

## CHARTRE INFORMATIQUE

### PREAMBULE

Le groupe Eurisole composé des sociétés Soprovise, Normandie Echafaudages, Dongisol et Euromat met à disposition de ses utilisateurs un système d'information et de communication nécessaires à l'exécution de ses missions comprenant notamment un réseau informatique et un réseau téléphonique.

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

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

Cette charte a pour but :

a) de sensibiliser les utilisateurs sur les risques et conséquences pour l'entreprise et eux-mêmes d'une mauvaise utilisation, incontrôlée ou non sécurisée tels que le piratage des informations ou logiciels du groupe, les attaques virales, le préjudice à l'image de l'entreprise, les indiscretions, la détention ou diffusion de données protégées par la loi, la consommation exagérée de ressources.

b) d'informer les utilisateurs

c) de permettre dans le cadre de la loi les contrôles nécessaires de l'usage du système d'information et de communication du groupe.

### Article 1 : Utilisateurs concernés

La présente charte s'applique à l'ensemble des utilisateurs du système d'information et de communication du groupe, quel que soit leur statut, y compris les mandataires sociaux, salariés, intérimaires, stagiaires, employés de sociétés prestataires ou même visiteurs occasionnels.

Il appartient aux utilisateurs 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 fixes ou portables
- smartphones
- réseau informatique (serveurs, routeurs et connectique)
- photocopieurs
- 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 du groupe, sauf exception prévue par les présentes, ou par la loi.

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

## Article 4 : sécurité informatique

Le groupe met en oeuvre 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.

L'usage des ressources informatiques doit se faire dans le respect de la loi et règlements en vigueur. Les utilisateurs s'engagent à respecter les règles de courtoisie et de politesse.

## 4.1 Obligation générale de confidentialité

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

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.

Il doit en toutes circonstances veiller au respect de la législation qui protège notamment les droits de propriété intellectuelle, le secret des correspondances, les données personnelles, les systèmes de traitement automatisé de données, le droit à l'image des personnes, l'exposition des mineurs aux contenus préjudiciables. Il ne doit en aucun cas se livrer à une activité concurrente à celle du groupe ou susceptible de lui causer un quelconque préjudice en utilisant le système d'information et de communication.

## 4.2 Mot de passe

L'accès aux SI ou aux ressources informatiques mises à disposition est protégé par un 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. 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 de plus de 12 caractères ;
- ces caractères doivent être une combinaison de caractères alphanumériques de chiffres,
- de majuscules,
- de minuscules,
- et de caractères spéciaux

## 4.3 Verrouillage de sa session

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

#### 4.4 Installation de logiciels

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

#### 4.5 Copie de données informatiques

L'utilisateur doit respecter les procédures définies par le groupe 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...).

#### 4.6 Utilisation du matériel

L'utilisateur doit veiller à la sécurité du matériel utilisé et à son innocuité.

Il s'engage à en prendre soin. Il informe la direction et le prestataire informatique assurant la maintenance de toute anomalie constatée. Une anomalie peut être l'indice d'une infection par un virus ou autre problème de sécurité.

Il doit respecter les consignes de sécurité du réseau, ne pas changer la configuration de son poste informatique.

Le vol ou le détournement d'un ordinateur et/ou d'un téléphone doivent être signalés aussi rapidement que possible à la direction du groupe.

L'utilisateur doit enregistrer les données sur les serveurs prévus à cet effet et ne stocker sur un support autre que le strict nécessaire.

L'utilisateur doit veiller à l'utilisation professionnelle du matériel permettant une consommation raisonnable des ressources informatiques à disposition.

#### 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.

Il est rappelé que les utilisateurs ne doivent en aucun cas se livrer à une activité illicite ou portant atteinte aux intérêts et/ou à l'image du groupe avec les moyens qu'elle met à leur disposition.

Seuls ont vocation à être consultés les sites internet présentant un lien direct et nécessaire à l'activité professionnelle au regard des fonctions exercées.

En particulier, l'utilisateur ne doit pas se connecter sous peine de dénonciation aux instances judiciaires sur des sites à caractère pornographiques mettant en cause des mineurs.

La transmission ou mise à disposition d'informations ou documents professionnels par le biais d'internet ou de tout moyen de diffusion ou de stockage en ligne est prohibée si elle ne sert pas directement l'activité professionnelle de l'utilisateur.

## **Article 7 : Email**

Chaque employé peut disposer 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.

Par exception, les utilisateurs peuvent utiliser la messagerie à des fins personnelles, dans les limites posées par la loi. 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.

Les correspondances électroniques ne doivent comporter aucun élément illicite, tel que des propos diffamatoires, racistes, haineux, injurieux, contrefaisants ou susceptibles de constituer des actes de concurrence déloyale ou parasitaires.

## **Article 8 : Les téléphones fixes et Smartphones**

L'utilisation des téléphones fixes et smartphones est réservée à des fins professionnelles. Leur utilisation est interdite depuis et/ou vers l'étranger sauf dérogation expresse.

Leur utilisation à des fins personnelles doit rester occasionnelle et discrète.

## Article 8 : Contrôle des activités

Le système d'information et de communication s'appuie sur des fichiers journaux créés en grande partie automatiquement par le prestataire informatique. Ces fichiers sont stockés sur les postes informatiques et 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 y accédant.

L'attention des utilisateurs est attirée sur le fait qu'il est possible de contrôler leur activité et leurs échanges.

## Article 9 : 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 10 : Données personnelles

Les données à caractère personnel des utilisateurs sont traitées conformément aux lois locales applicables en la matière et conformément aux procédures et règles internes de l'entreprise. Les règles internes en matière de protection des données personnelles de l'entreprise sont applicables aux traitements de données à caractère personnel, et garantissent un niveau de protection conforme à celui exigé par la Directive Européenne 95/46/CE.

Chaque utilisateur a le droit d'accéder et de rectifier ses données personnelles en contactant le Data Protection Officer de l'entreprise à : [m.heckenroth@soprovise.fr](mailto:m.heckenroth@soprovise.fr)

## Article 11 : Information et entrée en vigueur

La présente charte est communiquée individuellement à chaque utilisateur, après consultation du CSE.

Elle entre en vigueur au 15 juillet 2020

Le Président

