NOCIBÉ
la beauté libérée

Charte d'utilisation des ressources informatiques

Annexe du REGLEMENT INTERIEUR
APPLICABLE AUX ETABLISSEMENTS
DE L'UES NOCIBE

SOMMAIRE

Préambule

L'usage de la messagerie, l'accès aux ressources informatiques de l'Entreprise et notamment de l'Internet fait courir aux Utilisateurs et à l'Entreprise de nouveaux risques liés aux flux entrants et sortants.

Face à ces risques et usages, l'Entreprise s'est interrogée légitimement sur sa politique de sécurité basée sur l'information, la sensibilisation, la loyauté et la responsabilisation de chacun, tout en respectant un nécessaire équilibre entre droits fondamentaux des Utilisateurs et le devoir de contrôle et de surveillance de l'Entreprise.

C'est la raison pour laquelle cette Charte a été conçue comme un guide d'utilisation des ressources informatiques allié à un rappel des règles essentielles décrivant les principes directeurs de la sécurité.

Article 1 – Objet

La Charte d'utilisation des ressources informatiques de l'Entreprise définit les règles d'utilisation des ressources informatiques, qu'elles soient en libre service ou mises à disposition de chaque Utilisateur.
Elle informe les divers Utilisateurs en leur faisant prendre conscience des éventuelles sanctions auxquelles ils s'exposent en cas de non observation, dans le respect de la législation en vigueur et en application du règlement intérieur applicable aux établissements de l'UES Nocibé.

Article 2 – Définitions

- *Donnée à caractère personnel* : toute information relative à une personne physique identifiée ou qui peut être identifiée, directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres, tels que l'image ou l'identité, sans que cette liste ne soit exhaustive.

- *Entreprise* : l'UES NOCIBE, constituée de son siège social et de l'ensemble de ses établissements actuels et futurs.

- *Système d'Information ou « SI »* : Ensemble organisé de ressources (matériel, logiciel, personnel, données, procédures…) permettant d'acquérir, de stocker, de transformer et de communiquer des informations sous forme de textes, images, sons, données codées, ou autre dans des organisations.

- *Système de Traitement Automatisé de Données ou « STAD »* : Ensemble des moyens techniques (logiciels, matériels, systèmes, programmes, données, réseaux, …) permettant la réalisation de traitements informatiques au sein d'une organisation.

- *Mail, Courriel, Message électronique* : Désigne la notion de messagerie stockée et véhiculée de manière électronique.

- *Malware* : désigne un logiciel développé en tout ou partie dans le but de porter atteinte au Système d'Information et de Communication de l'Entreprise.

Article 3 – Statut de la Charte

En sa qualité d'annexe au règlement intérieur applicable aux établissements de l'UES Nocibé, la présente charte a été soumise à la procédure d'adoption suivante : consultation du CHSCT puis du Comité d'Entreprise, envoi à l'Inspection du Travail, affichage dans les locaux de l'Entreprise.

Toute violation de ses règles constituera une faute (simple, grave ou lourde au sens du Code du travail, selon les circonstances) susceptible de sanctions disciplinaires allant du simple avertissement au licenciement sans préavis ni indemnités selon sa gravité.

Les règles et obligations ci-dessous énoncées s'appliquent à tout Utilisateur autorisé à utiliser les moyens et systèmes informatiques de l'Entreprise.

Ces derniers comprennent toutes les ressources informatiques de l'Entreprise et notamment les serveurs, stations de travail, périphériques, micro-ordinateurs et équipements mobiles propriétés de l'Entreprise, qu'ils soient connectés ou non aux réseaux de l'Entreprise.

Le respect des règles définies par la présente Charte s'étend également à l'utilisation des systèmes informatiques d'organismes extérieurs à l'Entreprise, systèmes accessibles par l'intermédiaire des réseaux de l'Entreprise, par exemple le réseau Internet.

Article 4 – Principes

4.1 – Utilisation professionnelle

L'Utilisateur est responsable de l'usage qu'il fait des ressources informatiques de l'Entreprise mises à sa disposition, dans l'exercice de sa fonction. Il réserve cet usage au cadre de son activité professionnelle. Un usage personnel exceptionnel ne doit en aucun cas empêcher la bonne exécution du contrat de travail ou de la mission et ne doit pas nuire à l'intérêt de l'Entreprise, de ses clients ou de ses salariés.

L'Utilisateur est responsable de la pérennité de ses fichiers et de l'intégrité de son espace de travail dans la mesure où il respecte les règles d'usages recommandées par la DSI.

