail par l'Utilisateur. Il ne peut pas non plus porter atteinte à l'image et à la réputation d'Electrabel à l'égard des tiers.
4.1. Tijdens de gewone werkuren	4.1. Pendant les heures de service normales
Art. 7. Onder "gewone werkuren" moeten de uren worden verstaan die in toepassing van de arbeidsovereenkomst en het arbeidsreglement worden gepresteerd.	Art. 7. Par « heures de services normales », il faut entendre les heures prestées en application du contrat de travail et du règlement de travail.
Art. 8. Enkel in dringende en uitzonderlijke gevallen kan het gebruik voor Privé-doeleinden worden toegestaan tijdens de gewone werkuren. Het gebruik van het TIC-Materiaal voor Privé-doeleinden mag in geen geval de normale uitoefening van de functie verstoren en/of de goede werking van de dienst en de onderneming belemmeren.	Art. 8. Seule l'utilisation urgente et exceptionnelle à des Fins privées peut être admise pendant les heures de service normales. L'utilisation du Matériel TIC à des Fins privées ne peut en tout cas pas perturber l'exercice normal de la fonction et/ou remettre en cause le bon fonctionnement du service et de l'entreprise.
4.2. Buiten de gewone werkuren	4.2. En dehors des heures de service normales
Art. 9. Het gebruik van het TIC-Materiaal voor Privé-doeleinden is toegestaan tijdens de maaltijdpauze en buiten de gewone werkuren, voor zover dit binnen de grenzen van de redelijkheid gebeurt.	Art. 9. L'usage du Matériel TIC est autorisé à des Fins privées, pendant la pause de repas ou en dehors des heures de service normales, pour autant que cet usage reste raisonnable.
Art. 10. Wie de beschikking heeft over een draagbare PC van Electrabel en thuis een verbinding heeft, o.a. via ADSL of via de kabel, mag dit TIC-Materiaal buiten de normale kantooruren voor Privé-doeleinden gebruiken, op voorwaarde dat hij er als een goede huisvader gebruik van maakt, dat hij de	Art. 10. Les détenteurs d'un PC portable appartenant à Electrabel et d'un accès à domicile tels que l'ADSL ou le câble peuvent utiliser ce Matériel TIC à des Fins privées en dehors des heures normales de bureau pour autant qu'ils l'utilisent en bons pères de famille, qu'ils n'entravent pas le bon fonctionnement

