Règles régissant l'utilisation du matériel Technologique d'Information et de Communication (TIC) par les contractants

Art. 1
Le présent document s'applique aux personnes se voyant confier, dans le cadre de l'exécution d'un contrat d'entreprise de services ou de travaux entre (i) Electrabel s.a. Client ou une autre société du groupe ENGIE (désigné «le Client» dans la suite du document) et (ii) un contractant (désigné « Contractant » dans la suite du document), du matériel Technologique d'Information et de Communication (désigné «matériel TIC» dans la suite du document) par le Client. Ces personnes sont désignées «Usagers» ci-après.

Le Contractant est responsable envers le Client, du respect des obligations reprises dans ce document par son personnel. Il s'engage à porter ce document à la connaissance de son personnel avant toute utilisation du matériel TIC du Client et à en demander le respect.

Art.2
Le matériel TIC doit être exclusivement utilisé avec des logiciels et du matériel informatiques officiels installés (développés pour le Client, achetés ou loués sous licence).

Toute installation d'un programme ne faisant pas partie du paquet standard sur le matériel TIC mis à disposition par le Client (PC, PDA, etc.) doit être expressément demandée auprès de l'Information Security Manager (ISM) du Client.

Art. 3
Chaque utilisateur doit prendre les mesures requises pour éviter le vol du matériel TIC mis à sa disposition par le Client. Ce dernier est responsable des dispositifs de protection du matériel informatique.

Art. 4
L'Usager doit l'utiliser en bon père de famille et son utilisation ne peut mettre en danger le bon fonctionnement de l'entreprise du Client ni porter atteinte à l'image et à la réputation du Client à l'égard de tiers.

Art. 5
Le Client attribue un mot de passe et un user ID à chaque Usager. Le mot de passe doit être formé suivant les règles définies dans la «Politique en matière de mot de passe» accessible en consultation sur l'intranet du Client.

Art. 6
Le user ID permet à l'Usager d'être clairement identifié par les systèmes informatiques.

Le mot de passe est personnel et ne peut être communiqué à d'autres personnes.

Art. 7
Tout Usager ayant accès au système informatique du Client, quelle que soit sa forme, est responsable de l'utilisation qu'il fait de ce système.

Art. 8
L'Usager doit, lorsqu'il envoie des e-mails, systématiquement signer le message au nom de son employeur/de son organisation, et ce de la manière suivante:

Prénom et nom de l'Usager
Nom de l'organisation/de l'employeur de l'Usager, contractant du Client

p.e. :
Jacques Dupont
Bullax s.a., contractant d'Electrabel n.v.

L'Usager n'est pas autorisé à envoyer des e-mails au nom d'un autre Usager, sauf s'il dispose de l'autorisation expresse de ce dernier.

Il est formellement interdit d'utiliser le mot de passe et le login d'un autre Usager.

Il est interdit de déroger à ces règles sans l'autorisation écrite préalable de l'Information Security Manager (ISM) compétent du Client.

Art. 9
Les applications informatiques ne peuvent être laissées sans surveillance pendant une période prolongée sans protection de l'accès aux applications (Control-Alt-Delete / Lock computer).

Art.10
Les e-mails envoyés au sein de l'entreprise du Client sont confidentiels et ne peuvent être réexpédiés («forwardés») vers des adresses externes à l'entreprise du Client ou vers d'autres Usagers, sauf s'ils doivent être communiqués à des fins relevant de la prestation de services et que le destinataire peut être considéré comme personne habilitée. Tout mail contenant des informations confidentielles doit être désigné comme tel.

L'envoi de messages très confidentiels par e-mail est à éviter, sauf lorsque des mesures de sécurité suffisantes ont été prises.

Art. 11
Les e-mails entrants sont systématiquement contrôlés quant à la présence de virus. Tout message contenant un virus sera automatiquement éliminé. L'expéditeur et le destinataire en seront informés par le biais d'une notification spécifique.

Art. 12
Un «disclaimer» doit être ajouté au bas des e-mails envoyés vers des adresses externes à l'entreprise du Client. Ce disclaimer sera automatiquement ajouté à tous les e-mails sortants.

Art. 13
L'Usager n'est pas autorisé à faire suivre automatiquement des e-mails vers son adresse privée (notamment en activant la fonction de réacheminement automatique des e-mails entrants), et ce même pendant les périodes d'absence (congés, par exemple). Il lui est conseillé dans ce dernier cas d'utiliser un message «Out of Office» dans lequel il indiquera le nom de la personne du Contractant effectuant provisoirement ses tâches pendant son absence, le cas échéant.