4.2 – Règles de bonne conduite

Tout Utilisateur s'engage à respecter les règles d'usage des outils informatiques et notamment à ne pas effectuer intentionnellement des opérations ayant pour but:

- De masquer sa véritable identité ou usurper l'identité d'autrui.
- D'installer et d'utiliser un logiciel à des fins non conformes aux missions de l'Entreprise.
- De contourner les mesures de sécurité mises en place sur son poste.
- D'installer ou utiliser tout matériel informatique sans l'autorisation de l'entreprise.
- De récupérer, copier, ou sauvegarder tout logiciel présent sur son poste.

4.3 – Préservation de la sécurité technique et applicative du système

L'Utilisateur ne doit pas :

- Mettre en place un programme ou une solution pour contourner les moyens de sécurité et la politique de sécurité informatique de l'Entreprise.
- Accéder aux données d'autrui sans l'accord exprès des détenteurs même lorsque ces données ne sont pas explicitement protégées.
- Désactiver le pare-feu, anti-virus ou toute autre mesure de sécurité mise en place sur son poste ou le poste d'autrui.
- Installer ou connecter des périphériques nomades professionnels non sécurisés.
- Utiliser des matériels ou périphériques personnels sans accord de la DSI.
- Récupérer des données de l'entreprise sans y être explicitement habilité et autorisé.
- Contourner les règles de filtrage des accès Internet.

4.4 – Absences et départs

En cas d'absence prolongée du salarié, et si ce dernier n'a pas fait le nécessaire pour que ses messages soient transférés auprès d'un collègue ou le cas échéant de son supérieur hiérarchique ou encore pour qu'un message d'alerte informe ses correspondants, un e-mail type sera envoyé à chaque personne ayant contacté par e-mail le salarié, indiquant que ce dernier est indisponible. Ce message comportera l'adresse e-mail d'un autre salarié joignable.

Article 5 – Utilisation du courrier électronique ou courriel

L'Entreprise met à disposition de certains Utilisateurs du SI, un Système de messagerie. L'Entreprise ne pourra être tenue responsable du contenu des Courriels transitant au sein du système de messagerie.

L'Utilisateur doit respecter les contraintes techniques qui lui ont été indiquées en terme de :

- Nombre maximum de messages pouvant être envoyés en une seule fois ;
- Taille maximale des documents attachés ;
- Conservation ou effacement des messages reçus ou envoyés ;
- Précautions à prendre lors de la réception de messages d'origine inconnue.

Article 6 – Utilisation d'Internet

L'Entreprise met à la disposition de certains Utilisateurs du SI, un système d'accès à Internet bénéficiant d'une politique active de sécurité visant à protéger l'Entreprise contre les Virus et les actions malveillantes pouvant lui porter préjudice. L'Entreprise ne pourra être tenue responsable du contenu des sites visités par l'Utilisateur.

Seuls ont vocation à être consultés et utilisés les sites Internet présentant un lien direct et nécessaire avec l'activité professionnelle. L'utilisateur ne doit absolument pas consulter de sites illégaux : contenus racistes, terroristes etc...

Les conséquences juridiques des activités individuelles ne faisant partie des missions du collaborateur ne sont pas de la responsabilité de l'entreprise.

Article 7 – Utilisation du téléphone

L'utilisation des téléphones fixes et portables professionnels est exclusivement réservée à des fins professionnelles, sous réserve de la législation relative aux avantages en nature.
En tout état de cause, l'usage du téléphone à titre personnel est strictement limité aux communications locales, incluses dans les forfaits et non surtaxées.

Article 8 – Utilisation des équipements nomades professionnels

On entend par « équipements nomades » tous les moyens techniques mobiles (ordinateur portable, tablette tactile, imprimante portable, téléphone mobile ou smartphone, CD ROM, clé USB, etc...).

Le matériel fournit par l'entreprise doit faire l'objet de tous les soins nécessaires pour éviter les dégradations et les vols. En matière de perte ou de vol, l'utilisateur doit prévenir la DSI sans délai, notamment pour les matériels contenant des données confidentielles.

Article 9 – Utilisation des accès à distance

L'Entreprise met à la disposition de certains Utilisateurs du SI, un système de connexion au Système d'information à distance (ex. : Intranet par WiFi, VPN...). Ce système bénéficie d'une politique active de sécurité destinée à protéger l'Entreprise contre les actions malveillantes pouvant lui porter préjudices.

