**Modèle CHARTE INFORMATIQUE**

**Télétravail**

*Une charte informatique permet d’informer les utilisateurs d’un système d’information des règles qui s’imposent quant à l’utilisation de ces ressources. Juridiquement, la charte permet de fixer de manière transparente les conditions dans lesquelles la responsabilité des utilisateurs peut être mise en cause. Corrélativement, elle permet également de protéger la responsabilité des dirigeants (le Dsystème d’information, le CEO). La charte est là pour résoudre de nombreuses problématiques, dont celle épineuse, liée à limitation de l’usage des ressources informatiques de l’organisation à des fins privées par les usagers, qui suscite beaucoup de jurisprudence.*

*Vous trouverez ci-dessous****un modèle type de charte informatique que vous pouvez adapter et réutiliser au sein de votre structure****. Ce modèle pourra vous servir de base de travail et de réflexion pour gérer l’utilisation des ressources informatiques internes.*

La charte informatique doit permettre de gérer un certain nombre de problèmes :

* comment les ressources informatiques peuvent être utilisées par les utilisateurs (et éviter la fraude informatique)
* l’application interne du [RGPD](https://www.donneespersonnelles.fr/rgpd)
* comment gérer la propriété intellectuelle de l’association, et celle de tiers
* les règles internes relatives aux communications électroniques…

Il est important de prévoir également les modalités d’entrée en vigueur et de révision de la charte. Sa mise en oeuvre doit être faite conformément aux procédures prévues en droit du travail (adoption dans le respect de l’art. [1321-4 du code du travail](https://www.legifrance.gouv.fr/affichCodeArticle.do?idArticle=LEGIARTI000006901435&cidTexte=LEGITEXT000006072050), information du salarié, cf. art. [1222-4 du code du travail](https://www.legifrance.gouv.fr/affichCodeArticle.do?idArticle=LEGIARTI000006900861&cidTexte=LEGITEXT000006072050), proportionnalité des mesures en place - [art. 1321-3 du code du travail](https://www.legifrance.gouv.fr/affichCodeArticle.do?idArticle=LEGIARTI000006901434&cidTexte=LEGITEXT000006072050&dateTexte=20090804&oldAction=rechCodeArticle) et information du comité d’association). Pour être opposable, elle doit découler du règlement intérieur de l’organisation.

**PREAMBULE**

L’association / l’association / XXX met à disposition de ses utilisateurs un système d’information (système d’information) 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’association.

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 système d’information.

**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
* …

Aux fins d’assurer la sécurité informatique du système d’information, tout matériel connecté au système d’information de l’association, y compris le matériel personnel des utilisateurs indiqués à l’article 1, est régi par la présente charte.

*NOTE: 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 système d’information par les IRP, l’organisation d’élections ou le télétravail qui peuvent relever de chartes distinctes*

**Article 3 : Règles générales d’utilisation**

Le système d’information 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 système d’information 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’association 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 système d’information 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 système d’information 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](https://www.cnil.fr/fr/authentification-par-mot-de-passe-les-mesures-de-securite-elementaires) 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

*4.3 Verrouillage de sa session*

L’utilisateur doit veiller à verrouiller sa session dès lors qu’il quitte son poste de travail.

*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 (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**

*Note : 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**

L’accès à l’Internet est autorisé au travers du système d’information, toutefois, pour des raisons de sécurité l’accès à certains sites peut être limité.

**Article 7 : Email**

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.

*NOTE: l’association peut édicter ses règles propres pour procéder à la distinction des messages privés/pro en fonction de son système d’information, toutefois il est impossible de supprimer un usage raisonnable à titre privé des outils informatiques mis à disposition par l’employeur (arrêt Nikon : Cass. soc., 2 oct. 2001, Nikon France), elle doit donc nécessairement édicter des règles à ce titre. Attention par contre au contrôle de la messagerie par les institutions représentatives du personnel, car cela peut constituer un délit d’entrave.*

**Article 8 : 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.

**Article 9 : Information et entrée en vigueur**

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

Elle entre en vigueur au \_\_\_\_\_