goede werking van de onderneming niet in gevaar brengt en dat dit gebruik de reputatie van Electrabel tegenover derden niet schaadt.	de l'entreprise et que cette utilisation ne porte pas préjudice à la réputation d'Electrabel à l'égard des tiers.
4.3. Werkzaamheden buiten de kantoren van Electrabel tijdens de gewone werkuren	4.3. Travail en dehors des bureaux d'Electrabel pendant les heures de service normales
Art. 11. In het kader van thuiswerk, werk in open offices, externe opleidingen of externe vergaderingen blijven de bepalingen van deze CAO volledig van toepassing.	Art. 11. Dans le cadre du travail à domicile, du travail en open offices, des formations externes ou des réunions externes, les dispositions de la présente CCT restent entièrement d'application.
Hoofdstuk 5. Vertrouwelijkheid en beveiliging van Gegevens <i>Toepassing van artikel 9 van de sectorale CAO</i>	Chapitre 5. Confidentialité et sécurité des Données <i>Application de l'article 9 de la CCT sectorielle</i>
5.1. Toegang tot de informaticawerkpost van de Gebruiker	5.1. Accès au Poste de travail informatique de l'Utilisateur
5.1.1. Paswoord en login Art. 12. Electrabel kent aan elke Gebruiker een paswoord en een user-ID toe. Het paswoord moet worden gevormd volgens de regels die zijn vastgelegd in de "Policy inzake paswoorden" die op het intranet van de onderneming worden geraadpleegd. Electrabel zal alles in het werk stellen om ervoor te zorgen dat de nieuw aangeworvenen, binnen de kortste tijd, een paswoord en een user-ID ontvangen. Art. 13. Dankzij zijn user-ID kan de Gebruiker op eenduidige wijze worden geïdentificeerd door de informaticasystemen. Het paswoord is persoonlijk en mag niet aan andere personen meegegeed worden. Art. 14. Elke Gebruiker die toegang heeft tot het informaticasysteem van de onderneming, ongeacht onder welke vorm, is verantwoordelijk voor het gebruik dat hij van dit systeem maakt conform deze CAO.	5.1.1. Mot de passe et login Art. 12. Electrabel octroie à chaque Utilisateur un mot de passe et un user-ID. Le mot de passe doit être formé selon les règles définies dans la « <i>Politique en Matière de Mots de Passe</i> », publié sur l'intranet de l'entreprise. Electrabel mettra tout en œuvre en vue de mettre à la disposition des nouveaux engagés un mot de passe et un user-ID et ce, dans les meilleurs délais. Art. 13. Le user-ID permet d'identifier l'Utilisateur dans les systèmes informatiques de façon unique. Le mot de passe est donc personnel et ne peut être communiqué à d'autres personnes. Art. 14. Chaque Utilisateur qui a accès au système informatique de l'entreprise, sous quelque forme que ce soit, est responsable de l'usage qu'il fait de ce système conformément à la présente CCT.
5.1.2. Persoonlijk gebruik	5.1.2. Usage personnel
Art. 15. Het is de Gebruiker niet toegestaan om e-mailberichten te versturen in naam van een andere Gebruiker, uitgezonderd met diens uitdrukkelijke toestemming. Het is ten strengste verboden om gebruik te maken van het paswoord en de login van een andere Gebruiker.	Art. 15. Il est interdit à l'Utilisateur d'envoyer des courriers électroniques au nom d'un autre Utilisateur, sauf autorisation expresse de celui-ci. Il est strictement interdit d'utiliser le mot de passe et le login d'un autre Utilisateur.

Er kan niet worden afgeweken van deze regels zonder de voorafgaande schriftelijke toestemming van de bevoegde Métier Information Security Manager (MISM). 5.1.3. Tijdens afwezigheidsperiodes Art. 16. Teneinde de continuïteit van de dienst te verzekeren en voor zover dit nodig is en in de mate van het mogelijke, dient de Gebruiker er tijdens zijn geplande afwezigheden voor te zorgen dat: - zijn vervanger(s) toegang heeft (hebben) tot de nodige bestanden; - de "out of office"- functie in Outlook is geactiveerd om zijn afwezigheid te melden en/of de berichten door te sturen naar zijn vervanger(s). Deze bepaling mag geenszins de uitvoering van de syndicale activiteit belemmeren. Art. 17. De informaticawerkposten mogen niet voor een langdurig tijdspanne verlaten worden zonder dat de toegang tot de applicaties is beschermd (Control-Alt-Delete / Lock computer).	Il ne peut être dérogé à ces règles sans avoir obtenu l'accord préalable écrit du Métier Information Security Manager (MISM) compétent 5.1.3. Pendant les périodes d'absence Art. 16. En vue d'assurer la continuité du service et lorsque cela s'avère nécessaire et dans la mesure du possible, l'Utilisateur doit, durant ses absences prévues, s'assurer : - de donner accès à son (ses) remplaçant(s), aux fichiers nécessaires ; - d'activer la fonctionnalité « out of office » dans Outlook, pour avertir de son absence et/ou de rediriger les messages vers son (ses) remplaçant(s). Cette disposition ne peut toutefois pas entraver l'exercice de l'activité syndicale. Art. 17. Les postes de travail informatiques ne peuvent être abandonnés de manière prolongée sans que les accès aux applications soient protégés (Control-Alt-Delete / Lock computer).
5.2. E-mailberichten & Webfilter	5.2. Messages électroniques & Webfilter
5.2.1. E-mailberichten Art. 18. E-mailberichten die binnen de onderneming worden verstuurd, zijn vertrouwelijk en mogen niet worden doorgestuurd ('forwarded') naar adressen buiten de onderneming of naar andere Gebruikers, uitgezonderd indien zij voor Beroepsdoeleinden moeten worden meegedeeld en de bestemming kan worden omschreven als een bevoegd persoon. Wanneer een bericht vertrouwelijke informatie bevat, moet het als dusdanig worden aangeduid. Het versturen van zeer vertrouwelijke berichten via e-mail moet worden vermeden, tenzij wanneer er afdoende veiligheidsmaatregelen zijn getroffen. Hetzelfde geldt voor berichten die Electrabel verbinden en waarvoor een brief, een overeenkomst of een traditionele bestelbon de voorkeur moeten krijgen, met inachtneming van de ondertekeningsbevoegdheden. Art. 19. De binnenkomende e-mailberichten worden systematisch gecontroleerd op virussen. Een bericht dat een virus bevat, wordt automatisch verwijderd. De afzender en de bestemming worden hiervan op de hoogte gebracht door middel van een specifieke melding.	5.2.1. Messages Electroniques Art. 18. Les messages électroniques envoyés au sein de l'entreprise sont confidentiels et ne peuvent être envoyés ('forwardés') hors de l'entreprise ou à d'autres Utilisateurs à moins qu'ils ne doivent être communiqués à des Fins professionnelles et que le destinataire puisse être qualifié de personne compétente. Lorsqu'un message contient des informations confidentielles, celles-ci doivent être indiquées comme telles. L'envoi de messages hautement confidentiels par voie électronique doit être évité, sauf si les mesures adéquates de sécurité ont été prises. Il en est de même de messages engageant Electrabel et pour lesquels un courrier, un contrat ou un bon de commande traditionnel doit être préféré, en respect des pouvoirs de signature. Art. 19. Les messages électroniques entrants sont systématiquement analysés à la recherche de virus. Un message contenant un virus est automatiquement éliminé; l'émetteur et le destinataire en sont avertis par un message spécifique.

