Modèle type d'une charte informatique

1. Préambule

L'entreprise ……met à disposition de ses utilisateurs.trices un système d'information (SI) et des moyens informatiques essentiels à l'exécution de leurs missions et activités. Ce système comprend les ressources suivantes :

- Un réseau informatique (serveurs, routeurs et connectique),
- Un réseau téléphonique,
- Des ordinateurs,
- Des photocopieurs,
- Des logiciels,
- Des bases de données informatisées …

La présente charte définit les conditions d'accès et les règles d'utilisation des moyens informatiques et des ressources extérieures via les outils de communication de l'entreprise…….
Elle a également pour objet de sensibiliser les utilisateurs.trices aux risques liés à l'utilisation de ces ressources en termes d'intégrité et de confidentialité des informations traitées. Ces risques imposent le respect de certaines règles de sécurité et de bonne conduite. L'imprudence, la négligence ou la malveillance d'un.e utilisateur.trice peuvent en effet entraîner des conséquences graves de nature à engager sa responsabilité civile et / ou pénale ainsi que celle de l'entreprise…….

2. Article 1. – Les utilisateurs.trices concerné.e.s

Cette charte s'applique à l'ensemble des utilisateurs.trices des ressources informatiques de l'entreprise, qu'ils soient internes ou externes à celle-ci. Cela inclut :

- Les dirigeants ;
- Les salarié.e.s ;
- Les intérimaires,
- Les stagiaires ;
- Les employé.e.s de sociétés prestataires ;
- Les visiteurs occasionnels …

Les salarié.e.s de l'entreprise……sont tenus de faire accepter la présente charte à toute personne à laquelle ils permettraient l'accès au SI.
Le bon fonctionnement des outils et des systèmes d'information suppose le respect des règles législatives et réglementaires, portant notamment sur la sécurité et la conservation des données professionnelles et personnelles.

3. Article 2. – Les règles de sécurité générales

Tout utilisateur.trice s'engage à respecter les règles de sécurité suivantes :

- Signaler au service informatique interne de l'entreprise……toute violation ou tentative de violation suspectée de son compte et de manière générale tout dysfonctionnement,
- Ne pas confier son identifiant/mot de passe,
- Ne pas masquer sa véritable identité,
- Ne pas usurper l'identité d'autrui,

- Ne pas modifier les paramétrages du poste de travail,
- Ne pas installer de logiciels sans autorisation,
- Ne pas copier, modifier, détruire les logiciels propriétés de l'entreprise ……,
- Verrouiller son ordinateur dès qu'il quitte son poste de travail,
- Ne pas accéder, tenter d'accéder, supprimer ou modifier des informations qui ne lui appartiennent pas,
- Toute copie de données sur un support externe est soumise à un accord préalable dans les conditions de cet accord. En outre, il convient de rappeler que les visiteurs ne peuvent avoir accès au Système d'Information de l'entreprise ……sans l'accord préalable du service/responsable informatique interne,
- Les intervenant.e.s extérieurs doivent s'engager à respecter la présente charte.

Les moyens d'authentification :
Un contrôle d'accès aux outils et ressources informatiques est mis en place dans la structure. Chaque utilisateur.trice se voit attribuer une identification personnelle sous forme d'un identifiant et d'un mot de passe. Il.elle est responsable de l'utilisation qui peut en être faite et doit les garder confidentiels.
Il.elle ne doit en aucun cas les communiquer à un tiers non habilité ni être rendu accessible. Si, pour des raisons exceptionnelles et ponctuelles, l'utilisateur.trice se trouve dans l'obligation de communiquer son mot de passe à un tiers, il devra en informer les personnes visées à l'article 4 et le modifier dès que possible.

En cas d'absence du.de la salarié.e, et si l'utilisation des identifiants de connexion aux postes de travail est urgente et nécessaire à la poursuite de l'activité, l'entreprise……est en droit de demander les réclamer.

