METHODOLOGIE POUR L'ELABORATION D'UNE CHARTE INFORMATIQUE

Attention : *ce document offre des pistes aux avocats pour élaborer une charte informatique, prenant en compte les recommandations de la Commission nationale de l'Informatique et des Libertés (CNIL) ainsi que de l'Agence nationale de la sécurité des systèmes d'information (ANSSI).*
Ce document n'est en aucun cas un modèle complet de charte informatique à reprendre tel quel, méthode qui se révèlerait contre-productive car chaque cabinet possède un système d'information et de communication ainsi qu'une organisation qui lui sont propres.
Ainsi, ce document nécessite expressément d'être revu et développé par l'avocat.

avocat

Nom du cabinet – Adresse postale

METHODOLOGIE POUR L'ELABORATION D'UNE CHARTE INFORMATIQUE

I/ Conseils de la CNIL

(sources : https://www.cnil.fr/fr/securite-informatique-sensibiliser-les-utilisateurs)

Sensibiliser les utilisateurs (aussi bien internes qu'externes à l'organisme) travaillant avec des données personnelles aux risques liés aux libertés et à la vie privée des personnes, les informer des mesures prises pour traiter ces risques et des conséquences potentielles en cas de manquement.

Cette sensibilisation passe notamment en interne par l'édition d'une charte informatique à laquelle le cabinet doit nécessairement donner une force contraignante (ex. : annexion à un éventuel règlement intérieur).

Cette charte devrait au moins comporter les éléments suivants :

1. **Le rappel des règles de protection des données et les sanctions encourues en cas de non-respect de celles-ci.**

2. **Le champ d'application de la charte, qui inclut notamment :**
- les modalités d'intervention des équipes chargées de la gestion des ressources informatiques de l'organisme
- les moyens d'authentification utilisés par l'organisme et la politique de mots de passe que l'utilisateur doit respecter
- les règles de sécurité auxquelles les utilisateurs doivent se conformer, ce qui doit inclure notamment de :
    - signaler au service informatique interne toute violation ou tentative de violation suspectée de son compte informatique, toute perte ou vol de matériel et, de manière générale, tout dysfonctionnement
    - ne jamais confier son identifiant/mot de passe à un tiers
    - ne pas installer, copier, modifier, détruire des logiciels et leur paramétrage sans autorisation
    - verrouiller son ordinateur dès que l'on quitte son poste de travail
    - ne pas accéder, tenter d'accéder, ou supprimer des informations si cela ne relève pas des tâches incombant à l'utilisateur
    - respecter les procédures préalablement 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

3. **Les modalités d'utilisation des moyens informatiques et de télécommunications mis à disposition comme :**
- le poste de travail
- les équipements nomades (notamment dans le cadre du télétravail)
- les espaces de stockage individuel
- les réseaux locaux
- les conditions d'utilisation des dispositifs personnels
- l'accès à Internet
- la messagerie électronique
- la téléphonie

4. **Les conditions d'administration du système d'information, et l'existence, le cas échéant, de :**
- systèmes automatiques de filtrage
- systèmes automatiques de traçabilité
- systèmes de gestion du poste de travail

5. **Les responsabilités et sanctions encourues en cas de non-respect de la charte.**

II/ Conseils de l'ANSSI

(sources : https://www.ssi.gouv.fr/uploads/2017/06/guide-charte-utilisation-moyens-informatiques-outils-numeriques_anssi.pdf)

1. **L'OJBECTIF :** La charte d'utilisation des moyens informatiques a pour finalité de contribuer à la préservation de la sécurité du système d'information de l'entité et fait de l'utilisateur un acteur essentiel à la réalisation de cet objectif.
   De façon pragmatique, elle permet d'informer l'utilisateur (bien souvent le salarié) sur :
   ■ les usages permis des moyens informatiques mis à sa disposition ;
   ■ les règles de sécurité en vigueur ;
   ■ les mesures de contrôle prises par l'employeur ;
   ■ et les sanctions encourues par l'utilisateur.

   Il est donc primordial que la charte soit aisément lisible et parfaitement compréhensible par chacun des utilisateurs, quel que soit son degré de familiarité avec l'informatique. Au besoin, la charte servira également de support juridique à la collecte de preuves numériques en cas de contentieux.
   L'objectif du document peut être abordé dès le préambule en soulignant le rôle de l'utilisateur à qui incombe une utilisation raisonnée et responsable des ressources informatiques et technologiques de l'entité mises à sa disposition.

