Charte informatique

Conditions générales d'utilisation

Toute personne utilisant le système d'information de TRISKEM INTERNATIONAL s'engage à :

- respecter la charte informatique
- ne pas modifier la configuration des systèmes et du réseau en place
- ne pas introduire de programme nuisible (virus, cheval de Troie, vers, …)
- ne pas installer de logiciel sur sa station de travail. Cependant, si un logiciel est nécessaire il devra être installé par la personne en charge du système d'information

Les utilisateurs ont le droit de stocker des données personnelles sous condition de les stocker sur leur propre ordinateur et non sur les lecteurs réseau qui eux sont réservés aux documents concernant l'entreprise ou son bon fonctionnement.

Chaque utilisateur est responsable pour ce qui le concerne du respect du secret professionnel et de la confidentialité des informations qu'il est amené à détenir, consulter ou utiliser. Les règles de confidentialité ou d'autorisation préalable avant diffusion externe ou publication sont définies par la direction et applicables quel que soit le support de communication utilisé.

L'utilisateur est responsable des ressources qui lui sont confiées dans le cadre de l'exercice de ses fonctions. Il doit concourir à la protection des dites ressources, en faisant preuve de prudence et de vigilance. En particulier, il doit signaler à la direction toute violation ou tentative de violation de l'intégrité de ces ressources, et, de manière générale tout dysfonctionnement, incident ou anomalie.

Identification

Chaque salarié/prestataire dispose d'identifiants personnels, pour se connecter aux stations de travail. L'identification (login + mot de passe) est unique et confiée à chaque utilisateur. Ce dernier est personnellement responsable de l'utilisation qui peut en être faite, et ne doit en aucun cas la communiquer. Le mot de passe permettant d'accéder aux différents services, doit obligatoirement se composer d'une majuscule, d'une minuscule d'un caractère spécial ainsi que d'un chiffre. Il devra se composer de 8 caractères minimum.

L'identification permet en particulier de contrôler l'activité des utilisateurs, dans un but de sécurisation et de détection de toute utilisation inhabituelle.

En cas d'absence, même temporaire, il est impératif que l'utilisateur verrouille l'accès au matériel qui lui est confié ou à son propre matériel, dès lors que celui-ci contient des informations à caractère professionnel.

Messagerie électronique

Chaque salarié dispose, pour l'exercice de son activité professionnelle, d'une adresse de messagerie électronique normalisée attribuée par la direction informatique. Les messages électroniques reçus sur la messagerie professionnelle font l'objet d'un contrôle antiviral et d'un

filtrage anti-spam. Les salariés sont invités à informer la direction des dysfonctionnements qu'ils constateraient dans ce dispositif de filtrage.

Les utilisateurs doivent veiller au respect des lois et règlements, et notamment à la protection des droits de propriété intellectuelle et des droits des tiers. Les correspondances électroniques ne doivent pas comporter d'éléments illicites, tels que des propos diffamatoires, injurieux, contrefaisants ou susceptibles de constituer des actes de concurrence déloyale ou parasitaire.

Les messages à caractère personnel sont tolérés, à condition de respecter la législation en vigueur, de ne pas perturber et de respecter les principes posés dans la présente charte. Les messages envoyés doivent être signalés par la mention "Privé" ou "Perso" dans leur objet et être classés dès l'envoi dans un dossier lui-même dénommé de la même façon. Les messages reçus doivent être également classés, dès réception, dans un dossier lui-même dénommé "Privé" ou "Perso". En cas de manquement à ces règles, les messages sont présumés être à caractère professionnel. Toutefois, les utilisateurs sont invités, dans la mesure du possible, à utiliser leur messagerie personnelle via un client en ligne pour l'envoi de messages à caractère personnel plutôt que la messagerie de l'entreprise.

Utilisation d'Internet

Il est interdit :

- de communiquer à des tiers des informations techniques concernant son matériel
- de diffuser des informations sur l'entreprise via des sites Internet
- de participer à des forums *(même professionnels)*
- de participer à des conversations en ligne (« chat »).

La consultation de sites à caractère illicite, violent, pornographique, xénophobe ou dont le contenu est contraire à l'ordre public, aux bonnes mœurs ou à l'image de marque de l'entreprise, ainsi qu'à ceux pouvant comporter un risque pour la sécurité du système d'information de l'entreprise ou engageant financièrement celle-ci est strictement interdite au sein de l'entreprise. TRISKEM INTERNATIONNAL se dégage cependant de toute responsabilité en cas d'un usage d'internet à des fins illégales.

Les utilisateurs sont informés que la direction informatique enregistre leur activité sur Internet et que ces traces pourront être exploitées à des fins de statistiques, contrôle et vérification dans les limites prévues par la loi.