4. Article 3. – Les règles d'utilisation

Utilisation professionnelle :
Les ressources informatiques mises à la disposition des utilisateurs.tices ainsi que les réseaux permettant d'y accéder doivent être utilisés à des fins professionnelles, conformément aux objectifs de l'entreprise et dans le respect des lois et règlements en vigueur.
Chaque utilisateur s'engage à ne pas utiliser les données en particulier les données à caractère personnel auxquelles il peut accéder à des fins autres que celles prévues dans le cadre de son intervention (ses missions, ses attributions...).
Il est rappelé aux utilisateurs l'importance de cloisonner la partie professionnelle de la partie personnelle de leur(s) équipement(s) ainsi que la possibilité pour l'entreprise d'accéder aux contenus professionnels qui sont stockés sur ledit (lesdits) équipements.

Principe général de responsabilité :
Chaque utilisateur.trice est responsable des ressources auxquelles il a accès et doit concourir à leur protection. Il doit en faire une utilisation prudente et loyale qui ne doit pas mettre en danger la sécurité et/ou l'intégrité du matériel informatique.
Les utilisateurs accédant au SI à distance doivent sécuriser leur connexion Wifi afin d'éviter les intrusions sur le réseau. Les systèmes anti-virus installés sur le matériel des utilisateurs doivent être mis à jour par les utilisateurs, aux fréquences indiquées par lesdits systèmes.

Il est interdit d'utiliser le SI de l'entreprise/l'association pour :

- Porter atteinte aux intérêts de l'entreprise *(sa réputation, la sécurité de son SI, la confidentialité des données…)* ;
- Porter atteinte aux mœurs, à l'honneur, à la vie privée ou à l'intégrité morale d'une personne privée ou publique, interne ou externe à l'entreprise ;
- Visionner, télécharger, détenir et/ou conserver sur le matériel mis à sa disposition par l'entreprise des données *(photos, vidéos...)* à caractère violent, pornographique, pédophile, raciste ou incitant à la haine raciale, révisionniste, offensant ou diffamatoire et, de manière générale, toute donnée à caractère illicite ;
- Se livrer à des activités concurrentes et/ou susceptibles de porter préjudice à l'entreprise.

De manière générale, les utilisateurs.trices sont tenus, sur demande de l'entreprise, de restituer les éléments matériels et de communiquer les informations qu'ils détiennent, lorsqu'elles sont nécessaires à la poursuite de l'activité de l'entreprise. Lorsqu'une personne cesse définitivement d'utiliser le SI de l'entreprise/l'association, elle s'engage à restituer intégralement les données, fichiers informatiques et tout support d'information relatif à ces données.

Confidentialité :
L'utilisateur.trice doit s'interdire d'accéder, de tenter d'accéder à des informations confidentielles et des données à caractère personnel ou encore de les supprimer si cela ne relève pas des missions qui lui ont été confiées.
Chaque utilisateur.trice se doit de préserver la confidentialité des informations auxquelles il a accès via le SI de l'entreprise et en particulier les données personnelles.
L'utilisateur.trice s'engage à prendre toutes les précautions nécessaires pour éviter la divulgation d'informations confidentielles et des données à caractère personnel à des personnes non expressément autorisées à les recevoir et ce, que ladite divulgation soit de son fait ou du fait de personnes dont il a la responsabilité. L'engagement de confidentialité demeure effectif, même lorsque les personnes cessent d'utiliser le SI de l'entreprise.

5. Article 4. – Les personnes chargées de la gestion des ressources informatiques

L'entreprise met en œuvre une série de moyens pour assurer la sécurité de son SI et des données traitées.
Dans l'entreprise, les personnes (la personne) responsable(s) de la gestion des ressources informatiques et par conséquent de la mise en œuvre de la présente charte sont(est) :

- …… …… ……..
- ……... ……... ……*(noms, prénoms, intitulés du poste, téléphone, adresse mail)*

L'utilisateur.trice se doit, au plus vite, de signaler aux personnes (à la personne) susvisée(s) toute violation ou tentative de violation suspectée ou avérée de son compte informatique et de manière générale tout dysfonctionnement.
L'installation de nouveaux périphériques et/ou le téléchargement de programmes par les utilisateurs.trices sur le matériel mis à disposition par l'entreprise doit être préalablement et expressément autorisée par les personnes (la personne) susvisée(s).

