SOCIETE GENRERALE MARITIME

CHARTE INFORMATIQUE GEMA V1.0

Avril 2024

PREAMBULE

L'EPE GEMA SPA met à disposition de ses employés un système d'information (SI) et de communication à son activité, comprenant notamment un réseau informatiques et téléphonique mobiles, ainsi que des équipements informatiques nécessaires à l'exécution de ses missions et de ses activités.

Celui-ci comprend :

- Un Réseau informatique (PC bureau, PC portable, Serveur, Imprimante)
- Un réseau téléphonique (Mobiles, Tablette)
- Logiciels (TSA, Illulot, PC Paie, CETIC, Gest. des immobilisations, Sage comptabilité, Sage paie, Bassma)
- Internet
- Intranet (GEMAWEB)

Les employés, dans l'exercice de leurs fonctions, sont conduits à utiliser lesdits équipements informatiques ainsi que les systèmes d'informations et de communication mis à leur disposition.

L'utilisation du système d'information et de communication doit être effectuée exclusivement à des fins professionnelles.

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

Article 1 : Utilisateurs concernés

La présente charte s'applique à l'ensemble des employés utilisateurs du système d'information, à savoir :

- Les Cadres dirigeants
- les salariés (toutes catégories socioprofessionnelles)
- Les consultants
- les apprenants et stagiaires

Article 2 : Périmètre du système d'information

Le système d'information est composé des ressources suivantes :

- ordinateurs portables ou de bureau,
- périphériques (y compris clés USB, disques Rack, …etc),

- réseaux informatiques (serveurs, routeurs/modems, commutateur, WIFI....etc),
- photocopieurs,
- téléphones (fixes et portables) et smartphones,
- tablettes électroniques,
- logiciels,
- fichiers informatiques et bases de données,
- espaces de stockage NAS,
- messagerie,
- connexions internet, intranet.

Aux fins d'assurer la sécurité informatique du SI, tout matériel connecté, 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 la présente charte, ou par la loi.

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

Article 4 : Sécurité informatique et 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.

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 dans le SI.

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

L'accès au Système d'Informations ou aux ressources informatiques mises à la disposition des utilisateurs est protégé par mot de passe. Ce mot de passe doit être gardé confidentiel par l'utilisateur. 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.

4.4 Sécurité de la protection du poste de travail :

L'utilisateur doit respecter soigneusement les consignes de sécurité suivantes :

- Verrouillage de sa session dès qu'il quitte son poste de travail durant les heures de travail.
- Eteindre l'ordinateur pendant les périodes d'inactivité prolongée (nuit, weekend, et congé).
- Scanner tous les supports amovibles connectés au poste de travail avant de les utiliser.
- S'assurer que son poste de travail dispose d'un antivirus, et informer la DOSI de toute alerte de sécurité.
- Ne pas intervenir physiquement sur le matériel (ouvrir les unités centrales, …)

4.5 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 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

L’utilisateur doit prévenir la direction informatique de toute tentative de violation de son compte et, de façon générale, toute anomalie qu'il peut constater.

L’utilisateur doit contribuer à mettre en application les recommandations fournies par la DOSI en termes de sécurité.

L’utilisateur ne doit pas apporter volontairement des perturbations touchant le bon fonctionnement du système informatique et des réseaux (Internes ou externes) de l’entreprise ; par exemple des téléchargements massifs sur le net (Fichiers, Vidéos, Musique,etc).

Article 6 : Accès à Internet

Dans le cadre de leur activité, les utilisateurs peuvent avoir accès à l’internet, toutefois, pour des raisons de sécurité l’accès à certains sites peut être bloqué par la direction informatique.

Il est rappelé que les utilisateurs ne doivent en aucun cas se livrer à une activité illicite portant atteinte aux intérêts de l’entreprise.

Article 7 : Email

Chaque employé peut disposer d'une adresse email professionnelle pour l'exercice de ses missions.

Par principe, tous les messages envoyés ou reçus sont présumés être envoyés à titre professionnel.

L'échange de données professionnelles à travers un autre compte de messagerie autre que celui de l'entreprise est strictement interdit. L'utilisation d'un compte privé n'est tolérée que pour communiquer des informations à des fins personnelles.

Les salariés sont invités à informer la direction informatique de tout dysfonctionnement constaté.

Avant tout envoi, il est impératif de bien vérifier l'identité des destinataires du message et de leur qualité à recevoir les informations transmises. En présence d'informations à caractère confidentiel, de données à caractère personnel ou de données sensibles, ces vérifications doivent être renforcées.

L'utilisateur ne doit pas ouvrir, ni répondre à des messages électroniques tels que spam, messages électroniques répétés, ni les transférer lorsque ceux-ci sont reçus à son insu sur leur messagerie électronique professionnelle et ne présentent aucun rapport avec ses fonctions et ses attributions au sein de l'entreprise. Il s'engage, dans pareil cas, à les détruire immédiatement et à avertir le responsable des systèmes d'information en cas d'abus manifeste de fréquence ou de volume.

Tous les messages envoyés doivent être signés électroniquement.

Article 10 : Comptes d'accès nominatifs

Un compte nominatif est un compte associé directement à un employé au sein de l'entreprise, Il permet de suivre précisément les actions effectuées (reporting) sur le système d'information (Applications/Logiciels) dans le but d'assurer la traçabilité et la sécurité des données de notre système.

Article 11 : Fin de la relation liant l'utilisateur à l'organisme

Lorsque la relation liant l'utilisateur à l'entreprise prend fin, l'utilisateur doit restituer toutes les ressources mises à sa disposition définies à l'article 02. L'entreprise procédera à la suppression de l'ensemble des accès aux ressources informatiques mises à sa disposition (Compte email, Mot de passe, ..etc).

En outre, l'utilisateur devra respecter la discrétion la plus totale sur l'ensemble des informations et des procédés recueillis pendant toute la durée de son emploi au sein de l'entreprise ou après la fin de son contrat. Cette obligation s'appliquera sans limitation de temps.

Article 12 : 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 Système d'Information, sanctions disciplinaires ou judiciaires).

Article 13 : Information et entrée en vigueur

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

Elle entre en vigueur dès sa signature