Il doit faire l'objet d'une demande d'autorisation individuelle. Il est strictement interdit de céder ou prêter ses moyens de connexion à distance à un tiers, même s'il s'agit d'un collaborateur de l'entreprise.

Article 10 – Utilisation des imprimantes

Des imprimantes sont mises à disposition des employés de l'entreprise. Dans le cadre de l'utilisation de ces imprimantes le personnel doit considérer qu'il s'agit de matériel destiné à un usage professionnel.

Nombre de documents peuvent contenir des informations confidentielles. Ils ne peuvent donc pas être abandonnés sur les imprimantes.

Dans une perspective de développement durable, il est recommandé d'utiliser les impressions à bon escient.

Article 11 – Respect des droits des tiers

Le personnel doit veiller à respecter les droits des tiers, tant sur le plan du respect du Code Pénal que sur le plan de la responsabilité civile. S'il portait atteinte à ces droits à partir de son poste professionnel, il engagerait non seulement sa responsabilité personnelle, mais il pourrait aussi engager la responsabilité de l'Entreprise. En conséquence, il est interdit au personnel d'enfreindre les différentes lois et réglementations. Cette interdiction comprend aussi le droit à l'image et le droit à la propriété intellectuelle.

Article 12 – Respect des droits du personnel

L'Entreprise s'interdit de prendre connaissance, sans son autorisation expresse, des messages envoyés et reçus par le personnel portant la mention « *PRIVE* » ou « PERSONNEL ». En cas de nécessité technique, l'Entreprise ne pourra ouvrir un message qu'avec l'accord préalable de l'intéressé, et en sa présence sauf urgence justifiée par des motifs impératifs de sécurité ou sur autorisation judiciaire.

Article 13 - Droits d'expression

Si le salarié, lorsqu'il s'exprime sur Internet, s'exprime à destination de l'extérieur de l'Entreprise, même si l'accès à Internet lui est offert par l'Entreprise, ce droit d'expression ne doit pas donner lieu à des abus.

Article 14 – Dispositifs de sécurité et protection de la vie privée

Dans le cadre de sa politique de sécurité du Système d'information, l'Entreprise met en place des outils et solutions de sécurité active visant à éviter toutes activités malveillantes ou pouvant porter préjudice à l'Entreprise , à ses clients, à ses partenaires et à ses collaborateurs.

L'Entreprise est attachée au respect de la vie privée de ses collaborateurs sur le lieu de travail.

La détection et l'éradication de virus sont effectuées par des dispositifs automatisés, qui n'impliquent pas l'ouverture des messages par un membre du personnel technique.

Par contre, les données de connexion aux sites consultés font l'objet d'une analyse *a posteriori,* de façon globale et par poste de travail. Ces données permettent éventuellement :

- Le suivi des consommations, globalement, par service ou par poste.
- L'analyse statistique du trafic vers les sites Internet, en particulier en fonction de leur nature et de leur localisation.
- La mise en œuvre de procédures ad hoc, lorsque la sécurité des systèmes d'information est en cause.

14.1 – Contrôle de l'utilisation

Les solutions de sécurité utilisées par l'Entreprise génèrent des enregistrements ou traces utilisés pour le suivi, l'administration et le support de ces solutions. Ces traces peuvent de manières exceptionnelles être utilisées pour effectuer des recherches en cas de suspicion d'une activité malveillante pouvant porter atteinte à la sécurité du SI de l'Entreprise.

L'ensemble des applications fournissent une traçabilité de l'activité des utilisateurs.

14.2 – Système d'authentification et d'habilitation

Plusieurs ressources mises à disposition de l'Utilisateur utilisent un Système

d'authentification et d'habilitation. Ce système bénéficie d'une trace enregistrant l'identification de l'Utilisateur et la date et l'heure de sa demande d'authentification ou d'usage de ses habilitations.

14.3 – Protection de la messagerie

La protection de la messagerie repose sur une solution AntiVirus, le contrôle des pièces jointes, le contrôle de la taille du Courriel, et un système de trace enregistrant, pour chaque Courriel, l'adresse électronique de l'expéditeur de Courriel, l'adresse électronique du destinataire, la date et l'heure, la taille du Courriel ainsi que les caractéristiques des pièces jointes (le nombre, la taille et le type).

14.4 – Protection de l'accès internet

La protection de l'accès Internet repose sur une solution de filtrage, une authentification d'accès, une restriction d'accès (basée sur le profil de l'Utilisateur) aux sites consultables et un système de trace, enregistrant pour chaque connexion, l'identifiant de l'Utilisateur, le site consulté, la date et l'heure de la consultation.