Art. 20. Onderaan de e-mailberichten die naar adressen buiten de onderneming worden verstuurd, moet er een “disclaimer” worden toegevoegd, welke automatisch toegevoegd bij alle uitgaande e-mails.

Art. 21. Het is de Gebruiker niet toegestaan om e-mails automatisch naar zijn privé-adres door te sturen (met name door de automatische forward-functie voor inkomende e-mails te activeren), zelfs niet tijdens afwezigheidsperiodes (bv. vakanties, arbeidsongeschiktheid, enz.). In dit laatste geval wordt hem aangeraden om, conform de bepalingen die zijn opgenomen in hoofdstuk 5.1.3., gebruik te maken van een ‘Out of Office’-bericht waarin hij de naam vermeldt van de persoon binnen de onderneming die in zijn afwezigheid tijdelijk zijn taken waarneemt.

Art. 22. Wanneer een Gebruiker thuis Gegevens van Electrabel moet raadplegen, kan hij gebruik maken van de “remote access” (toegang op afstand) die door Electrabel ter beschikking worden gesteld.

Art. 23. De Gebruikers kunnen niet aansprakelijk worden gesteld voor de berichten die zij ontvangen voor zover zij deze berichten niet hebben gevraagd. Indien een Gebruiker evenwel verscheidene keren naar eenzelfde collega berichten zou hebben verstuurd die in strijd zijn met deze CAO, dient deze collega passende maatregelen te treffen om een einde te stellen aan het versturen van deze berichten (hetzij door de zaak uit te klaren met de auteur van de berichten, hetzij door ITS Security op de hoogte te brengen), hetzij door de procedure met betrekking tot geweld of pesterij op het werk op te starten.

5.2.2. Webfilter

Toepassing van artikel 12 van de sectorale CAO

Art. 24. Electrabel heeft een software geïnstalleerd die de inhoud filtert van de internetsites waartoe de Gebruikers zich toegang willen verschaffen. Dankzij deze filter wordt de toegang tot internetsites waarvan de inhoud onwettig, beledigend of ongepast wordt geacht, geblokkeerd. Op die manier heeft Electrabel de toegang geblokkeerd tot alle sites die tot bepaalde categorieën behoren, o.a. Pornografie, Naakt, Onlinespelletjes, MP3, Chat of Instant messenger. Wanneer een Gebruiker tracht toegang te krijgen tot één van deze sites, ontvangt hij een bericht met de boodschap dat de toegang wordt geblokkeerd, met vermelding van de categorie waartoe de site behoort.

