Modèle de Charte Informatique

PARIS TRONCHET

PARIS TRONCHET vous propose un modèle de charte informatique à personnaliser !

La charte informatique vous permet de définir les règles de bon usage et de bonne utilisation des outils informatiques au sein de votre entreprise.

Ainsi, vous renforcez la protection de votre réseau !

Le modèle est simple d'utilisation :

- Remplacez les annotations en vert par les choix mis en place dans votre entreprise.
- Des exemples sont proposés : n'hésitez pas à vous en inspirer, à en ajouter ou à les supprimer !

PARIS-TRONCHET
mon assureur

CHARTE INFORMATIQUE

[NOM DE L'ENTREPRISE]

PREAMBULE :

L'entreprise/L'association [NOM DE L'ENTREPRISE] 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.

Celui-ci comprend :

- Un réseau informatique
- Un réseau téléphonique
- [LISTER LES AUTRES ACTIFS RÉGIS PAR LA CHARTE]

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.

Article 1 : Utilisateurs concernés

La présente charte s'applique à l'ensemble des utilisateurs du système d'information dont notamment :

- Les dirigeants et mandataires sociaux
- Les salariés
- Les intérimaires
- Les stagiaires
- Les employés de sociétés prestataires
- Les visiteurs occasionnels

Il appartient aux salariés de l'organisation 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
- Téléphones
- Réseau informatique (serveurs, routeurs et connectique)
- Photocopieurs
- Logiciels
- Données informatisées
- Messagerie
- Intranet
- SIRH
- [TRIER ET COMPLETER LES RESSOURCES EN QUESTION]

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.

***ASTUCE** : Il faut définir ici le périmètre des biens qui sont soumis aux règles de la charte. Idéalement il faut également prévoir les règles spécifiques qui régissent l'utilisation du SI par le CSE (droits d'accès éventuels), ou en cas de télétravail.*

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 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 4 : Sécurité informatique

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.

4.1 Obligation générale de confidentialité

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

4.2 Mot de passe

L’accès aux SI ou aux ressources informatiques mises à disposition est protégé par 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

***ASTUCE** : Confirmer la politique de mot de passe avec votre prestataire/responsable informatique interne. On peut également préciser une durée avant mise à jour.*

4.3 Verrouillage de sa session

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 doit effectuer des sauvegardes régulières des fichiers dont il dispose sur le matériel mis à sa disposition. (Détailler ici les procédures de sauvegarde propres à l'entreprise)

4.4 Installation de logiciels

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

4.5 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.

Article 5 : Modalités d'utilisation des ressources informatiques

***ASTUCE** : Décrire ici les modalités d'usage normal des ressources informatiques mises à disposition des utilisateurs - par exemple leur poste de travail, les différentes applications utilisées, la téléphonie mobile, etc.*

Article 6 : Accès à Internet

Dans le cadre de leur activité, les utilisateurs peuvent avoir accès à Internet. Pour des raisons de sécurité, l'accès à certains sites peut être limité ou prohibé par le < SERVICE INFORMATIQUE >. Celui-ci est habilité à imposer des configurations du navigateur et à restreindre le téléchargement de certains fichiers.

La contribution des utilisateurs à des forums de discussion, systèmes de discussion instantanée, blogs, sites est interdite **OU** autorisée, sous réserve d'autorisation préalable du < SERVICE COMMUNICATION > **OU** autorisée. Un tel mode d'expression est susceptible d'engager la responsabilité de l'entreprise, une vigilance renforcée des utilisateurs est donc indispensable.

Choisir votre niveau d'autorisation ici.

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.

Article 7 : Email

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 attribuée par le < SERVICE INFORMATIQUE >.

[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 le < SERVICE INFORMATIQUE > des dysfonctionnements qu'ils constatent dans le dispositif de filtrage.]

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

Les utilisateurs doivent veiller au respect des lois et règlements, et notamment à la protection des droits de propriété intellectuelle et des droits des tiers. Les correspondances électroniques ne doivent comporter aucun élément illicite, tel que des propos diffamatoires, injurieux, contrefaisants ou susceptibles de constituer des actes de concurrence déloyale ou parasitaire.

[La forme des messages professionnels doit respecter les règles définies par le < SERVICE DE COMMUNICATION >, notamment en ce qui concerne la mise en forme et la signature des messages.]

Utilisation personnelle de la messagerie

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.

***ASTUCE** : L'entreprise peut édicter ses règles propres pour procéder à la distinction des messages privés/pro en fonction de son SI. Toutefois il est impossible de supprimer un usage raisonnable à titre privé des outils informatiques mis à disposition par l'employeur, elle doit donc idéalement édicter des règles à ce titre.*

Utilisation de la messagerie pour la communication destinée aux institutions représentatives du personnel

Afin d'éviter l'interception de tout message destiné à une institution représentative du personnel, les messages présentant une telle nature doivent être signalés et classés de la même manière que les messages à caractère personnel.

Article 8 : Procédure de contrôle manuel

En cas de dysfonctionnement constaté par le < SERVICE INFORMATIQUE >, il peut être procédé à un contrôle manuel et à une vérification de toute opération effectuée par un ou plusieurs utilisateurs.

Lorsque le contrôle porte sur les fichiers d'un utilisateur et sauf risque ou événement particulier, le < SERVICE INFORMATIQUE > ne peut ouvrir les fichiers identifiés par le salarié comme personnels contenus sur le disque dur de l'ordinateur mis à sa disposition qu'en présence de ce dernier ou celui-ci dûment appelé. (Préciser les modalités d'appel du salarié)

Le contenu des messages à caractère personnel des utilisateurs, ne peut en aucun cas être contrôlé par le < SERVICE INFORMATIQUE >.

Article 9 : Sanctions

Le manquement aux règles et mesures de sécurité de la présente charte est susceptible d'engager la responsabilité de l'utilisateur et d'entraîner à son encontre des avertissements, des limitations ou suspensions d'utiliser tout ou partie du système d'information et de communication, voire des sanctions disciplinaires, proportionnées à la gravité des faits concernés.

Dès lors qu'une sanction disciplinaire est susceptible d'être prononcée à l'encontre d'un salarié, celui-ci est informé dans un bref délai des faits qui lui sont reprochés, sauf risque ou événement particulier.

Article 10 : Information et entrée en vigueur

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

Elle entre en vigueur au [DATE ENTREE EN VIGUEUR]

[Elle a été adoptée après information et consultation du CSE (Préciser ici les éventuelles autres instances représentatives du personnel).

Fait à [LIEU], le [DATE]

[NOM DU RESPONSABLE DE L'ENTREPRISE]