6. Article 5. – Le téléphone

Pour préserver la sécurité des personnels et du public, l'entreprise interdit toute communication téléphonique dans les espaces suivants : …….

Aussi, conformément à la législation en vigueur, toute communication téléphonique est proscrite dans un véhicule en circulation appartenant à l'entreprise.
L'utilisation des téléphones de l'entreprise à des fins personnelles par les utilisateurs est autorisée tant qu'elle ne porte pas aux intérêts légitimes de la structure. L'utilisation raisonnable des téléphones à des fins personnelles est autorisée uniquement dans les espaces non accessibles au public.
Les messages écrits, envoyés ou reçus par les utilisateurs.tices, au moyen d'un téléphone mise à disposition par l'entreprise sont présumés professionnels. Si lesdits messages ne sont pas identifiés « personnels » ou « privés », l'entreprise peut les consulter hors de la présence de l'utilisateur.

Un système de gestion des relevés téléphoniques a été mis en place par l'entreprise sur la base de la préservation de son intérêt légitime. Dès lors, pour assurer la sécurité des communications et pour limiter le cas échéant les risques d'abus d'une utilisation trop personnelle des téléphones, l'entreprise conserve le droit, en cas d'utilisation manifestement anormale du téléphone, d'accéder aux relevés téléphoniques individuels.
Les destinataires des données issues de ce contrôle sont…….
La durée de conservation de ces données est de …….

L'entreprise rappelle aux utilisateurs.trices leur droit d'opposition pour motif légitime, leurs droits d'accès et de rectification ainsi que la possibilité d'introduire une réclamation auprès de la CNIL.

7. Article 6. – La messagerie électronique

Les utilisateurs.trices doivent faire une utilisation licite de la messagerie mise à leur disposition. Les propos injurieux, diffamatoires, racistes ou antisémites sont proscrits.

Protection et stockage des informations :
L'entreprise rappelle aux utilisateurs.trices que tout message électronique peut potentiellement être intercepté et/ou lu par un tiers. Dès lors, aucune information confidentielle et/ou stratégique ne doit être transmise par ce moyen sans avoir été préalablement cryptée conformément aux procédures applicables dans l'entreprise.
Les messages électroniques sont conservés sur le serveur de messagerie de l'entreprise pendant …….jours. Lorsque les messages transitent sur le serveur de messagerie, une copie de sauvegarde est réalisée *(même si ces messages sont ensuite supprimés par le destinataire)* et conservée pendant …….jours.

Utilisation privée de la messagerie :
Les messages électroniques envoyés ou reçus sur une messagerie professionnelle sont présumés avoir un caractère professionnel. L'entreprise se réserve le droit de les consulter hors de la présence des utilisateurs. L'utilisation de la messagerie électronique à des fins personnelles est tolérée, dans des proportions raisonnables et à la condition que cela n'affecte pas le trafic normal des messages professionnels. L'utilisation à titre privé de la messagerie professionnelle ne doit pas altérer le bon fonctionnement de l'entreprise, y compris l'intégrité de son réseau informatique ou encore la productivité des salariés.
Les messages personnels doivent alors porter la mention « personnel » ou « privé » dans l'objet ou être classés dans un répertoire nommé « personnel » ou « privé » dans la messagerie.

8. Article 7. – Logiciels

L'utilisateur.trice ne doit pas installer, copier, modifier ou détruire des logiciels ou de progiciels sur le matériel mis à sa disposition par l'entreprise, sans y avoir expressément et au préalable été autorisé par les personnes habilitées en ce sens.
Chaque utilisateur.trice se doit de respecter les restrictions d'utilisation des logiciels et progiciels mis à sa disposition par l'entreprise/l'association.