2. **DES DÉFINITIONS CLAIRES ET PRÉCISES** : Définir les termes clés du document permet de limiter leur interprétation juridique (administrateur, messagerie électronique, moyens d'authentification, système d'information, utilisateur, etc.).
   Ces définitions peuvent tenir compte de spécificités propres à l'entité et ne pas se contenter d'une explication générique. À titre d'exemple, les moyens d'authentification peuvent différer d'une entité à une autre.

3. **L'OBJET ET SA PORTEE** : La charte doit rappeler ce sur quoi elle porte. Notamment, elle doit exprimer de manière explicite qu'elle a pour objet de préciser les droits et devoirs de l'utilisateur.
   Plusieurs types de charte existent selon l'économie envisagée du document (liste exhaustive ou utilisation raisonnable, grands principes, etc.). Une charte précise sur les droits et devoirs des utilisateurs sera toujours préférable afin d'éviter toute interprétation divergente.
   À noter que, l'administrateur peut faire l'objet d'une partie de la charte, voire d'une charte spécifique. Ses devoirs seront à la mesure des droits souvent étendus qui lui sont confiés. En effet, l'administrateur bénéficie de privilèges élevés qui le conduisent, par conséquent, à porter une responsabilité plus grande. En particulier, l'administrateur est tenu par des obligations de loyauté, de transparence et de confidentialité renforcées.

4. **LES USAGES** : De nombreuses questions sont à envisager lorsque l'entité souhaite fixer les règles d'usage de son système d'information. L'entité met-elle à disposition une messagerie professionnelle ? L'utilisateur dispose-t-il d'une connexion Wi-Fi ? Quels sont les moyens d'authentification prévus par l'entité ? L'utilisateur peut-il avoir recours à des supports amovibles ? Si oui, lesquels ? À quelles fins la navigation sur Internet au moyen des ressources informatiques de l'entité est-elle permise ?
   Autant d'aspects à considérer au travers des étapes suivantes :
   ■ Recenser l'ensemble des besoins auxquels le système d'information doit répondre. Par exemple, le système d'information peut permettre aux employés de gérer les besoins RH, de communiquer en interne ou en externe par messagerie sur des sujets sensibles ou non, ou encore de gérer certains besoins métier dont il s'agit de faire l'inventaire. Cette analyse permettra, in fine, de déterminer les pratiques autorisées en fonction de la sensibilité du système d'information concerné.
   ■ Répertorier l'ensemble des moyens informatiques et outils numériques mis à disposition des utilisateurs. Il peut s'agir d'un poste de travail nomade ou non, d'un ordiphone (smartphone), de supports amovibles (clé USB), d'imprimantes avec ou sans serveur d'impression, de serveurs de partage de fichiers, d'un service de messagerie, d'une application web de gestion RH, ou encore d'une application métier.
   ■ Définir les pratiques autorisées afin de permettre à l'utilisateur d'identifier les règles applicables aux systèmes d'information sur lesquels il intervient. Citons par exemple, le transfert de documents entre postes par clé USB, l'envoi de documents en pièce jointe par mail, ou encore la navigation sur Internet à titre privé.

Les usages doivent définir de façon précise les limites de l'utilisation à titre privé des moyens informatiques, qu'elle soit raisonnable, résiduelle ou interdite.
Il est également fortement déconseillé par l'ANSSI d'utiliser ses outils personnels à des fins professionnelles (et inversement) en raison du manque de contrôle de ces équipements et des risques en matière de sécurité des données. La charte doit impérativement prendre en compte cette pratique largement répandue et définir les mesures que l'entité entend faire appliquer pour préserver la sécurité de son système d'information et protéger les informations personnelles de l'utilisateur.
Le cas échéant, l'entité devra définir les modalités d'exercice du droit à la déconnexion du salarié, conformément à l'article L. 2242-8 du Code du travail.

