GSA+
Groupement de Services Assurance

Charte d'utilisation des ressources informatiques, numériques et technologiques

Introduction :

La présente charte définit les conditions d'accès et les règles d'utilisation des moyens informatiques et ressources extérieures via les outils de communication de GSA+ et des groupements.

- Protection des données à caractère personnel

Le Règlement n°2016/679 du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel (RGPD) est entré en vigueur le 25 mai 2018. Le RGPD, complété par la nouvelle Loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, dans sa version consolidée du 14 juin 2018, impose les conditions dans lesquelles des traitements de données à caractère personnel peuvent être réalisés.
Cette réglementation ouvre aux personnes concernées par les traitements un droit d'information, d'accès, de rectification, d'effacement, de portabilité et d'opposition des données enregistrées sur leur compte.

- Délégué à la protection des DPO :

GSA+ a désigné, un salarié, en qualité de Délégué à la Protection des Données à caractère personnel (DPO). Ce dernier a pour mission de veiller au respect des dispositions du RGPD Il a pour rôle de s'assurer de la conformité juridique des traitements.
Le nom et coordonnées du DPO sont inscrites sur le tableau d'affichage direction.

Article 1. Qu'est-ce qu'une charte ?

Une charte s'inscrit dans une démarche d'explication et de sensibilisation quant aux enjeux et aux risques liés aux ressources informatiques numériques et technologiques.

C'est un document qui vise à informer les salariés sur les conditions et modalités de leur utilisation dans le cadre de leur activité professionnelle : navigation à des fins privés, utilisation de la messagerie électronique personnelle, connexion à des forums, connexion à des « chats », téléchargements de logiciels...

Article 2. Objet

Cette charte a pour objectif :

- De faire prendre conscience de l'importance des problèmes liés à la sécurité des informations et de responsabiliser chaque utilisateur, individuellement.
- De mettre en évidence la nécessité, pour la sécurité de tous, que chaque utilisateur respecte ces règles.
- De préciser les principaux droits, devoirs et responsabilités des utilisateurs, en accord avec la législation en vigueur, les règles de déontologie et, le cas échéant, le règlement intérieur.
- De conduire chaque utilisateur à adopter les comportements de sécurité qui sont nécessaires.

Article 3. Engagement et Champs d'application de la charte

La présente charte annexée au Règlement Intérieur :

- ✓ S'applique à tous les salariés fixes ou temporaires, les mandataires, les stagiaires, les employés des entreprises prestataires, faisant usage des matériels informatiques et de communication fournis par l'entreprise.
  Les salariés veillent à faire accepter valablement les règles posées dans la présente Charte à toute personne à laquelle ils permettraient d'accéder au système d'information et de communication.
- ✓ Concerne tous les matériels de communication qui font partie du système d'information de l'entreprise. Ces éléments sont : les ordinateurs fixes ou portables, les périphériques, les réseaux informatiques, les assistants personnels, les photocopieurs, les téléphones, les fichiers, les bases de données, les logiciels, la messagerie intranet et extranet, les différents abonnements à des services interactifs...
- ✓ Les outils personnels des employés sont également soumis à la même règlementation par souci de sécurité sur le réseau.

Le manquement aux règles et mesures de sécurité de la présente charte pourra être passible d'une des sanctions définies au Chapitre III du Règlement Intérieur.

Article 4. Règles de bonne conduite

A - Confidentialité des paramètres 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 (identifiants, mots de passe).
- ✓ Ces paramètres sont personnels à l'utilisateur et doivent rester confidentiels
  Dans la mesure du possible, ils doivent être mémorisés par l'utilisateur et ne pas être conservés, sous quelque forme que ce soit. En tout état de cause, ils ne doivent pas être transmis à des tiers ou aisément accessibles. Ils doivent être saisis par l'utilisateur à chaque accès et ne pas être conservés en mémoire dans le système d'information.
- ✓ Lorsqu'ils sont choisis par l'utilisateur, les paramètres doivent respecter un certain degré de complexité et être modifiés régulièrement.

B - Protection des ressources sous la responsabilité de l'utilisateur

- ✓ L'entreprise 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.
- ✓ 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.
- ✓ En cas d'absence, même temporaire, il est impératif que l'utilisateur verrouille l'accès au matériel qui lui est confié ou à son propre matériel, dès lors que celui-ci contient des informations à caractère professionnel.