L'utilisation d'Internet à des fins privées est tolérée dans des limites raisonnables et à condition que la navigation n'entrave pas l'accès professionnel.

Mobilité

Les utilisateurs qui effectuent des déplacements avec du matériel informatique doivent prendre conscience que les données stockées dans les équipements peuvent nuire gravement à l'entreprise si elles venaient à être volées de quelques manières que ce soit. Les personnes amenées à faire des déplacements doivent se signaler auprès des/du responsable(s) informatique afin de mettre en place des protections spécifiques.

On entend par « nomade » tous les moyens techniques (ordinateur portable, téléphone, smartphone, tablette,…) qui peuvent être utilisés hors des murs de l'entreprise. Lorsque ces matériels sont utilisés hors des murs de l'entreprise, l'utilisateur en assure la garde et la responsabilité. Il assiste l'entreprise ou procède lui-même selon les cas à toutes les démarches (déclaration assurance, dépôt de plainte,...) rendues nécessaires à la suite d'un incident de quelque nature que ce soit.

L'utilisation de moyens informatiques et de communication électronique nomades impose à l'utilisateur un niveau de surveillance et de confidentialité renforcée. Il doit notamment veiller à ce que des tiers non autorisés ne puissent utiliser ou accéder aux contenus des appareils nomades.

En cas d'incident avéré mais aussi en cas de doute, il doit immédiatement en aviser sa hiérarchie.

Lorsqu'un accès à distance est accordé à un utilisateur, celui-ci s'engage à utiliser les moyens techniques d'authentification forte qui lui sont remis et aucun autre.

En termes de sécurité et de confidentialité, l'utilisateur devra suivre toutes les prescriptions complémentaires qui lui seront signifiées.

En cas de perte ou de vol des moyens d'authentification à distance, il devra aviser, sans délai, le(s) personnes responsable(s) de l'informatique.

Surveillance des activités

Le système d'information et de communication s'appuie sur des fichiers journaux ("logs"), créés en grande partie automatiquement par les équipements informatiques et de télécommunication. Ces fichiers sont stockés sur les postes informatiques et sur le réseau. Ils permettent d'assurer le bon fonctionnement du système, en protégeant la sécurité des informations de l'entreprise, en détectant des erreurs matérielles ou logicielles et en contrôlant les accès et l'activité des utilisateurs et des tiers accédant au système d'information. Les utilisateurs sont informés que de multiples traitements sont réalisés afin de surveiller l'activité du système d'information et de communication. Sont notamment surveillées et conservées les données relatives :

- à l'utilisation des logiciels applicatifs, pour contrôler l'accès, les modifications et suppressions de fichiers
- aux connexions entrantes et sortantes au réseau interne, à la messagerie et à Internet, pour détecter les anomalies liées à l'utilisation de la messagerie et surveiller les tentatives d'intrusion et les activités, telles que la consultation de sites ou le téléchargement de fichiers.

L'attention des utilisateurs est attirée sur le fait qu'il est ainsi possible de contrôler leur activité et leurs échanges. Des contrôles automatiques et généralisés sont susceptibles d'être effectués pour limiter les dysfonctionnements, dans le respect des règles en vigueur.

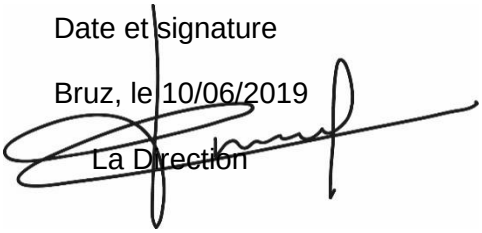
En cas de dysfonctionnement constaté par la direction informatique, il peut être procédé à un contrôle manuel et à une vérification de toute opération effectuée par un ou plusieurs utilisateurs. Le contrôle concernant un utilisateur peut porter sur les fichiers contenus sur le disque dur de l'ordinateur, sur un support de sauvegarde mis à sa disposition ou sur le réseau de l'entreprise, ou sur sa messagerie. Alors, sauf risque ou événement particulier, la direction ne peut ouvrir les fichiers ou messages identifiés par l'utilisateur comme personnels ou liés à la délégation de personnel conformément à la présente charte, qu'en présence de l'utilisateur ou celui-ci dûment appelé.

Charte informatique

Le manquement aux règles et mesures de sécurité décrites dans la présente charte est susceptible d'engager la responsabilité de l'utilisateur. Le Représentant de l'entreprise ou son représentant légal, se réserve le droit d'engager ou de faire engager des poursuites pénales à l'encontre de ce dernier.

Date et signature

Bruz, le 10/06/2019



La Direction

Date et signature

L'utilisateur