5. **DEFINIR LES DEVOIRS DE L'UTILISATEUR** : Outre les obligations générales qu'il est bon de rappeler, les devoirs de l'utilisateur découlent directement des usages autorisés définis en amont.
Ces devoirs vont du simple bon sens au respect d'obligations techniques spécifiques qui sont fonction de l'architecture du système d'information de l'entité et des mesures de sécurité qu'elle applique.
Un certain nombre de principes essentiels peuvent être rappelés afin, notamment, de sensibiliser l'utilisateur sur le rôle déterminant qui est le sien dans la protection du système d'information de l'entité. La charte abordera la question du respect par l'utilisateur d'obligations générales telles que la confidentialité, la discrétion, la loyauté ou la vigilance.
Chacun de ces principes essentiels peut, dans un second temps, être décliné par des mesures concrètes plus détaillées dont voici quelques exemples :
■ l'utilisateur ne pourra communiquer d'informations qu'aux personnes ayant besoin d'en connaître ;
■ il devra utiliser les moyens mis à sa disposition pour chiffrer les informations de l'entité.
■ il ne devra en aucun cas transmettre à des tiers les moyens d'authentification qui lui sont fournis par l'entité, lesquels doivent rester personnels et confidentiels ;
■ il devra utiliser des mots de passe qui respectent les bonnes pratiques en vigueur ;
■ il devra appliquer les mesures de sécurité demandées par l'entreprise avant tout import de données d'origine extérieure ;
■ il ne devra jamais mener d'actions engageant la responsabilité juridique ou financière de l'entité en répondant par exemple à un courriel dont l'authenticité n'est pas vérifiée.
L'ensemble des devoirs de l'utilisateur prévu par la charte doit conduire ce dernier à adopter un comportement responsable vis-à-vis du système d'information de l'entité.

6. **LES MESURES DE CONTROLE** : Les mesures de contrôle que l'entité peut mettre en place peuvent être étendues, pourvu qu'elles aient fait l'objet d'une information préalable des utilisateurs (via la charte) et qu'elles soient conformes au droit en vigueur.
La charte devra donc lister les mesures et les conditions dans lesquelles elles sont mises en œuvre (conservation des données de connexion, chiffrement des données, déchiffrement de flux https, gestion stricte des accès, contrôle des messageries professionnelles, etc.).
Ces mesures devront être proportionnées à l'objectif poursuivi.

7. **LES SANCTIONS** : La charte informatique étant un document de portée juridique, elle permettra de fonder les sanctions à l'encontre d'un utilisateur qui ne l'aurait pas respectée.
Il est impératif de prévoir une échelle des sanctions disciplinaires. La sanction doit être proportionnée à la gravité du manquement, le licenciement pour faute apparaissant comme la sanction ultime pour une faute grave commise par l'utilisateur.
D'autres sanctions, de nature civile ou pénale, peuvent être prononcées par les juridictions compétentes.
Si les sanctions disciplinaires découlent directement de la charte informatique, les sanctions pénales peuvent s'appliquer indépendamment de la charte, dès lors qu'une infraction est commise.
Il est utile de rappeler à l'utilisateur que ses actions peuvent avoir des conséquences juridiques lourdes eu égard à des comportements non autorisés. Citons parmi les plus évidents le non-respect de ses obligations, le téléchargement illégal, la consultation de sites à caractère pédopornographique, etc.

8. **S'ASSURER DE L'OPPOSABILITE DE LA CHARTE** : L'opposabilité de la charte nécessite également son acceptation par les utilisateurs (signature de la charte ou annexe au contrat de travail).
Toutefois, afin d'éviter tout refus de l'utilisateur ou renégociation du contrat de travail, la charte peut être annexée au règlement intérieur de l'entité. Dans ce cas, outre la consultation des instances représentatives du personnel lorsqu'elles existent et la communication à l'inspection du travail, la charte devra être portée à la connaissance des utilisateurs (information seule).

III/ Conseils divers

Dans une perspective d'édification d'une charte informatique, il est conseillé d'élaborer non pas un mais deux documents :

- une charte pour les utilisateurs du cabinet qui porte sur les outils bureautiques et leurs usages (cf. supra),
- mais aussi une charte pour les administrateurs réseaux ainsi que les comptes disposant de droits étendus entraînant assez logiquement des dérogations par rapport aux utilisateurs classiques (avec un contrôle de ces droits étendus), si le contexte du cabinet le nécessite évidemment.