Elk probleem in verband met de webfilter – met name wanneer een Gebruiker om professionele redenen toch toegang moet krijgen tot een geblokkeerde site – moet worden gemeld aan de ITS Service Desk.

Art. 20. L’addition d’une garantie « disclaimer » à la fin des messages e-mail envoyés hors de l’entreprise est obligatoire ; elle est jointe automatiquement à tous les e-mails sortants.

Art. 21. L’Utilisateur n’est pas autorisé à envoyer automatiquement des e-mails à son adresse privée (notamment en activant un “forward” automatique des e-mails entrants), même pendant ses périodes d’absence (ex. vacances, incapacité de travail, etc.). Dans cette dernière hypothèse, il lui est recommandé, conformément à ce qui est prévu au chapitre 5.1.3., d’utiliser un message “Out of Office” mentionnant qui dans l’organisation assume temporairement ses tâches en son absence.

Art. 22. Lorsqu’un Utilisateur doit consulter des Données d’Electrabel à partir de son domicile, il peut utiliser les services “remote access” (accès à distance) fournis par Electrabel.

Art. 23. Les Utilisateurs ne pourront pas être tenus responsables des messages qu’ils reçoivent pour autant que ces messages n’aient pas été sollicités. En revanche, dans l’hypothèse où des messages, en contravention avec la présente CCT, seraient envoyés à plusieurs reprises par un Utilisateur à un même collègue, ce dernier est tenu de prendre les mesures appropriées afin que l’envoi de ces messages prenne fin (soit en mettant les choses au clair avec l’auteur des messages, soit en informant ITS Security), soit en déclenchant la procédure pour harcèlement ou pour violence au travail.

5.2.2. Webfilter

Application de l’article 12 de la CCT sectorielle

Art. 24. Electrabel a placé un software filtrant le contenu des sites internet auxquels les Utilisateurs souhaitent accéder. Grâce à ce filtre, l’accès aux sites internet dont le contenu est considéré comme illégal, offensif ou inapproprié est bloqué. Electrabel a ainsi bloqué l’accès à tous les sites appartenant à certaines catégories tels que Pornographie, Nudité, Jeux en ligne, MP3, Chat ou Messagerie instantanée. Lorsqu’un Utilisateur tentera d’accéder à un de ces sites, il recevra un message lui indiquant que l’accès est bloqué ainsi que la catégorie à laquelle ce site appartient.

Tout problème concernant le webfilter, notamment lorsqu’un Utilisateur doit accéder, pour des raisons professionnelles, à un site bloqué, doit être adressé au ITS Service Desk

