CHARTE UTILISATION DES EQUIPEMENTS INFORMATIQUES ET TELEPHONIQUES

SOCIETE: SOPHAL SPA

DIRECTION: DIRECTION DES SYSTEMES D'INFORMATIONS

Suivi du Document

Version	*Date*	*Description*	*Auteur*	*Relecteur*
V1.0	21/03/2022	Rédaction de la charte informatique	Mohammed SEMATI	
V1.1	31/03/2022	Relecture de la charte informatique	Amine SENOUCI	Amine SENOUCI

SOMMAIRE

1- Préambule

Les salariés, dans l'exercice de leurs fonctions, sont conduits à utiliser les outils informatiques et téléphoniques mis à leur disposition et à accéder aux services de communication de l'entreprise.

L'utilisation du système d'information et de communication doit se faire 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 et de communication.

La présente charte pose les règles relatives à l'utilisation de ces ressources. Elle définit aussi les moyens de contrôle et de surveillance de cette utilisation mise en place, non seulement pour la bonne exécution du contrat de travail des salariés, mais aussi dans le cadre de la responsabilité pénale et civile de l'employeur.

Elle dispose d'un aspect réglementaire et est communiquée individuellement à chaque salarié et annexée a son contrat de travail. Elle ne remplace en aucun cas les lois en vigueur que chacun est censé connaître.

2- Champ d'application

2.1 Utilisateur 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.

2.2 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 y compris clés USB, réseau informatique (serveurs, routeurs et connectique), photocopieurs, télécopieurs, téléphones, smartphones, tablettes et clés 4G, logiciels, fichiers, données et bases de données, système de messagerie, connexion internet, intranet, extranet, abonnements à des services interactifs.

3- Confidentialité

3.1 Paramètre D'accès :

L'accès à certains éléments du système d'information (comme la messagerie électronique ou téléphonique, les sessions sur les postes de travail, le réseau, certaines applications ou services interactifs) est protégé par des paramètres de connexion (identifiant, mot de passe).

Ces paramètres sont appropriés à l'utilisateur et doivent être gardés confidentiels. Ils permettent en particulier de contrôler l'activité des utilisateurs. Ils ne doivent être communiqués à personne, ni responsable hiérarchique.

Dans la mesure du possible, ces paramètres doivent être mémorisés par l'utilisateur. En tout état de cause, ils ne doivent pas être transmis à des tiers ou aisément accessibles.

Des consignes de sécurité sont élaborées par la direction des systèmes d'informations afin de recommander les bonnes pratiques en la matière. Aucun utilisateur ne doit se servir pour accéder au système d'information de l'entreprise d'un

autre compte que celui qui lui a été attribué. Il ne doit pas non plus déléguer à un tiers les droits d'utilisation qui lui sont attribués.

3.2 Données :

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.

4- Responsabilité

4.1 Rôle de la société :

La société met en œuvre les moyens humains et techniques appropriés pour assurer la sécurité matérielle et logicielle du système d'information et de communication. À ce titre, il lui appartient de limiter les accès aux ressources sensibles et d'acquérir les droits de propriété intellectuelle ou d'obtenir les autorisations nécessaires à l'utilisation des ressources mises à disposition des utilisateurs.

La direction des systèmes d'informations est responsable de la mise en œuvre et du contrôle du bon fonctionnement du système d'information et de communication. Elle doit prévoir un plan de sécurité et de continuité du service, en particulier en cas de défaut matériel. Elle veille à l'application des règles de la présente charte. Elle est assujettie à une obligation de confidentialité sur les informations qu'elle est amenée à connaître.

4.2 Responsabilité de l'utilisateur :

L'utilisateur est responsable quant à lui 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 des systèmes d'informations toute violation ou tentative de violation de l'intégrité de ces ressources, et, de manière générale tout dysfonctionnement, incident ou anomalie.

En cas d'absence, même temporaire, il est impératif que l'utilisateur verrouille l'accès au matériel qui lui est confié.

L'utilisateur doit éviter d'installer ou de supprimer des logiciels, de copier ou d'installer des fichiers susceptibles de créer des risques de sécurité au sein de l'entreprise. Il ne doit pas non plus modifier les paramétrages de son poste de travail ou des différents outils mis à sa disposition, ni contourner aucun des systèmes de sécurité mis en œuvre dans l'entreprise. Il doit dans tous les cas en alerter La direction des systèmes d'informations.