La charte informatique doit aussi intégrer les principes fondamentaux régissant les traitements de données personnelles et sensibiliser les utilisateurs en ce sens, notamment sur le fait de ne pas déployer de solutions applicatives ou de créer de nouveaux fichiers informatiques concourant à une nouvelle finalité par exemple de leur côté sans en avertir le responsable de traitement ou le référent RGPD du cabinet (voire le délégué à la protection des données)

Également, la charte informatique ne devrait pas être diffusée aux membres du cabinet sans formalité préalable, sa communication devrait être accompagnée d'une phase de sensibilisation par exemple via un document explicatif simplifié et imagé voire des sessions de formation ou des réunions pour expliquer la démarche et les principaux points d'attention. En effet, la charte doit devenir un véritable processus de responsabilisation de l'ensemble des composantes du cabinet.

Cas particulier du « BYOD » (« Bring your own device ») ou « AVEC » (« Apportez Votre Equipement personnel de Communication ») : il n'est pas toujours aisé en pratique, pour un cabinet, d'interdire totalement l'utilisation des ressources professionnelles via les matériels personnels des membres du cabinet bien que cette pratique soit clairement déconseillée car elle induit mécaniquement un risque plus grand de faille de sécurité et une grande difficulté, voire une impossibilité, pour l'organisme de mettre en œuvre les mesures de sécurité optimale.
La question se pose aussi pour un avocat exerçant à titre individuel qui utiliserait son ordinateur et son téléphone personnels pour traiter les dossiers de ses clients, sans avoir pu forcément doubler ses équipements et ainsi mieux cloisonner les sphères professionnelles et personnelles.
Ainsi, les outils et matériels personnels, c'est-à-dire ceux non fournis par le cabinet, pour les collaborateurs de l'entreprise (ordinateurs, téléphones, tablettes, clés USB...) devraient être empêchés d'accéder aux ressources professionnelles, sauf si l'avocat peut mettre en place un cloisonnement technique complet empêchant une exposition et une compromission des données des clients, salariés, collaborateurs, etc. du cabinet.

IV/ Matrice de charte informatique

Charte individuelle relative à l'usage
des ressources informatiques et des outils numériques

Préambule

Dans le cadre de son activité, le cabinet XXXX met en œuvre un ensemble de ressources informatiques et d'outils numériques professionnels constituant un Système d'information et de communication (SI) dont l'utilisation requiert la vigilance de l'ensemble des Utilisateurs.

Le présent document constitue une Charte individuelle relative à l'usage des ressources informatiques et des outils numériques dont l'objectif est d'engager chaque Utilisateur à appliquer des bonnes pratiques. L'Utilisateur s'engage à alerter les responsables du cabinet en cas de difficulté d'appliquer le contenu de la Charte, de même qu'en cas de survenance de toute situations susceptibles de contrevenir aux principes qui la composent.

Glossaire

Utilisateur : …

Système d'information et de communication : …

… :

1. Utilisateurs concernés par la Charte

La Charte s'applique individuellement à chaque Utilisateur du Système d'information :

- Collaborateurs non-avocats intervenant dans le cadre de la gestion de structure du cabinet ou ayant une activité non avocat au sein de la structure ;
- Avocats statutaires intervenant conduisant une activité juridique dans le cadre de leur inscription au tableau de l'Ordre des avocats ;
- L'ensemble des autres utilisateurs, ayant une activité ou une présence non permanente dans la structure.

Les destinataires de la Charte s'engagent à en faire respecter le contenu par toute personne utilisant le cas échéant le Système d'information sous leur responsabilité.

2. Système d'information concerné par la Charte

La Charte s'applique à l'usage d'un Système d'information et de communication comprenant différentes composantes, notamment :

- Les postes de travail et différents terminaux, les serveurs et les équipements nomades ;
- Les supports et espaces de stockage ;
- Les réseaux informatiques internes et les accès au réseau Internet ;
- Les moyens d'accès à Internet ;
- Les imprimantes, les copieurs multifonction, les équipements médicaux ;
- La messagerie électronique ;
- Les outils de communication (téléphonie, visioconférence, télécopieurs …) ;
- Les différents logiciels ;
- Les bases de données, les différents services en ligne, l'Intranet.