- ✓ En cas d'accès au système d'information avec du matériel n'appartenant pas à l'entreprise (assistants personnels, supports amovibles…), il appartient à l'utilisateur de veiller à la sécurité du matériel utilisé et à son innocuité.
- ✓ L'utilisateur ne doit pas installer des logiciels, copier ou installer des fichiers susceptibles de créer des risques de sécurité au sein de l'entreprise, sauf autorisation préalable de son supérieur, lui-même devant en informer le correspondant informatique.
- ✓ L'utilisateur ne doit en aucun cas sous peine de sanction se livrer à une activité concurrente à celle de l'entreprise ou susceptible de lui causer un quelconque préjudice en utilisant le système d'information et de communication.
- ✓ L'utilisateur veille au respect de la confidentialité des informations en sa possession. 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.

C - Accès à Internet

Dans le cadre de leur activité, les utilisateurs sont autorisés à avoir accès à Internet. Pour des raisons de sécurité, l'accès à certains sites peut être limité ou prohibé par l'entreprise. Celle-ci est habilitée à imposer des configurations du navigateur et à restreindre le téléchargement de certains fichiers.

Il est rappelé que les utilisateurs ne doivent en aucun cas se livrer à une activité illicite ou portant atteinte aux intérêts de l'entreprise, y compris sur Internet.

D- Messagerie électronique

La messagerie électronique est un moyen d'amélioration de la communication au sein des entreprises et avec les tiers. Chaque salarié dispose, pour l'exercice de son activité professionnelle, d'une adresse de messagerie électronique.
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 l'entreprise des dysfonctionnements qu'ils constatent dans le dispositif de filtrage.

- ✓ Conseils généraux =

L'attention des utilisateurs est attirée sur le fait qu'un message électronique a la même portée qu'un courrier manuscrit et peut rapidement être communiqué à des tiers. 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/ou de l'utilisateur.

- ✓ Avant tout envoi, il est impératif de vérifier l'identité des destinataires du message et de leur qualité à recevoir communication des informations transmises. En cas d'envoi à une pluralité de destinataires, l'utilisateur doit respecter les dispositions relatives à la lutte contre l'envoi en masse de courriers non sollicités. Il doit également envisager l'opportunité de dissimuler certains destinataires, en les mettant en copie cachée, pour ne pas communiquer leur adresse électronique à l'ensemble des destinataires. En cas d'envoi à une liste de diffusion, il est important de vérifier la liste des abonnés à celle-ci, l'existence d'archives accessibles par le public et les modalités d'abonnement.

✓ Limites techniques
La taille de la messagerie Outlook par utilisateur est de 99 GO, Ce qui permet de conserver les messages directement dans la BAL active.

Les partages de fichiers lourds peuvent se faire via l'outil OneDrive, accessible par identifiant : (adresse mail) et MDP (celui de la session de travail).

✓ Utilisation personnelle de la messagerie
Les messages à caractère personnel sont tolérés, à condition qu'ils soient utilisés avec modération et qu'ils ne perturbent pas le travail. Les messages envoyés doivent être signalés par la mention "Personnel" dans leur objet et être classés dès l'envoi dans un dossier lui-même dénommé "Personnel". Les messages reçus doivent être également classés, dès réception, dans un dossier lui-même dénommé "Personnel". En cas de manquement à ces règles, les messages sont présumés être à caractère professionnel.

E- Contrôle des activités et du contenu

Il est rappelé que pour assurer la sécurité et la fiabilité des systèmes, des contrôles automatiques, généralisés et/ou ponctuels, peuvent être réalisés (Article 15 du Règlement Intérieur).

Il est précisé qu'afin de pouvoir procéder à des investigations visant à déterminer la cause de certains dysfonctionnements, ou en cas de violation délibérée des règles d'usage de la messagerie, il pourra être procédé à la lecture de l'enveloppe (contenant la date et l'heure de l'émission, l'émetteur, le(s) destinataires, l'objet, le nom et le type des pièces jointes) de certains messages.

Dans les cas d'absolue nécessité à la demande de l'entreprise (ce qui devra rester exceptionnel), le contenu d'un message pourra être consulté dans les conditions suivantes :

✓ Accord préalable de l'intéressé

✓ Présence d'une « enveloppe » indiquant que le message n'a manifestement pas un caractère personnel.

De plus, cette lecture ne pourra être effectuée qu'en présence de l'intéressé ou d'un représentant du personnel.

Article 5. Information des salariés

Un exemplaire de la chartre sera remis à chaque salarié lors de son entrée dans l'entreprise.

La présente charte est consultable dans le tableau d'affichage réservé à la Direction ainsi que sur le site Internet GSA+, à la rubrique « Informations GSA+ - Informatique »

Article 6. Entrée en vigueur et modification

La présente charte est applicable à compter du 1er décembre 2020.

Elle a été adoptée après consultation des membres du Comité Social et Economique lors de la réunion du 20 octobre 2020.

Toute modification ultérieure, adjonction ou retrait à la présence charte sera soumise en consultation aux membres du Comité Social et Economique.