14.5 – Protection de l'accès à distance

La protection de l'accès à distance repose sur une authentification d'accès, un contrôle d'accès (basé sur le profil de l'Utilisateur) et un système de trace, enregistrant pour chaque connexion, l'identifiant de l'Utilisateur, la date et l'heure de la connexion ainsi que les ressources accédées à distance dans le SI.

14.6 – Protection du poste de travail

La protection du poste de travail repose sur une solution AntiVirus, une solution de pare-feu personnel (système protégeant le poste de travail de toute intrusion externe), une authentification d'accès, un système de trace enregistrant, pour chaque session de travail, l'identifiant de l'Utilisateur et la date et l'heure de démarrage de la session de travail ainsi que les accès filtrés localement.

14.7 – Accès aux informations

En application des articles 38 à 40 de la loi n° 78-17 du 6 janvier 1978, modifiée relative à l'informatique, aux fichiers et aux libertés, le collaborateur dispose d'un droit d'accès, de rectification et d'opposition de ses données qui le concernent.

Article 15 – Administrateur du Système d'Information et de Communication

Le terme « Administrateur » désigne toute personne qui a pour rôle d'assurer le bon fonctionnement de l'ensemble du Système d'Information de l'Entreprise . Pour mener à bien sa mission, il dispose de pouvoirs et de droits d'accès étendus sur le Système d'Information.
L'Administrateur est autorisé à prendre toutes les dispositions nécessaires au maintien de la sécurité et du fonctionnement des ressources dans son périmètre de responsabilité. Il a notamment le droit de :

- Créer, modifier et supprimer les droits d'accès des utilisateurs ;
- Appliquer les modifications et évolutions nécessaires aux applications ;
- Consulter l'historique d'activité des utilisateurs, dans le cadre de besoin de

traçabilité ou d'investigation en cas de problème

Une prise de contrôle à distance des PC est mise en place afin d'améliorer l'efficacité des dépannages sur les PC.
Ce dispositif, aussi appelé prise en main à distance, s'active de manière visible. Pratiquement, l'administrateur envoie une demande de connexion sur le poste de l'utilisateur concerné. L'utilisateur voit alors une fenêtre de demande d'accord s'afficher sur son écran. L'administrateur obtient l'accès uniquement si l'utilisateur valide la fenêtre de demande.

Article 16 – Révision, dépôt et publicité de la charte

En tant qu'annexe du règlement intérieur, la présente charte fait l'objet des mêmes formalités et dépôt, ainsi que le prévoit l'article 41 dudit règlement.

En conséquence, les dispositions de la présente charte informatique NOCIBE, qui ont vocation à s'appliquer dans tous les établissements de l'UES NOCIBE, ont fait l'objet d'une consultation du Comité d'Hygiène de Sécurité et des Conditions de Travail et du Comité d'entreprise.

Elle a été adressée en deux exemplaires à Monsieur l'Inspecteur du Travail de Lille dont dépend le siège social de la société Nocibé, accompagné des avis émis par les Comités et déposé au secrétariat greffe du conseil des prud'hommes de Lille le 21 Décembre 2015.
Elle est affichée dans chacun des établissements de l'UES Nocibé.
Elle entrera en vigueur le 1er février 2015

Toute modification ultérieure, adjonction ou retrait à la présente charte sera soumis à la même procédure, conformément aux prescriptions de l'article L. 1321-4 du Code du Travail et sera communiqué en deux exemplaires à l'inspecteur du travail, accompagné de l'avis des représentants du personnel.

Article 17 – Sanctions et procédures disciplinaires

L'ensemble du Titre 4 du règlement intérieur s'applique concernant tant la définition, que la nature et l'échelle des sanctions applicables, et la procédure disciplinaire permettant de préserver les droits de la défense.

Il est spécifiquement précisé qu'en cas d'abus de l'usage d'Internet, l'utilisateur concerné est prévenu de l'anomalie d'usage et peut se voir appliquer une restriction des sites accessibles. En cas de récidive il peut se voir privé temporairement ou durablement de l'usage d'Internet, ces restrictions d'accès n'ayant pas de caractère disciplinaire en ce qu'elles ne sont pas de nature à affecter immédiatement ou non la présence du salarié dans l'entreprise, sa fonction, sa carrière ou sa rémunération.

Fait à Villeneuve d'Ascq, le 21 Décembre 2015

Luc VALENTIN
Directeur des Ressources Humaines