9. Article 8. – Internet

L'entreprise incite les utilisateurs.trices à prendre conscience des risques que comporte Internet en matière de sécurité et de confidentialité.
Il est donc interdit de :

- Communiquer à des tiers non habilités des informations techniques ou juridiques relatives au matériel de l'entreprise ;
- Accéder à des sites de streaming ou encore à des sites de jeux d'argent ;
- Diffuser sur Internet des informations relatives à l'entreprise sans autorisation expresse et préalable des personnes habilitées visées à l'article 4 ;
- Participer à des forums, même professionnels ;
- Participer à des conversations en ligne (chat).

Il est également interdit de consulter des sites non autorisés par l'entreprise, ainsi que ceux à caractère violent, pornographique, pédophile, raciste ou incitant à la haine raciale, révisionniste, offensant ou diffamatoire et, de manière générale, tout site à caractère illicite.

Utilisation d'Internet à des fins privées
L'utilisation d'Internet à des fins privées est tolérée dans des limites raisonnables, à condition que la navigation n'entrave pas l'accès professionnel.

10. Article 9. – L'outil informatique (ordinateur, tablette…)

Les dossiers et fichiers créés par un.e utilisateur.trice grâce à l'outil informatique mis à sa disposition par l'entreprise sont présumés avoir un caractère professionnel, sauf si l'utilisateur.trice les a identifiés comme « personnels » ou « privés ».
S'ils ne sont pas identifiés comme « personnels » ou « privés », l'entreprise peut avoir accès aux fichiers stockés sur l'outil informatique professionnel hors de la présence de l'utilisateur.trice.

11. Article 10. – Protection des données personnelles

L'entreprise rappelle la nécessité de respecter les règles protectrices en matière de données personnelles, lesquelles implique aussi un certain nombre d'obligations en la matière.
Toute création ou modification de fichier comportant des données à caractère personnel directes ou indirectes doit, préalablement à sa mise en œuvre, être déclarée au.à la délégué.e à la protection des données (DPO), Madame/Monsieur……, qui étudie alors la pertinence des données recueillies, la finalité du fichier, les durées de conservation, les destinataires des données, le moyen d'information des personnes concernées ainsi que les mesures de sécurité à prévoir pour protéger les données.
Le.la DPO veille à la conformité des pratiques de l'entreprise à la loi Informatique et Libertés et au Règlement général sur la protection des données (RGPD).
En cas de non-respect des obligations relatives à la loi informatique et libertés, le.la délégué.e à la protection des données sera informé.e et pourra prendre toutes les mesures nécessaires pour mettre

fin au traitement illégal. Il.elle pourra également en informer le.la responsable hiérarchique de l'utilisateur.trice à l'origine du traitement illégal.

12. Article 11. – Respect de la propriété intellectuelle

L'utilisateur.trice doit s'interdire de faire un usage prohibé du SI notamment en matière de propriété intellectuelle. L'utilisateur.trice ne doit aucunement reproduire, télécharger, copier, diffuser, modifier ou utiliser des logiciels, bases de données, pages web, images, photographies ou autres créations protégées par le droit d'auteur ou tout autre droit lié, sans y avoir au préalable été autorisé par les titulaires de ces droits.

13. Article 12. – Sanctions disciplinaires

Le non-respect des dispositions contenues dans la présente charte entraîne la responsabilité personnelle de l'utilisateur.trice s'il est prouvé que les faits fautifs lui sont personnellement imputables. Les manquements aux règles édictées par la présente charte peuvent entraîner des sanctions à l'encontre de l'utilisateur.trice *(exemples : limitation d'usage du SI, sanction disciplinaire pour un salarié, rupture contractuelle avec un intervenant, exclusion de l'association pour un adhérent ou un bénévole…).*

14. Article 13. – Informations et entrée en vigueur

La présente charte est annexée au règlement intérieur de l'entreprise et communiquée à chaque salarié.e.
Le Comité social et économique a été consulté le ../../…. *(date)*
La charte a été déposée au Conseil des prud'hommes de…. *(lieu)*, le ../../…. *(date)*
Elle entrera en vigueur le ../../…. *(date).*