5.3. Goede werking van het TIC-Materiaal	5.3. Bon fonctionnement du matériel TIC
Art. 25. In toepassing van artikel 10 alinea 2 van de sectorale CAO, moet men onder “dienst informatica” verstaan: de Métier Information Security Manager (MISM) of rechtstreeks met Information Security Governance via de brievenbus SOSSecurity. Art. 26. Het is verboden: - De verspreiding van vertrouwelijke informatie in verband met de onderneming, één of meer Gebruikers, klanten of derden, uitgezonderd indien dit naar behoren wordt gerechtvaardigd door redenen van professionele aard; - Pogingen om zich toegang te verschaffen tot de e-mailberichten van andere Gebruikers of derden, of om deze te lezen; - Het bekijken, doorsturen of bewaren van teksten, beelden of klankbanden met racistische, erotische, pornografische, seksuele, obscene of daarmee vergelijkbare inhoud, ongeacht de herkomst van deze teksten, beelden of klankbanden (bv: USB-poort, CD, DVD, enz.). Art. 27. Onverminderd de afwijkingen die worden toegestaan door bijlage 1 van de sectorale CAO aan de leden van de vakbondsorganisaties, is het eveneens verboden om berichten te versturen aan grote groepen personeelsleden (>100 personen) zonder de uitdrukkelijke voorafgaande en schriftelijke toestemming van de HR-verantwoordelijke of de verantwoordelijke Interne Communicatie van de onderneming, de entiteit of de métier. Het kan daarbij gaan om berichten van professionele aard (dienstmededelingen, algemene informatie, uitnodigingen voor vergaderingen, informatiebrochures) of van niet-professionele aard (vriendenkring, overlijdensbericht, informatie over wegwerkzaamheden, ...). Art. 28. Om de beschikbaarheid van het netwerk niet in gevaar te brengen, wordt het versturen en ontvangen van grote berichten automatisch beperkt. Elke bijlage bij een inkomend of uitgaand e-mailbericht dat via het internet wordt verstuurd van meer dan 25MB, en alle inkomende berichten met in de bijlage uitvoerbare bestanden worden verwijderd. Indien een Gebruiker regelmatig berichten moet kunnen versturen of ontvangen waarvan de grootte de opgegeven limiet overschrijdt, dient hij contact op te nemen met de ITS Service Desk. Art. 29. Continue verspreiding (streaming) is niet	Art. 25. En application de l'article 10, alinéa 2 de la CCT sectorielle, il faut entendre par « service informatique »: le Métier Information Security Manager (MISM) ou bien directement l'Information Security Governance, via la boîte aux lettres SOSSecurity. Art. 26. Sont interdits : - La dispersion d'informations confidentielles relatives à l'entreprise, à un ou plusieurs Utilisateurs, clients ou tiers, sauf si cette diffusion est dûment justifiée par des motifs à caractère professionnel ; - Les tentatives d'accéder, ou de lire, les messages électroniques d'autres Utilisateurs ou tiers ; - La visualisation, la transmission ou la sauvegarde de textes, d'images ou de bandes sonores à caractère raciste, érotique, pornographique, sexuel, obscène ou de nature similaire, quelle que soit l'origine de ces textes, images ou bandes sonores (ex : Port USB, CD, DVD, etc.). Art. 27. Sans préjudice des dérogations accordées aux membres des organisations syndicales par l'annexe 1 de la CCT sectorielle, est également interdit l'envoi de messages à des grands groupes de personnel (>100 personnes) sans autorisation expresse écrite et préalable du responsable des Ressources Humaines ou du responsable de la Communication Interne de l'entreprise, l'entité ou du métier. Il peut s'agir ici tant de messages professionnels (communications de service, informations générales, invitations à des réunions, brochures d'information) que de messages non professionnels (cercle d'amis, communication personnelle d'un décès, information sur des travaux routiers, ...). Art. 28. Pour ne pas mettre en péril la disponibilité du réseau, l'envoi et la réception de messages volumineux seront automatiquement limités. Toute annexe d'un message électronique entrant et sortant de l'Internet dépassant 25MB ainsi que toutes les annexes entrantes exécutables seront supprimées. Si l'Utilisateur a régulièrement besoin d'envoyer ou recevoir des messages dont la taille dépasse la limite déterminée il devra prendre contact avec le ITS Service Desk. Art. 29. La diffusion en continu (streaming) n'est

