20210906 v3

Charte informatique de l'INMA

La charte informatique définit les règles d'utilisation des technologies de l'information et de la communication au sein de l'entreprise.

Elle vise à renforcer la protection du réseau et, par-là même, veille à ce que les salariés n'abusent pas des outils mis à leur disposition.

D'une manière générale, l'utilisateur doit s'imposer le respect des lois et, notamment, celles relatives aux publications à caractère injurieux, raciste, pornographique, diffamatoire, sur le harcèlement sexuel/moral.

PREAMBULE

L'Institut National de Médecine Agricole met à disposition de ses utilisateurs un système d'information (SI) et des moyens informatiques nécessaires à l'exécution de ses missions et de ses activités.

Celui-ci comprend :

- un réseau informatique
- un réseau téléphonique
- un accès distant en télétravail

Dans le cadre de leurs fonctions, les utilisateurs sont conduits à utiliser les ressources informatiques mises à leur disposition par l'association.

Dans un objectif de transparence, la présente charte définit les règles dans lesquelles ces ressources peuvent être utilisées.

Article 1 : Utilisateurs concernés

La présente charte s'applique à l'ensemble des utilisateurs du système d'information dont notamment :

- les dirigeants et mandataires sociaux
- les salariés
- les intérimaires
- les stagiaires
- les employés de sociétés prestataires
- les visiteurs occasionnels

Il appartient aux salariés de l'organisation de s'assurer de faire accepter la présente charte à toute personne à laquelle ils permettraient l'accès au SI.

Article 2 : Périmètre du système d'information

Le système d'information est composé des ressources suivantes :

- ordinateurs
- téléphones
- réseau informatique (réseau local, wifi, serveurs, routeurs et connectique)
- photocopieur
- logiciels
- données informatisées
- messagerie

Aux fins d'assurer la sécurité informatique du SI, tout matériel connecté au SI de l'entreprise, y compris le matériel personnel des utilisateurs indiqués à l'article 1, est régi par la présente charte.

Article 3 : Règles générales d'utilisation

Le SI doit être utilisé à des fins professionnelles, conformes aux objectifs de l'organisation, sauf exception prévue par les présentes, ou par la loi.

Les utilisateurs ne peuvent en aucun cas utiliser le SI de l'organisation pour se livrer à des activités concurrentes, et/ou susceptibles de porter préjudice à l'organisation de quelque manière que ce soit.

Article 4 : sécurité informatique

L'entreprise met en œuvre une série de moyens pour assurer la sécurité de son système d'information et des données traitées, en particulier des données personnelles. A ce titre elle peut limiter l'accès à certaines ressources.

4.1 Principe général de responsabilité et obligation de prudence

L'utilisateur est responsable des ressources informatiques qui lui sont confiées dans le cadre de ses missions, et doit concourir à leur protection, notamment en faisant preuve de prudence. L'utilisateur doit s'assurer d'utiliser les ressources informatiques mises à sa disposition de manière raisonnable, conformément à ses missions.

4.2 Obligation générale de confidentialité

L'utilisateur s'engage à préserver la confidentialité des informations, et en particulier des données personnelles, traitées sur le SI de l'organisation.

Il s'engage à prendre toutes les précautions utiles pour éviter que ne soient divulguées de son fait, ou du fait de personnes dont il a la responsabilité, ces informations confidentielles.

4.3 Mot de passe

Le contrôle d'accès permet d'identifier toute personne utilisant un ordinateur sur le réseau interne et via vpn. Cette identification permet, à chaque connexion, l'attribution de droits et privilèges propres à chaque utilisateur sur les ressources du système dont il a besoin pour son activité. L'accès aux SI ou aux ressources informatiques mises à disposition est protégé par mot de passe individuel. Ce mot de passe doit être gardé confidentiel par l'utilisateur afin de permettre le contrôle de l'activité de chacun, ce dernier est personnellement responsable de l'utilisation qui peut en être faite. Le mot de passe doit être mémorisé et ne doit pas être écrit sous quelque forme que ce soit. Il ne doit pas être transmis ou confié à un tiers ou être rendu accessible. Le login et le mot de passe doivent être saisis lors de chaque accès au système d'information.

Le mot de passe doit se conformer à la politique de mot de passe édictée conformément aux prescriptions de la CNIL relativement à la protection des données personnelles et notamment :

- être composé d'au moins 12 caractères ;
- ces caractères doivent être une combinaison de
  - caractères alphanumériques,
  - de chiffres,
  - de majuscules,
  - de minuscules,
  - et de caractères spéciaux.

