ANNEXE AU REGLEMENT INTERIEUR

CHARTE INFORMATIQUE – GROUPE GRIM

Version du 09 janvier 2025

Préambule

Le Groupe GRIM 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.

Le Groupe GRIM attache une grande importance à l'efficacité et à la sécurité de son système d'information. L'évolution constante des technologies et des cybermenaces nous oblige à adapter nos pratiques pour garantir la protection des informations sensibles. Il est essentiel que chaque collaborateur ait une connaissance de base en informatique pour assurer une résolution rapide des problèmes courants et maintenir la sécurité des données.

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

Article 1 Objectifs de la Charte Informatique

Cette charte vise à :

- Sensibiliser les collaborateurs à l'importance de la sécurité des données récoltées.
- Encourager l'auto-résolution des problèmes informatiques mineurs.
- Optimiser l'utilisation des ressources de l'équipe informatique.
- Renforcer la capacité des collaborateurs à utiliser efficacement les outils informatiques.
- Intégrer la sécurité informatique dans les pratiques quotidiennes des collaborateurs.

Cette charte a également pour objectif de garantir une utilisation sécurisée et éthique des ressources informatiques de l'entreprise. Elle s'applique à tous les acteurs impliqués dans les activités de l'entreprise, en veillant à respecter les règles de sécurité, de confidentialité, et de responsabilité environnementale.

Le respect de ces directives contribue à maintenir la sécurité des données et à favoriser un environnement de travail respectueux des bonnes pratiques.

Article 2 Utilisateurs concernés

Cette charte s'applique à tous les utilisateurs des ressources informatiques des filiales du Groupe GRIM. Elle est opposable aux personnes suivantes :

- **Dirigeants et mandataires sociaux** : La charte s'applique également aux dirigeants et à toute personne en position de mandataire social au sein de l'entreprise, qui doit en respecter les principes.

- **Salariés** : Tous les collaborateurs de l'entreprise doivent respecter cette charte dans l'exercice de leurs fonctions.
- **Intérimaires et Stagiaires** : Les intérimaires et stagiaires ayant accès aux ressources informatiques de l'entreprise sont également soumis à cette charte.
- **Prestataires externes** : Les collaborateurs des sociétés prestataires, ayant accès aux systèmes informatiques de l'entreprise, doivent se conformer à cette charte.
- **Visiteurs occasionnels** : Toute personne accédant temporairement aux ressources informatiques de l'entreprise (par exemple, un consultant extérieur) doit respecter cette charte dans la mesure où elle leur est applicable.

Article 3 Périmètre du système d'information

Cette charte ne se limite pas aux ordinateurs de bureau ou portables. Elle s'applique à **l'ensemble des ressources informatiques** de l'entreprise, y compris :

- **Smartphones et tablettes** : Toute utilisation des appareils mobiles connectés au système informatique de l'entreprise est soumise à cette charte.
- **Messagerie électronique** : L'utilisation des systèmes de messagerie (internes ou externes) doit se conformer aux règles définies dans cette charte, en particulier en matière de sécurité des données et de respect de la vie privée.
- **Autres équipements connectés** : Tout matériel connecté aux réseaux de l'entreprise (imprimantes, scanners, etc.) doit être utilisé conformément à ces directives.

Article 4 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 5 Compétences Informatiques de Base Requises

Tous les collaborateurs du Groupe GRIM doivent posséder les compétences informatiques suivantes :

- Connaissance des composants de base d'un ordinateur (écran, clavier, souris, unités centrales, etc.).
- Capacité à vérifier les connexions physiques de l'équipement informatique (câbles d'alimentation, câbles HDMI/VGA, etc.).
- Savoir redémarrer un ordinateur ou un périphérique.
- Utilisation des logiciels de base (navigateur internet, suite bureautique, email).

- Compréhension des bases de la sécurité informatique (utilisation de mots de passe forts, reconnaissance des liens frauduleux, etc.).

Article 6 Rôles et Responsabilités

6.1 Pour les Collaborateurs :

- Auto-résolution des problèmes mineurs : Avant de contacter l'équipe informatique, chaque collaborateur doit vérifier les connexions physiques des équipements et tenter de redémarrer l'appareil concerné.

6.2 Pour l'Équipe Informatique

- Support technique avancé : Fournir un support pour les problèmes complexes qui ne peuvent être résolus par les collaborateurs.
- Formation et documentation : Offrir des sessions de formation régulières et maintenir une documentation claire et accessible sur les procédures informatiques de base.
- Maintenance et sécurité : Assurer la maintenance des systèmes informatiques et veiller à la sécurité des données de l'entreprise.

Article 7 Utilisation Responsable du Matériel et Protection des Données de l'Entreprise

Chaque collaborateur du Groupe GRIM est responsable de la bonne utilisation et de l'entretien du matériel informatique mis à sa disposition. Pour garantir la longévité et le bon fonctionnement de l'équipement, il est essentiel de suivre les recommandations suivantes :

- Manipulation avec Précaution : Manipuler les ordinateurs, écrans, claviers, souris et autres périphériques avec soin pour éviter les dommages physiques.
- Maintenir la Propreté : Garder les appareils propres et exempts de poussière. Utiliser des produits de nettoyage appropriés pour les écrans et les claviers.
- Vérification des Connexions : Assurer que tous les câbles et connexions sont correctement branchés et éviter de tirer brusquement sur les câbles pour les débrancher.
- Stockage Sécurisé : Ranger le matériel informatique dans des lieux sûrs et protégés contre les chutes, les chocs et les déversements de liquides.
- Signalement des Dysfonctionnements : Informer immédiatement l'équipe informatique de tout dysfonctionnement ou dommage afin qu'une réparation ou un remplacement puisse être effectué rapidement.

