Règlement sur l'utilisation des outils informatiques

§ 1 Domaine d'application

- Tous les utilisateurs de l'infrastructure IT

§ 2 Bases légales

- Les directives de sécurité sur la protection des données conformément à la «Loi fédérale sur la protection des données» (LPD) doivent être respectées lors de l'utilisation d'outils informatiques.

§ 3 Installation et configuration des outils informatiques

- Les outils informatiques sont installés et entretenus par la division IT conformément à ses directives et normes.
- L'installation de matériel et/ou logiciel privé est en principe interdite. Dans des cas particuliers, l'approbation formelle du chef de la division IT est nécessaire.

§ 4 Utilisation professionnelle des outils informatiques

- Tous les appareils informatiques (p. ex. PC, portables) et leurs applications doivent être utilisés dans des buts professionnels, c'est-à-dire pour l'accomplissement des tâches professionnelles attribuées.
- Les chefs de division peuvent approuver l'utilisation de matériels informatiques hors du poste de travail en cas de nécessité professionnelle. Ils assument la responsabilité d'une mise au courant complète et correcte des collaborateurs.

§ 5 Processus d'utilisation des outils informatiques

- Les collaborateurs reçoivent le présent règlement lors de la première utilisation d'outils informatiques et confirment, par leur signature, avoir pris connaissance de son contenu et leur intention de le respecter.
- Ensuite, un login personnel nécessaire à l'accès au réseau ainsi qu'au courrier électronique et (si nécessaire) à l'Internet est créé pour chaque collaborateur.

§ 6 Utilisation de l'identifiant de l'utilisateur et des mots de passe

- Les identifiants personnels et les mots de passe correspondants ne doivent pas être transmis à des tiers.
- Les collaborateurs sont responsables de l'utilisation des dispositifs et mesures de contrôle d'accès existants (p. ex. mots de passe, choix, structure et conservation des mots de passe, etc.).

§ 7 Internet

- Tous les appareils connectés au réseau de l'entreprise doivent avoir recours exclusivement à l'accès Internet central proposé.
- Il n'existe aucun droit juridique à l'accès Internet. La direction se réserve le droit de bloquer et filtrer les informations/publications aux contenus inadaptés (p. ex. contenus pornographiques, à discrimination raciale, contraires aux règles de l'éthique, immoraux) ou comportant des risques discernables pour l'entreprise (risque de virus).

§ 8 Courrier électronique

- Les courriers électroniques doivent être utilisés de préférence afin d'accélérer et de simplifier les processus par rapport au courrier postal et aux télécopies dans la mesure où des raisons techniques, juridiques ou économiques ne s'y opposent pas.
- La transmission automatique de courriers électroniques à des adresses électroniques externes à l'entreprise (p. ex. propre boîte aux lettres électronique privée) n'est pas autorisée. Dans des cas justifiés, un accès alternatif peut être mis en place.
- Les informations qui méritent tout particulièrement d'être protégées, par exemple les informations personnelles, ne doivent pas être envoyées à l'extérieur sous forme non codée par courrier

électronique. Cela est applicable non seulement au contenu de courriers électroniques, mais aussi aux documents/annexes (attachments) joints.

§ 9 Accès à distance

- On entend par accès à distance l'accès au réseau de l'entreprise ou à ses appareils connectés lorsque cet accès a lieu hors des locaux de Vebego SA.
- La direction autorise l'accès à distance au réseau de l'entreprise sur demande écrite lorsqu'elle estime que cela est nécessaire pour des raisons inhérentes à l'entreprise.
- Seuls les appareils désignés par la division IT sont assistés.
- Les logiciels permettant l'accès au réseau de l'entreprise doivent être installés uniquement par la division IT.
- L'accès à distance est configuré de manière à ce que les frais de connexion incombent à l'entreprise. Par principe, les frais d'installation ou d'exploitation (électricité, téléphone, etc.) ne sont pas remboursés.