5- Internet

Dans le cadre de leur activité, les utilisateurs peuvent avoir accès à Internet. Pour des raisons de sécurité ou de déontologie, l'accès à certains sites peut être limité ou prohibé par La direction des systèmes d'informations qui est habilitée à imposer des configurations du navigateur et à installer des mécanismes de filtrage limitant l'accès à certains sites.

Dans ce cadre L'accès à Internet est divisé en deux catégories :

- Un accès Full (illimité) pour les directeurs et personnes utilisant l'internet à des fins professionnelles.
- Un accès limité aux sites autorisés à des fins professionnelles pour le reste du personnel.

Il est interdit de se connecter à des sites Internet 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.

La contribution des utilisateurs à des forums de discussion, systèmes de discussion instantanée, chats, blogs n'est autorisée qu'à titre professionnel et sur autorisation expresse de la hiérarchie qui devra en informer La direction des systèmes d'informations. De même, tout téléchargement de fichier, en particulier de fichier média, est prohibé, sauf justification professionnelle dûment validée par la hiérarchie. Il est rappelé que les utilisateurs ne doivent en aucun cas se livrer sur Internet à une activité illicite ou portant atteinte aux intérêts de l'entreprise.

6- Courrier électronique

Certains salariés disposent pour l'exercice de leur activité professionnelle, de deux adresses de messagerie électronique attribuée par La direction des systèmes d'informations, une interne (SOPHAL.NET), et une externe (SOPHAL.DZ).

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 systèmes d'informations des dysfonctionnements qu'ils constateraient dans ce dispositif de filtrage.

Un message électronique peut être communiqué très rapidement à des tiers et il convient de prendre garde au respect d'un certain nombre de principes, afin d'éviter les dysfonctionnements du système d'information, de limiter l'envoi de messages non sollicités et de ne pas engager la responsabilité civile ou pénale de l'entreprise et de l'utilisateur.

Avant tout envoi, il est impératif de bien vérifier l'identité des destinataires du message et de leur qualité à recevoir communication des informations transmises, en cas de doute sur l'expéditeur compétent pour envoyer le message, il convient d'en référer à son supérieur. En présence d'informations à caractère confidentiel, ces vérifications doivent être renforcées ; en cas de besoin, un cryptage des messages pourra être aussi proposé par la direction informatique

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.

7- Téléphonie

Pour leur activité professionnelle, les utilisateurs peuvent disposer d'un poste fixe et d'un terminal mobile, smartphone, tablette, clé 4G ou puce. Pour ce qui est de l'utilisation des terminaux mobiles en connexion pour accès à des sites Internet ou à la messagerie électronique, les règles édictées ci-dessus s'appliquent de la même manière.

Les utilisateurs sont informés que La direction des systèmes d'informations enregistre leur activité téléphonique, aussi bien sur les postes fixes que sur les mobiles. Ces traces seront exploitées à des fins de statistiques, contrôle et vérification dans les limites prévues par la loi. Toutefois, seule la direction pourra avoir accès aux numéros détaillés, permettant d'identifier les interlocuteurs d'un utilisateur, et seulement en cas de différend avec lui.

8- Protection physique de l'équipement

SOPHAL SPA met à votre disposition des équipements (Ordinateur, imprimante, scanner, tablette, smartphone, téléphone, appareil photo…) pour des besoins professionnels et vous encourage à utiliser ces outils pour votre travail qui impose un certain nombre de règles élémentaires dont les deux objectifs sont :

- Protéger le matériel et ses périphériques
- Protéger les données contenues dans ce matériel

1- protéger le matériel

- C'est respecter les règles minimales afin d'éviter le vol, la casse et le vieillissement anticipé du matériel
- C'est maintenir le matériel dans un état de propreté convenable (nettoyage de tâches, poussière …), c'est aussi en prendre soin et signaler tout dysfonctionnement constaté
- Ne pas coller de stickers ou tout type d'adhésif ou autocollants
- Ne pas décoller les étiquettes de codification de matériel (constructeur et SOPHAL)
- Ne pas apporter de modifications au matériel : ajout ou retrait de périphériques ou accessoires
- Ne pas ouvrir le matériel sous quelconque motif (interdit de dévisser le cache)