Art. 14
La responsabilité des Usagers ne peut être engagée pour des messages qu'ils reçoivent pour autant qu'ils n'aient pas sollicité ces messages. Si toutefois un Usager envoie des messages contraires au présent

document à une même personne à plusieurs reprises, l'Usager concerné doit prendre des mesures adéquates pour mettre un terme à l'envoi de ces messages (soit en procédant à une mise au point avec l'auteur des messages, soit en informant l'Information Security Manager du Client) ou en informer l'employeur, lequel devra ensuite examiner les mesures appropriées avec le Client.

Art. 15
Le Client a installé un logiciel filtrant le contenu des sites internet auxquels les Usagers souhaitent accéder. Ce filtre permet de bloquer l'accès aux sites internet dont le contenu est jugé illégal, offensant ou inapproprié. Le Client a, de cette manière, bloqué l'accès à tous les sites relevant de certaines catégories telles que pornographie, nudité, jeux en ligne, MP3, chat ou messagerie instantanée. Lorsqu'un Usager tente d'accéder à l'un de ces sites, il reçoit un message lui signalant que l'accès est bloqué, avec mention de la catégorie à laquelle appartient le site.

Tout problème relatif au filtre internet – à savoir lorsqu'un Usager doit tout de même accéder à un site internet pour des raisons professionnelles – doit être signalé à l'Information Security Manager du Client.

Art. 16
Il est interdit:

- De diffuser des informations confidentielles concernant le Client, un ou plusieurs Usagers, les collaborateurs du Client, les clients du Client ou des tiers, sauf si la diffusion de ces informations est dûment justifiée par des raisons de nature professionnelle;
- De tenter d'accéder aux e-mails d'autres Usagers ou de tiers pour les lire;
- De consulter, d'envoyer ou de conserver des textes, des images ou des bandes sonores à caractère raciste, érotique, pornographique, sexuel, obscène ou présentant un contenu comparable, quelle que soit l'origine de ces textes, de ces images ou de ces bandes sonores (par exemple port USB, CD, DVD, etc.).

Art. 17
Il est également interdit d'envoyer des messages à des groupes importants (> 100 personnes) sans l'autorisation expresse écrite préalable de l'Information Security Manager du Client.

Art. 18
L'envoi et la réception de messages longs sont automatiquement limités afin d'éviter tout risque pour la disponibilité du réseau. Toute annexe accompagnant un e-mail entrant ou sortant envoyé via l'internet de plus de 25 MB et tous les messages entrants contenant des fichiers exécutables en annexe seront supprimés. Les Usagers devant pouvoir régulièrement envoyer ou réceptionner des messages dont la taille dépasse la limite indiquée doivent contacter l'IS Service Desk du Client.

Art. 19
La diffusion continue (streaming) n'est pas autorisée, sauf pendant la prestation des services. Les vidéoconférences sont autorisées, de même que la projection ou l'écoute d'informations professionnelles. L'écoute de stations de radio ou la consultation de vidéos sans rapport avec les services fournis sur le matériel TIC sont interdites.

Art. 20
La procédure de contrôle vise essentiellement à faire respecter la vie privée des Usagers du matériel TIC et à définir préalablement des règles à prendre en considération par le Client lorsque celui-ci souhaite contrôler les communications électroniques (internet et e-mail).

Tous les contrôles seront effectués en tenant compte des principes suivants:

- **Objectifs**: le présent document résume de manière exhaustive les objectifs pour lesquels un contrôle peut être organisé.
- **Proportionnalité**: le contrôle et sa portée doivent être appropriés, pertinents et mesurés dans tous les cas. Ils doivent en outre être proportionnels à l'objectif ou aux objectifs visés, mais doivent toujours rester limités au minimum.
- **Transparence**: la communication du présent document a pour objectif d'informer les Usagers au sujet des droits et des obligations de chacune des parties.

Art. 21
Tous les contrôles seront effectués par le département IS, sous la responsabilité du service Ressources humaines du Client ou du Chief Security Officer du Client.

Art. 22
En cas de constatation d'une infraction aux dispositions du présent document, le Client communiquera au Contractant, employeur de l'Usager toutes les informations requises concernant les infractions et pourra demander de prendre des mesures correctives ou, le cas échéant, pourra refuser avec effet immédiat, toute utilisation du matériel TIC par l'Usager concerné.

Art. 23
Le non-respect des dispositions du présent document par un Usager peut en outre être considéré comme une faute contractuelle du Contractant, employeur de l'Usager dans le cadre de l'exécution du contrat d'entreprise.

Art. 24
Tout Usager qui constaterait une anomalie au niveau du fonctionnement du système informatique est tenu de le signaler à l'IS Service Desk ou, en cas de problèmes de sécurité, à l'Information Security Manager (ISM) du Client.