NOTE INTERNE	
Date de diffusion	**27 janvier 2016**
Objet	**Charte informatique Groupe NOX**
Destinataires	**Tous collaborateurs**
Emetteur	**Lionel LEMARECHAL – Directeur Général Adjoint Supports**

PREAMBULE

Le Groupe NOX met en œuvre un système d'information et de communication nécessaire à son activité, comprenant notamment un réseau informatique et téléphonique. Les salariés, dans l'exercice de leurs fonctions, sont conduits à accéder aux moyens de communication mis à leur disposition et à les utiliser. L'utilisation du système d'information et de communication doit être effectuée exclusivement à des fins professionnelles, sauf exception prévue dans la présente charte.
Dans un but de transparence à l'égard des utilisateurs, de promotion d'une utilisation loyale, responsable et sécurisée du système d'information, la présente charte pose les règles relatives à l'utilisation de ces ressources. L'utilisation des ressources informatiques impose le respect de règles pour garantir la disponibilité du système, la sécurité et la préservation des données. Les comptes mis à disposition de l'utilisateur sont révoqués à la date de départ du collaborateur.

I. CHAMPS D'APPLICATION

a. Utilisateurs concernés

Sauf mention contraire, la présente charte s'applique à l'ensemble des utilisateurs du système d'information et de communication de l'entreprise, quel que soit leur statut, y compris les mandataires sociaux, salariés, intérimaires, stagiaires, employés de sociétés prestataires, visiteurs occasionnels.
Les salariés veillent à faire accepter valablement les règles posées dans la présente charte à toute personne à laquelle ils permettraient d'accéder au système d'information et de communication.

b. Système d'information et de communication

Le système d'information et de communication de l'entreprise est notamment constitué des éléments suivants : ordinateurs (fixes ou portables), périphériques, assistants personnels, réseau informatique (serveurs, routeurs et connectique), photocopieurs, téléphones, logiciels, fichiers, données et bases de données, système de messagerie, intranet, extranet, abonnements à des services interactifs.

II. MATERIEL ET LOGICIEL

a. Poste de travail

Chaque collaborateur se voit confier un ordinateur et attribuer un identifiant et un mot de passe qui lui sont personnels. Il est recommandé de le changer tous les 6 mois minimum. La société se réserve le droit de forcer sa réinitialisation en cas de besoin de maintenance.

Avant toute utilisation, l'utilisateur doit s'assurer que l'antivirus est effectivement activé et qu'il n'y a aucune activité suspecte sur l'espace de travail.

b. Autres Matériels

Tous les supports connectés aux ordinateurs à des fins d'importation et exportation de données doivent impérativement être soumis à l'antivirus. (clés USB, disques dur, cartes mémoire etc.)
Le matériel du groupe est strictement réservé à l'exécution du travail interne à l'entreprise, tout usage personnel est prohibé sauf accord explicite de la Direction.
L'usage du matériel en libre-service est soumis à une planification qu'il convient de respecter.
Le matériel attaché à un ordinateur ne doit être en aucun cas dissocié du poste sans l'accord de la DSI.
Aucun échange de matériel entre collaborateur ne doit être effectué sans l'avis de la DSI (Direction Systèmes d'information). Il est interdit de relier quelconque matériel extérieur à l'entreprise au réseau interne (stockage, pc personnel etc…), sauf accord explicite de la DSI. Les matériels dits « nomades » sont soumis aux mêmes conditions d'utilisation (installation d'application, usage personnel, sensibilité des données, sauvegarde). Chaque matériel nomade devra être connecté au réseau de l'entreprise au minimum une fois par semaine.
L'achat de tout matériel informatique et logiciel, sans l'accord de la DSI est proscris. Sans accord ces achats ne seront ni installés, ni supportés, ni intégrés dans l'organisation informatique NOX.
Tout matériel doit être restitué à la date de départ du collaborateur.

c. Logiciels

Il est interdit d'installer un logiciel qui n'aurait pas été au préalable autorisé par la DSI. Il est interdit d'utiliser un logiciel sur un système sans s'être assuré préalablement que les droits de licence le permettent. Toute copie de logiciel et détournement de son utilisation première est formellement interdite.
Pour faire face à des problèmes d'assurance, la DSI impose une version minimale des logiciels. Toute version antérieure est proscrite, sauf avis de la DSI. L'installation de logiciel dit « CLOUD » est formellement interdit (Dropbox, skydrive, iCloud…) sauf accord explicite de la Direction et de la DSI.

d. Téléphones portables

Si le collaborateur se voit confier un téléphone portable, son usage est réservé à des fins professionnelles. A titre exceptionnel, l'utilisation à des fins personnelles, et exclusivement pour satisfaire aux besoins de la vie courante, est tolérée pour autant que par sa fréquence et/ou sa durée, elle ne perturbe pas l'activité professionnelle.
L'utilisation d'un téléphone personnel est autorisé (changement de carte SIM ou double carte SIM) mais la configuration du terminal (mail, etc.) n'incombe pas, dans ce cas, à la DSI, et le matériel confié non utilisé devra être restitué.

e. Divers

Aucun document à caractère privé ne doit être sauvegardé sur les serveurs. La DSI, avec l'accord express de la Direction, se réserve le droit de supprimer tout fichier manifestement personnel (par exemple de la musique ou des films), sans avertissement préalable.