2- protéger les données contenues dans ce matériel

- S'assurer de la sécurité des traitements
- S'assurer de la préservation des données confidentielles
- S'assurer de l'émission et de la réception de données
- S'assurer de l'intégrité des données
- S'assurer que les données sont enregistrées dans le dossier de l'application ''SOPHAL DRIVE''

Ces raisons qui justifient ces contraintes sont nombreuses :

- maintenir la sécurité du système d'information
- préserver la confidentialité des données de l'entreprise
- maintenir les performances du système
- limiter la prolifération erratique des logiciels
- Eviter l'accès à des droits privatifs

Dans le cadre des matériels remis, chaque utilisateur doit savoir que ces ressources lui sont remises à titre individuel et qu'il est responsable de l'usage qu'il fait de ces ressources dans l'exercice de ses fonctions.

9- Gestion du parc

- Les équipements individuels (Ordinateurs, imprimantes, scanner…) sont sous la responsabilité de l'utilisateur et ne sont utilisés qu'après accord formel de la direction des systèmes d'informations

- Les équipements partagés (Ordinateurs, imprimantes, Photocopieurs...) sont sous la responsabilité de La direction des systèmes d'informations

- Les équipements centraux (serveur, routeur, Switch, armoire réseau...) sont sous la responsabilité de La direction des systèmes d'informations.

- La direction des systèmes d'informations peut être amenée à changer le matériel en fonction de son adéquation au besoin de l'utilisateur. Dans ce cas précis, l'utilisateur est informé par le Helpdesk.

- L'utilisateur de l'équipement informatique se doit d'éteindre son équipement après la fin de ses horaires de travail.

- Aucun équipement ne doit être déplacé sans aviser La direction des systèmes d'informations.

10- Contrôle des activités

La Société se réserve le droit de contrôler le bon usage des règles d'utilisation des outils informatiques de l'entreprise dans le respect de la liberté individuelle de ses collaborateurs.

Les administrateurs qui gèrent les matériels afin d'en assurer le bon fonctionnement et assurer la sécurité du système d'information et faire respecter les règles définies dans la charte, sont investis des pouvoirs suivants :

- Contrôles des applications installées ou téléchargées sur les matériels ;
- Exploitation des traces laissées sur la mémoire des matériels afin de vérifier que le non-respect des règles n'a pas eu pour conséquence l'altération du fonctionnement du matériel ;
- Réinitialisation complète de poste à l'identique du jour où il vous a été remis en cas de force majeure.

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.

11- Information et sanction

La présente charte est partagée sur le portail SOPHAL et communiquée individuellement à chaque salarié par voie électronique.

La direction des systèmes d'informations est à la disposition des salariés pour leur fournir toute information concernant l'utilisation du système d'information, en particulier sur les procédures de sauvegarde et de filtrage. Elle les informe régulièrement sur l'évolution des limites techniques du système d'information et de communication ainsi que sur les menaces susceptibles de peser sur sa sécurité. Chaque utilisateur doit se conformer aux procédures et règles de sécurité édictées par la direction informatique dans le cadre de la présente charte.

Le manquement aux règles et mesures de sécurité décrites dans la présente charte est susceptible d'engager la responsabilité de l'utilisateur et d'entraîner à son encontre des avertissements, des limitations ou suspensions d'utiliser tout ou partie du système d'information et de communication, voire des sanctions disciplinaires, proportionnées à la gravité des faits concernés. Dans ce dernier cas, les procédures prévues dans le règlement intérieur et dans le Code du travail seront appliquées.

Le Représentant de l'entreprise ou son représentant légal, se réserve également le droit d'engager ou de faire engager des poursuites pénales indépendamment des sanctions disciplinaires mises en œuvre, notamment en cas de fraude informatique, de non-respect des droits d'auteur ou de violation du secret des correspondances.

12- Restitution du matériel

Le salarié est tenu de restituer à la société le matériel informatique qui a été mis à sa disposition en fin de la relation de travail.

En cas de perte, vol, casse, détérioration de l'état physique du matériel informatique, L'employé se doit de rembourser la totalité du montant d'achat de l'équipement informatique qui lui est affecté.

13- entré en vigueur

La présente charte est applicable de manière rétroactive pour l'ensemble des utilisateurs du système informatique Et communication de l'entreprise comme cité Ci-dessus.

Elle est annexée au contrat de travail de chaque salarié après signature du dernier.

La présente charte est applicable a compté du : / /2022

M/Mme

La Direction des Systèmes d'Informations