toegestaan, uitgezonderd tijdens de uitoefening van een functie. Videoconferenties zijn toegestaan, net als het projecteren of beluisteren van professionele informatie. Het beluisteren van radiozenders of het bekijken van video's op het TIC-Materiaal zonder dat er enig verband is met de professionele activiteit, is niet toegestaan.	pas autorisée, sauf dans l'exercice de la fonction. La visioconférence est autorisée, tout comme la projection ou l'écoute d'informations professionnelles. Ecouter la radio ou visionner des vidéos sur le Matériel TIC sans relation avec l'activité professionnelle n'est pas autorisé.
Hoofdstuk 6. Controle	Chapitre 6. Contrôle
6.1. Principes <i>Toepassing van hoofdstuk VI van de sectorale CAO</i>	6.1. Principes <i>Application du chapitre VI de la CCT sectorielle</i>
Art. 30. De controleprocedure is in hoofdzaak bedoeld om ervoor te zorgen dat de persoonlijke levenssfeer van de Gebruikers van het TIC-Materiaal wordt geëerbiedigd en om voorafgaandelijk regels vast te leggen die door de directie van Electrabel in acht moeten worden genomen indien zij een controle wenst uit te voeren op het elektronisch communicatieverkeer (internet en e-mail). Alle controles worden uitgevoerd met inachtneming van de volgende principes: - Doelstellingen: Deze CAO somt op exhaustieve wijze de doelstellingen op waarvoor er een controle kan worden georganiseerd. - Proportionaliteit: de controle en de omvang ervan moeten in alle gevallen passend, pertinent en niet overdreven zijn en moet in verhouding staan met de doelstelling of de doelstellingen die ermee worden nagestreefd; maar blijft altijd beperkt tot het minimum. - Transparantie: de goedkeuring van deze CAO heeft tot doel om de Gebruikers te informeren over de rechten en plichten van elk van de partijen. De werkgever informeert de werknemer regelmatig over de inhoud van deze CAO.	Art. 30. Le principal objectif de la procédure de contrôle est de garantir le respect de la vie privée des Utilisateurs du Matériel TIC et de prévoir préalablement des règles devant être respectées par le management d'Electrabel s'il souhaite exercer un contrôle sur les communications électroniques (internet et e-mail). Chaque contrôle s'effectuera dans le respect des principes suivants : - Finalité: la présente CCT énumère de manière exhaustive les finalités dans le cadre desquelles un contrôle peut être organisé. - Proportionnalité: le contrôle et l'ampleur de celui-ci devra revêtir dans tous les cas un caractère adéquat, pertinent et non excessif au regard de la ou des finalités qu'il poursuit mais restera toujours limitée à un minimum. - Transparence: l'adoption de la présente CCT a pour objet d'informer les Utilisateurs des droits et obligations de chacune des parties. L'employeur informera les travailleurs du contenu de la présente CCT de manière régulière.
6.2. Regels voor de globale controle van het elektronisch communicatieverkeer	6.2. Modalités de contrôle global des communications électroniques
Art. 31. Alle controles vermeld in artikels 13 en 14 van de sectorale CAO worden uitgevoerd onder de verantwoordelijkheid van de dienst Information Security Governance van Electrabel. Er kan door de hiërarchie een aanvraag tot controle worden aangevraagd aan de Métier Information Security Managers (MISM) die op hun beurt en na evaluatie en overleg met de Chief Security Officer (in samenwerking met de Social Relations Manager), de opdracht kunnen geven om een controle uit te voeren. Alle controles worden steeds uitgevoerd onder	Art. 31. Tous les contrôles visés aux articles 13 et 14 de la CCT sectorielle se font sous la responsabilité du service Information Security Governance d'Electrabel. Une demande de contrôle peut être demandé par la hiérarchie aux Métier Information Security Managers (MISM) qui, à leur tour et après évaluation et consultation du Chief Security Officer (en collaboration avec le Social Relations Manager), peuvent donner l'ordre de contrôle. Tous les contrôles se font toujours sous la responsabilité du service Informa-