L'utilisation de connexion internet tierce visant à passer outre les systèmes de sécurité de l'entreprise est strictement interdite.
Les outils biométriques qui sont installés de base sur les matériels sont par défaut désactivés. Toutefois si l'utilisateur procède à leurs exploitations, l'entreprise dégage toute responsabilité quant à l'utilisation frauduleuse des informations liées à la mauvaise utilisation de ces outils.

III. LA MESSAGERIE

Si chaque utilisateur a la possibilité de communiquer librement, il doit le faire sans abus, dans les limites des nécessités professionnelles et en respectant l'obligation de discrétion et de secret professionnel inhérente à ses fonctions. L'emploi à titre privé de la messagerie n'est autorisée qu'à titre exceptionnel et à condition que cela ne perturbe pas l'activité professionnelle, n'engorge pas le réseau informatique et n'ait pas vocation à générer un gain personnel.
Le contenu des données mises en ligne doit obéir aux règles générales de la communication, aussi bien dans le domaine privé que dans le domaine public. Les utilisateurs doivent donc impérativement respecter les règles de bonne conduite suivantes :

- ne pas communiquer d'informations à caractère diffamatoire, injurieux ou mensonger,
- ne pas communiquer des données à caractère illicite ou contraires aux bonnes mœurs,
- éviter de porter atteinte à des droits privatifs tels que des œuvres ou logiciels protégés.

Pour que ce système de communication constitue effectivement un outil permettant d'améliorer l'efficacité professionnelle, il convient de respecter un certain nombre de règles :

- éviter les listes de diffusion massives par courriel telle que la diffusion de chaîne,
- éviter la diffusion de messages trop volumineux ou de messages dont les fichiers joints seraient trop volumineux, (le cas échéant, des solutions ftp ou de transfert de gros fichiers en ligne sont disponibles), l'entreprise se réserve le droit de mettre en place des quotas.
- ne mettre en copie des messages que les personnes directement concernées par l'objet de la communication.

Tout message électronique est réputé professionnel sauf mention expresse révélant son caractère privé ou personnel, ce qui lui conférerait la nature d'une correspondance privée.
Pour éviter toute surcharge des boites de messagerie, chaque utilisateur doit régulièrement sauvegarder (fichier PST local) ou supprimer les éléments reçus et envoyés. L'utilisateur est invité à être sensible à la nature des messages qu'il reçoit. S'il a un doute sur la provenance ou le contenu d'une pièce jointe, il doit contacter le correspondant informatique le plus proche pour prévenir tout désagrément.

Le compte de messagerie est verrouillé à la date de départ du collaborateur, les données sont transférées à son responsable hiérarchique pour une période de 6 mois (après information du collaborateur), après laquelle le compte est supprimé.

IV. INTERNET

L'utilisation du réseau Internet doit être exclusivement réservée à des fins professionnelles. A titre exceptionnel, l'utilisation à des fins personnelles, et exclusivement pour satisfaire aux besoins de la vie courante, est tolérée, pour autant que par sa fréquence et/ou sa durée, elle ne perturbe pas l'activité professionnelle.
La contribution des utilisateurs à des forums de discussion, systèmes de discussion instantanée, blogs, sites est interdite, sauf à titre professionnel et sur autorisation expresse de la DSI.

L'utilisation d'Internet présente des risques en cas de mauvais contrôle de l'information, de récupération par téléchargement de contenus privatifs (logiciels ou œuvres protégées) ou la consultation de sites à contenus illicites et contraires aux bonnes mœurs. Il est à ce titre rappelé que l'utilisation d'internet pour accéder à des sites dont le contenu diffusé est en infraction avec la législation nationale (contenus pédophiles, incitation à la haine raciale etc.) est formellement interdite. La société se réserve le droit de bloquer l'accès à certains sites par l'intermédiaire d'une liste noire (« blacklist »). De même il convient de vérifier les droits d'auteur (images, textes) avant d'utiliser les données.
Ces règles s'appliquent aussi bien au sein du réseau interne de l'entreprise que lors de l'utilisation des outils nomades (ordinateurs portables sur wifi public, smartphones, tablettes, etc.).
Il est strictement interdit d'installer des outils pour passer outre les systèmes de sécurité de l'entreprise (modules internet, tunnels VPN privatifs).