Article 8 Comportements Interdits et Utilisation dans un Cadre Privé

8.1 Téléchargement Illégal

Il est formellement interdit de télécharger ou de distribuer des contenus illégaux via les ressources informatiques de l'entreprise. Ceci inclut, mais ne se limite pas à, des logiciels piratés, des films, de la

musique, ou toute autre forme de contenu protégé par des droits d'auteur sans autorisation. Le non-respect de cette règle peut entraîner des sanctions disciplinaires.

8.2 Limitation à l'Utilisation Personnelle

L'utilisation des ressources informatiques de l'entreprise (ordinateurs, smartphones, tablettes, etc.) à des fins personnelles doit être limitée et ne doit en aucun cas interférer avec les activités professionnelles. L'accès à des sites web personnels pendant les heures de travail doit être restreint afin de garantir l'efficacité et la sécurité des systèmes.

Article 9 Bonnes Pratiques et RSE (Responsabilité Sociétale des Entreprises)

9.1 Sauvegarde Régulière

Afin de prévenir la perte de données importantes, chaque collaborateur doit s'assurer de la sauvegarde régulière de ses fichiers personnels ou professionnels lorsque cela est nécessaire. L'entreprise peut fournir des solutions de sauvegarde, et il est de la responsabilité de chaque utilisateur de les utiliser pour protéger les informations sensibles.

9.2 Empreinte Numérique et Gestion de la Boîte de Réception

L'impact environnemental de l'utilisation des technologies est un sujet de préoccupation croissant. Les collaborateurs doivent être conscients de leur empreinte numérique et veiller à minimiser leur utilisation des ressources, en particulier en nettoyant régulièrement leur boîte de réception, en supprimant les fichiers inutiles et en évitant l'encombrement des serveurs internes.

9.3 Précautions contre les Menaces Numériques (Phishing, Malware, etc.)

Tous les collaborateurs doivent être particulièrement vigilants face aux menaces numériques telles que le phishing, les malwares et autres cyberattaques. Il est essentiel de :

- Ne jamais cliquer sur des liens suspects ou des pièces jointes provenant de sources inconnues.
- Signaler immédiatement toute tentative de phishing à l'équipe informatique.

9.4 Respect de la Déconnexion

Afin de favoriser un équilibre entre vie professionnelle et vie privée, les collaborateurs doivent respecter les horaires de travail et éviter l'envoi de mails professionnels en dehors des heures normales de travail, sauf en cas d'urgence. De plus, il est important de ne pas utiliser la fonction "répondre à tous" sans nécessité, afin de limiter l'impact des communications inutiles.

Article 10 Protection des Données Personnelles

10.1 Respect de la Vie Privée et des Données Personnelles

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.

L’entreprise s’engage à respecter la législation en vigueur relative à la protection des données personnelles (notamment le Règlement Général sur la Protection des Données - RGPD). Tous les collaborateurs doivent être conscients de l’importance de la sécurité des données personnelles, qu'elles soient celles des clients, des collaborateurs ou de toute autre personne liée à l’entreprise.

Deux principes généraux s’appliquent :

- ***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.

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.

- ***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.

La protection des données sensibles de l'entreprise est une priorité absolue. Chaque collaborateur doit s'assurer que les informations confidentielles et les données commerciales ne sont pas divulguées à des tiers non autorisés. Voici les règles à suivre :

- Confidentialité des Informations : Ne jamais partager des informations sensibles de l'entreprise avec des personnes non autorisées, que ce soit à l'intérieur ou à l'extérieur de l'entreprise.
- Sécurisation des Accès : Utiliser des mots de passe forts et uniques pour accéder aux systèmes informatiques et aux bases de données de l'entreprise. Ne pas laisser les mots de passe en évidence (comme sur des Post-it). 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

- Verrouillage des Sessions : Toujours verrouiller son ordinateur ou sa session utilisateur lorsque vous vous éloignez de votre poste de travail, même pour une courte période.
- Protection des Documents Physiques : Garder les documents sensibles dans des tiroirs verrouillés ou des espaces sécurisés. Ne pas laisser de documents confidentiels sur les bureaux ou dans des lieux accessibles au public.
- Utilisation Sécurisée des Outils de Communication : Éviter de discuter des informations sensibles par téléphone ou email non sécurisé. Utiliser les outils de communication sécurisés fournis par l'entreprise.
- Signalement des Violations de Sécurité : Informer immédiatement l'équipe informatique ou le responsable de la sécurité de toute violation suspectée ou avérée de la sécurité des données.

10.2 Collecte et Traitement des Données Personnelles

Les collaborateurs doivent veiller à ne collecter ou traiter les données personnelles que dans le cadre des activités professionnelles et conformément aux règles internes de l'entreprise. Toute collecte ou utilisation des données personnelles à des fins non professionnelles est interdite.

10.3 Stockage et Suppression des Données Personnelles

Les données personnelles doivent être stockées de manière sécurisée et ne doivent être conservées que pendant la durée nécessaire à leur traitement. Les collaborateurs doivent s'assurer de supprimer toute donnée personnelle lorsqu'elle n'est plus nécessaire à des fins professionnelles, en suivant les procédures de l'entreprise en matière de gestion des données.

10.4 Droits des Personnes Concernées

Les collaborateurs doivent respecter les droits des personnes concernées, y compris leur droit à l'accès, à la rectification, à la suppression et à la portabilité des données personnelles. Toute demande relative à ces droits doit être adressée à l'équipe en charge de la protection des données.

Article 11 : Information et entrée en vigueur

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

Elle entrera en vigueur au 1er mars 2025.