§ 10 Utilisation inappropriée ou privée

- L'utilisation des ordinateurs, de l'Internet et du courrier électronique doit prendre en considération les intérêts de l'entreprise, des risques juridiques ou opérationnels devant être en particulier exclus.
- Il est en particulier interdit d'avoir recours à des supports ayant des contenus illicites, contraires aux droits d'auteur, racistes, offensants, pornographiques ou dénigrants ou de diffuser de tels contenus.
- L'utilisation privée des applications Office, de l'Internet ou du courrier électronique est autorisée dans la mesure où des ressources négligeables (temps de travail, capacité du réseau, mémoire) sont sollicitées. L'utilisation privée ne doit pas nuire à l'accomplissement de tâches attribuées et doit se limiter à l'indispensable.
- Les données privées (p. ex. courriers électroniques privés) doivent être classées dans un registre séparé pourvu du nom «privé» ou «personnel».
- En cas d'utilisation inadaptée, la direction se réserve le droit de procéder à des restrictions techniques ou de bloquer certains identifiants d'utilisateurs.

§ 11 Téléchargement (download) ou copie d'informations

- Il est interdit aux collaborateurs de copier ou télécharger, puis d'installer ou de transmettre des logiciels de l'Internet ou de courriers électroniques et autres supports de données. Cette disposition n'est pas applicable aux services désignés à l'article 3, paragraphe 1.
- Les autres données (y compris celles comportant des contenus multimédias), peuvent être téléchargées sur le réseau de l'administration uniquement dans les conditions suivantes:
    a) les données doivent avoir un lien professionnel et ne doivent pas contrevenir aux dispositions particulières sur l'utilisation privée (article 10 ci-dessus);
    b) les données doivent être obtenues ou utilisées dans le respect de toutes les exigences de l'entreprise ainsi que des dispositions prévues par la loi;
    c) les données ne doivent pas être déclarées comme étant critiques en terme de sécurité par le scanner de virus installé sur tous les ordinateurs de l'entreprise.

§ 12 Newsletter

Les Newsletters commandées doivent être annulées lors du départ de l'entreprise.

§ 13 Evénements importants en terme de sécurité

Tous les événements importants pour la sécurité (p. ex. perte d'un appareil, comportement inexplicable du système, perte ou modification de données et programmes, disponibilité de services non explicitement validés, soupçon d'abus quant aux propres identifiants d'utilisateurs, etc.) doivent être immédiatement communiqués au chef de la division IT qui en examine les causes et prend si nécessaire des mesures complémentaires. Attention! Excepté lors de la perte d'un appareil, n'entreprenez en aucun cas de propres enquêtes; des indications et traces précieuses pourraient être en effet, dans un tel cas, effacées ou perdues.

§ 14 Contrôles et établissement de procès-verbaux

- Les données des procès-verbaux servent exclusivement à la sauvegarde de données et à assurer une utilisation en bonne et due forme dans des buts de contrôle de la protection des données et de la révision IT. Elles ne sont pas utilisées en vue d'une évaluation préventive du comportement ou des prestations.
- Le procès-verbal prend en considération la loi sur la protection des données, la protection de la vie privée dans le cadre des dispositions légales applicables et autres dispositions relatives à la conservation de documents.
- Afin de garantir les exigences en matière de sécurité de l'entreprise, le chef de la division IT vérifie périodiquement l'évaluation globale (sans limitation sur des personnes déterminées) de l'utilisation des systèmes, des applications, des réseaux, des courriers électroniques, de l'accès à distance et de l'Internet ainsi que les bases de données déposés sur les serveurs. Si cette vérification engendre un doute quant à un manquement au présent règlement, des contrôles adaptés des personnes peuvent être réalisés. Un contrôle préventif des personnes n'est pas autorisé.
- Par principe, les collaborateurs sont informés au préalable lors de la réalisation d'un contrôle de personnes. Il peut être renoncé à un avis préalable si
    - la sécurité des données, en particulier la disponibilité du système ne peut plus être garantie ou
    - en présence d'indices sur un acte illicite particulièrement répréhensible.
- Si un abus est constaté dans le cadre du contrôle d'une personne, le service compétent ou les autorités chargées des poursuites pénales sont informés.
- Le supérieur hiérarchique peut vérifier les données personnelles dans la mesure où cela est nécessaire à son activité de surveillance. L'application de dispositions particulières sur la confidentialité demeure réservée.

§ 15 Entrée en vigueur

- Le présent règlement a été mis en vigueur par la direction le 1er janvier 2004 et a été remanié le 22 septembre 2009.
- Le règlement sur l'utilisation des outils informatiques doit être signé par tous les collaborateurs qui y ont recours. La dernière page (page 3) avec la confirmation est émise en deux exemplaires; l'exemplaire pourvu de la signature est déposé dans le dossier du personnel.