- ne doit pas comporter une suite de chiffres (1234…) ou suite de caractères du clavier
- ne doit pas être identique au login, même en inversant les caractères
- ne doit pas comporter le nom et/ou prénom de l'utilisateur ou de membres de sa famille, la date de naissance, le numéro de téléphone, la marque de la voiture ou toute référence à quelque chose appartenant à l'utilisateur

S'agissant des téléphones mobiles mis à disposition, le code pin de la carte sim doit être personnalisé (les codes « 0000 » et « 1234 » sont à proscrire).

4.4 Verrouillage de sa session

L'utilisateur doit veiller à verrouiller sa session dès lors qu'il quitte son poste de travail.

4.5 Installation de logiciels

L'utilisateur ne doit pas installer, copier, modifier ou détruire de logiciels sur son poste informatique sans l'accord du service informatique en raison notamment du risque de virus informatiques.

4.6 Copie de données informatiques

L'utilisateur doit respecter les procédures définies par l'organisme afin d'encadrer les opérations de copie de données sur des supports amovibles, notamment en obtenant l'accord préalable du supérieur hiérarchique et en respectant les règles de sécurité, afin d'éviter la perte de données (ex : vol de clé usb, perte d'un ordinateur portable contenant d'importantes quantités d'informations confidentielles…).

Article 5 : Modalités d'utilisation des ressources informatiques

Chaque utilisateur doit prendre conscience qu'il est dangereux pour l'entreprise de communiquer à des tiers des informations techniques concernant son matériel.

5.1 Sauvegardes

La mise en œuvre du système de sécurité comporte des dispositifs de sauvegarde des informations et un dispositif miroir destiné à doubler le système en cas de défaillance.

Ceci implique, entre autres, que la suppression par un utilisateur d'un fichier de son disque dur n'est pas absolue et qu'il en reste une copie :

- sur le dispositif de sauvegarde ou miroir ;
- sur le serveur ;
- sur le proxy ;
- sur le firewall (pare-feu) ;
- chez le fournisseur d'accès ;
- Dans Office 365 pour les documents stockés dans OneDrive.

Article 6 : Accès à Internet

L'accès à l'Internet est autorisé au travers du SI, toutefois, pour des raisons de sécurité l'accès à certains sites peut être limité. Le pare-feu vérifie tout le trafic sortant de l'entreprise, aussi bien local que distant. Il vérifie également le trafic entrant constitué de la messagerie électronique, l'échange de fichiers et la navigation sur Internet.

Il détient toutes les traces de l'activité qui transite par lui s'agissant :

- de la navigation sur Internet : sites visités, heures des visites, éléments téléchargés et leur nature (textes, images, vidéos ou logiciels) ;
- des messages envoyés et reçus : expéditeur, destinataire(s), objet, nature de la pièce jointe (et éventuellement texte du message).

Il filtre les URL des sites non autorisés par le principe de la liste noire. Les catégories des sites visés sont les sites diffusant des données de nature pornographique, pédophile, raciste ou incitant à la haine raciale, révisionniste ou contenant des données jugées comme offensantes.

6.1 Utilisation d'Internet à des fins privées

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.

6.2 Contrôles de l'usage

Dans l'hypothèse la plus courante, les contrôles portent sur les sites visités, les durées des connexions et le volume de données téléchargées par un utilisateur.

Article 7 : Email

Chaque employé dispose d'une adresse email pour l'exercice de ses missions.

Par principe, tous les messages envoyés ou reçus sont présumés être envoyés à titre professionnel.
Lors du départ d'un collaborateur, il doit être indiqué au responsable de l'administration du système ce qu'il sera fait des fichiers et courriers électroniques de l'utilisateur.

Les messages électroniques sont conservés sur le serveur sans limite de temps ; une fois supprimés par leur destinataire ils restent récupérables pendant une période de 30 jours.

Les copies de sauvegarde conservent tous les messages au moment où ils passent sur le serveur de messagerie ainsi que les messages supprimés dans les conditions précitées.

7.1 Utilisation privée de la messagerie

L'utilisation du courrier électronique à des fins personnelles est autorisée dans des proportions raisonnables et à la condition de ne pas affecter le trafic normal des messages professionnels. Les messages personnels doivent alors porter la mention "PRIVE" dans l'objet et être classés dans un répertoire "PRIVE" dans la messagerie, pour les messages reçus.

7.2 Contrôle de l'usage

Dans l'hypothèse la plus courante, le contrôle éventuellement mis en œuvre porte sur :

- le nombre des messages échangés par l'utilisateur
- la taille des messages échangés
- le format des pièces jointes

Article 8 : Sanctions

Les manquements aux règles édictées par la présente charte peuvent engager la responsabilité de l'utilisateur et entraîner des sanctions à son encontre (limitation d'usage du SI, sanctions disciplinaires).

Article 9 : Information et entrée en vigueur

La présente charte est ajoutée en annexe du règlement intérieur et communiquée individuellement à chaque employé.

Elle entre en vigueur au **04 janvier 2021**

Signature de l'employeur