La Charte s'applique également aux dispositifs personnels des Utilisateurs dès lors qu'ils sont connectés au Système d'information commun de la structure.

3. Authentification d'accès au Système d'information

L'Utilisateur doit respecter les exigences d'authentification applicables à l'usage du Système d'information afin de protéger ses composantes contre tout accès et utilisations illégitimes.

Les paramètres d'authentification individuels doivent être maintenus confidentiels. Les mots de passe doivent être créés et renouvelés dans le respect des consignes et ne doivent en aucun cas être transmis à des tiers ou être aisément accessibles ou être conservés en mémoire dans les terminaux.

4. Règles de sécurité

L'Utilisateur doit se conformer aux règles de sécurité liées à l'usage professionnel du Système d'information afin d'assurer la protection des données et la continuité de l'activité.

L'Utilisateur doit notamment veiller à :

- Faciliter et ne pas empêcher les interventions liées à la gestion et au maintien en bon fonctionnement des composantes du Système d'information ;
- Ne pas entraver le fonctionnement du Système d'information ou effectuer des opérations qui pourraient nuire, de manière directe ou indirecte à son intégrité et à la disponibilité ;
- Ne pas connecter ou installer des matériels ou logiciels non préalablement autorisés ;
- Respecter les règles de gestion des sessions utilisateur ainsi que les exigences du nomadisme ;
- Ne pas contourner ou tenter de contourner les procédures et logiciels de sécurité ;
- Ne pas modifier les configurations des composantes du Système d'information ;
- Utiliser uniquement des équipements personnels autorisés respectant les règles de sécurité.

5. Protection des informations

L'Utilisateur doit veiller à la protection des informations et des fichiers, existant sous une forme papier ou numérique, ce qui implique à minima :

- De ne pas procéder à des stockages et impressions d'informations redondants et inutiles, ainsi que sur les éventuels équipements personnels ;
- De ne pas diffuser des informations sensibles ou concernant la vie privée des personnes à l'aide de ressources ou d'outils non sécurisés ;
- De protéger les informations à l'aide d'outils validés par la structure (chiffrement…) en cas d'échange avec des destinataires extérieurs ou d'usage de support mobile ;
- De ne pas effectuer des enregistrements multimédia (vidéo, phoniques, messagerie instantanée, copies d'écrans) à l'insu d'autres utilisateurs ;
- De ne pas modifier ou détruire des informations sans autorisation ;
- De respecter les règles d'utilisation des outils de communication ;
- Garder en toutes circonstances sous son contrôle exclusif et permanent les matériels, documents papier et numérique, au sein et en dehors de la structure.

6. Nomadisme

Outre les règles déjà énoncées, l'Utilisateur nomade veille à :

- Utiliser les ressources, outils et moyens de protection préconisés par la structure ;
- Respecter les exigences de la Chartes liées aux Règles de sécurité, à la Protection des informations, ainsi qu'à l'authentification d'accès au Système d'information.

7. Contrôle de l'application de la Charte, responsabilité et sanctions

Des fichiers de journalisation comportant des traces des usages et des connexions réalisées à partir des équipements de la structure ou d'équipements personnels, au sein de la structure ainsi qu'en cas de connexions à distance, sont susceptibles d'être mis en œuvre aux fins de sécurité du Système d'information et de protection des informations. Les données de journalisation sont conservées pour le seul suivi de l'usage du Système d'information. Les données pouvant être ainsi enregistrées sont notamment les suivantes :

- Date et heure des connexions aux composantes du Système d'information à partir de d'équipements de la structure ou d'équipements personnels ;
- Configuration des équipements et logiciels, changements ou détournements des paramétrages ;
- Activités liées à l'accès ou à l'usage des fichiers et des services ;
- Activité sur les serveurs d'impression ;
- Activité sur les annuaires (espace disque utilisé, statut du compte et du mot de passe, dernière connexion, nombre de fichiers ouverts) ;

Même si les technologies ou les configurations le permettent, l'Utilisateur se garde d'effacer toute trace liée à son activité lors de l'usage du Système d'information.

Le non-respect de la présente Charte engage la responsabilité de l'Utilisateur et pourrait constituer un manquement susceptible de sanction.

avocat
Nom du cabinet – Adresse postale

Je soussigné/e Monsieur/Madame

.

Fait à

le

Nom : Signature :