de verantwoordelijkheid van de dienst Information Security Governance. De leden van het ITS Security-team worden belast met de technische uitvoering van de controles. Ze kunnen echter nooit op eigen initiatief controles uitvoeren en zijn in ieder geval gebonden door het beroepsgeheim. De informatie die tijdens dergelijke controles wordt verkregen, wordt verwerkt door de Métier Information Security Manager (MISM), zodat deze een coherent antwoord kan formuleren op het oorspronkelijke probleem dat aanleiding had gegeven tot de controle. Information Security Governance en ITS Security worden ook gecontroleerd door een onafhankelijke, interne (audit) of externe instantie. Alle vragen in verband met de controles die door Electrabel worden uitgevoerd, moeten worden gericht aan de dienst Information Security Governance van Electrabel	tion Security Governance. Les membres de l'équipe ITS Security se chargeront de l'exécution technique des contrôles. Ils ne peuvent cependant jamais effectuer de contrôles de leur propre initiative et sont en tout cas liés par le secret professionnel. L'information obtenue lors de ces contrôles est traitée par le Métier Information Security Manager (MISM) de sorte que celui-ci puisse formuler une réponse cohérente à la problématique initiale qui a donné lieu au contrôle. Information Security Governance et ITS Security seront également contrôlés par une instance indépendante, interne (audit) ou externe. Toutes les questions relatives aux contrôles mis en place par Electrabel doivent être adressées au service Information Security Governance d'Electrabel.
6.3. Regels voor de individualisering van de globale controle van het elektronisch communicatieverkeer	6.3. Modalités d'individualisation du contrôle des communications électroniques
Art. 32. De individualisering van de controle van het elektronisch communicatieverkeer, vermeld in artikel 15 van de sectorale CAO, gebeurt onder de verantwoordelijkheid van de Chief Security Officer.	Art. 32. L'individualisation du contrôle des communications électroniques en réseau visée à l'article 15 de la CCT sectorielle se fait sous la responsabilité du Chief Security Officer
Hoofdstuk 7. Sancties	Chapitre 7. Sanctions
Art. 33. Electrabel kan bij de vaststelling van een inbreuk op de bepalingen van deze CAO één van de sancties opleggen die in de geldende arbeidsreglementen zijn vastgelegd en conform de hierin vastgelegde bepalingen.	Art. 33. En cas de constatation d'une infraction à la présente CCT, Electrabel pourra appliquer une des sanctions prévues par les règlements de travail en vigueur et conformément aux dispositions de ceux-ci.
Hoofdstuk 8. Diverse bepalingen	Chapitre 8. Dispositions diverses
Art. 34. Elke Gebruiker die een anomalie in het functioneren van het informaticasysteem zou vaststellen, dient dit te melden aan zijn Métier Information Security Manager (MISM) of rechtstreeks aan Information Security Governance via de brievenbus SOSSecurity. Art. 35. Elke afwijking van de bepalingen van deze CAO moet schriftelijk worden aangevraagd bij de ITS Service Desk of de MISM. Deze laatsten dienen hun toestemming schriftelijk te verlenen. De betrokken Gebruikers zijn verplicht om deze schriftelijke	Art. 34. Tout Utilisateur qui constaterait une anomalie dans le fonctionnement du système informatique doit le signaler à son Métier Information Security Manager (MISM) ou bien directement à l'Information Security Governance, via la boîte aux lettres SOSSecurity. Art. 35. Toute dérogation à la présente CCT doit être demandée par écrit au ITS Service Desk ou au MISM. Les autorisations accordées par ces derniers doivent également être données par écrit et être conservées par les Utilisateurs concernés.

toestemming te bewaren.	
Hoofdstuk 9. Inwerkingtreding en geldigheidsduur	Chapitre 9. Entrée en vigueur et durée de validité
Art. 36. Deze CAO treedt in werking op 1 juni 2007. Art. 37. Hij werd afgesloten voor een bepaalde duur van 1 jaar te rekenen vanaf de handtekening. Na evaluatie en unaniem akkoord wordt deze CAO van onbepaalde duur welke echter kan opgezegd worden door een aangetekend schrijven gericht aan de verantwoordelijke HR met een opzegperiode van 3 maanden.	Art. 36. La présente CCT entre en vigueur le 1^{er} juin 2007. Art. 37. Elle est conclue pour une durée déterminée de 1 an à dater de la signature. Après évaluation et accord unanime, cette CCT devient à durée indéterminée, elle peut toutefois être dénoncée par lettre recommandée adressée au responsable RH avec un préavis de 3 mois

Voor Electrabel N.V. / Pour Electrabel S.A.

Chantal Pont

Pierre Devillers

Voor ACV gas en elektriciteit / Pour la CSC gaz et électricité

Chris Vanmol

Voor ACV – CNE / Pour la CSC – CNE

Bruno Baudson

Voor AVBB-Gazelco / Pour la FGTB-Gazelco

Jean-Claude Galler

Filip Baeckelandt

Voor ACL VB / Pour la CGSLB

Valérie Vanhemelen