V. RESPONSABILITES DE L'UTILISATEUR

Lors de l'accès aux ressources informatiques mis à sa disposition par l'entreprise, l'utilisateur doit respecter les règles définies dans la présente Charte et agir en vertu de la réglementation applicable.
En cas de manquements, d'agissements frauduleux, fautifs ou dommageables :

- l'utilisateur pourra voir sa responsabilité personnelle engagée pour tout type de préjudice résultant de son fait,
- dans le cas où la responsabilité de la société serait engagée, elle pourra se retourner contre l'utilisateur ayant enfreint le présent règlement,
- l'utilisateur pourra également faire l'objet de sanctions disciplinaires.

Tout utilisateur est responsable de l'utilisation qu'il fait des ressources informatiques ; il s'engage à n'effectuer aucune opération qui pourrait nuire au fonctionnement normal du réseau, à l'intégrité des moyens informatiques, ou aux relations internes et externes de la société.
Tout utilisateur devra se garder strictement :

- d'interrompre le fonctionnement normal du réseau ou des systèmes connectés au réseau (manipulations anormales, introduction de virus),
- d'accéder à des informations appartenant à un autre utilisateur sans son autorisation,
- de modifier ou détruire des informations appartenant à un tiers sans son autorisation,
- de porter atteinte à l'intégrité d'un autre utilisateur ou sa sensibilité, notamment par l'intermédiaire de la messagerie,
- de masquer sa véritable identité, en particulier en se connectant sous le nom d'un autre utilisateur,
- de développer ou d'utiliser des outils mettant sciemment en cause l'intégrité des systèmes,
- de nuire à la société par une mauvaise utilisation des outils réseaux.

La sécurité est l'affaire de tous, chaque utilisateur doit y contribuer à son niveau et mettre en application les règles de bon sens et les recommandations fournies par la DSI. Parmi les règles de bon sens et de bon usage :

- user raisonnablement de toutes les ressources partagées (puissance de calcul, espace disque, logiciels à jetons, bande passante sur le réseau),
- ne jamais quitter son poste de travail en laissant une session ouverte,
- ne laisser aucun document affiché sur l'écran de visualisation après exploitation,
- suivre les recommandations de la DSI en matière de mots de passe. Ces mots de passe doivent être choisis non transparents et tenus secrets. Il ne faut donc ne jamais les écrire sur un support matériel ni les communiquer à un tiers. Il convient de les changer régulièrement, tous les 6 mois minimum.
- ne jamais prêter son compte sans contrôle
- sauvegarder régulièrement ses fichiers

VI. RESPONSABILITE ET DEVOIRS DE L'ENTREPRISE

L'entreprise est elle-même soumise aux règles de bon usage des moyens informatiques et se doit de faire respecter les règles définies dans ce document.
L'entreprise ne pourra être tenue pour responsable de la détérioration d'informations du fait d'un utilisateur ne s'étant pas conformé aux règles énoncées dans cette Charte.
A des fins de maintenance informatique, la DSI peut accéder à l'ensemble des postes de travail. Dans le cadre de mise à jour, de dépannage et d'évolutions du système d'information, et lorsqu'aucun utilisateur n'est connecté sur son poste de travail, la DSI peut être amenée à intervenir sur l'environnement technique des utilisateurs.
En cas de manquement de l'utilisateur aux règles et mesure de sécurité de la présente Charte, la DSI est susceptible de couper partiellement ou en totalité l'utilisation de certaines ressources (internet, imprimante, droits sur les dossiers).

VII. INFORMATION RELATIVE AUX MOYENS DE CONTROLE

Il a été mis en place des outils afin d'assurer la sécurité et le bon fonctionnement du réseau. Ces outils enregistrent les messages transmis ainsi que la nature et la durée des connexions Internet, poste par poste.
Suite à la consultation du Comité d'Entreprise, la société réalisera auprès de la CNIL une déclaration aux termes de laquelle elle se réserve le droit, notamment en cas de surcharge inexplicable de la messagerie, du réseau, ou d'augmentation inexpliquée du coût des communications via internet, laissant présumer une utilisation abusive ou détournée de son objet des moyens de communications susvisés, de contrôler par l'intermédiaire de ces outils, notamment les adresses de messagerie, le volume des fichiers chargés ou expédiés, les adresses des sites consultés, la géolocalisation, les logiciels installés ainsi que l'historique virale du poste et des outils de communications.

VIII. REGLES DE CONFIDENTIALITE ET DE SECURITE DES DONNEES

Du fait de la collecte et du traitement des informations nominatives effectuées, la société s'engage dans la mesure du possible, en particulier sur le plan technologique, à prendre toutes les précautions utiles afin de préserver la sécurité de ces informations et notamment d'empêcher qu'elles ne soient déformées, endommagées ou communiquées à des tiers non autorisés.

La mise en place d'outils de sécurité ne doit cependant pas dispenser les utilisateurs de signaler toutes tentatives d'intrusions extérieurs, de falsifications ou de présence de virus à son correspondant informatique directe.

IX. ENTREE EN VIGUEUR

La présente Charte est applicable à compter du : 01/02/2016