# Charte informatique

## Préambule

L'utilisation du système d'information et de communication doit être effectuée exclusivement à des fins professionnelles, sauf exception prévue dans la présente charte.

Dans un but de transparence à l'égard des utilisateurs, de promotion d'une utilisation loyale, responsable et sécurisée du système d'information, la présente charte pose les règles relatives à l'utilisation de ces ressources.

Tous les utilisateurs sont tenus de se soumettre aux dispositions de la présente charte, annexée au règlement intérieur.

## 1. Généralités

### 1.1. Objectifs de la charte informatique

La présente charte informatique a pour premier objectif de décrire la position de l'AGCSCDID quant à la politique de la sécurité informatique en son sein.

Le deuxième objectif est d'informer les utilisateurs et managers au sein de l'AGCSCDID des mesures essentielles de sécurité prises d'une part, pour la protection du personnel et, d'autre part, pour la protection du matériel informatique et la préservation de l'intégralité du réseau (sécurité et bon fonctionnement) de l'AGCSCDID qui sont des outils essentiels à son activité économique.

Le troisième objectif réside dans le rappel des règles de protection des données et les sanctions encourues en cas de non-respect de celles-ci.

### 1.2. Domaine d'application de la charte informatique

#### 1. 2.1. Utilisateurs concernés

Sauf mention contraire, la présente charte informatique s'applique à l'ensemble des utilisateurs du système d'information et de communication de l'entreprise, quel que soit leur statut, y compris les mandataires sociaux, salariés, intérimaires, stagiaires, employés de sociétés prestataires, visiteurs occasionnels qui, dans l'exercice de leurs fonctions, sont conduits à accéder aux moyens de communication mis à leur disposition et à les utiliser.

En d'autres termes, elle s'applique également à toute tierce partie avec laquelle l'AGCSCDID collabore dès lors qu'elle a été en mesure de prendre connaissance de la présente charte.

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.

### 1. 2.2. **Système d'information et de communication**

Le système d'information et de communication de l'entreprise est notamment constitué des éléments suivants : ordinateurs (fixes ou portables), périphériques, assistants personnels, réseau informatique (serveurs, routeurs et connectique), photocopieurs, téléphones, logiciels, fichiers, données et bases de données, système de messagerie, intranet, extranet, abonnements à des services interactifs.

La composition du système d'information et de communication est indifférente à la propriété sur les éléments qui le composent.

Pour des raisons de sécurité du réseau, est également considéré comme faisant partie du système d'information et de communication le matériel personnel des salariés connecté au réseau de l'entreprise, ou contenant des informations à caractère professionnel concernant l'entreprise.

### 1.2.3. **Autres accords sur l'utilisation du système d'information**

La présente charte est sans préjudice des accords particuliers pouvant porter sur l'utilisation du système d'information et de communication par les institutions représentatives, l'organisation d'élections par voie électronique ou la mise en télétravail.

L'AGCSCDID met en œuvre un système d'information et de communication nécessaire à son activité, comprenant notamment un réseau informatique et téléphonique.

Les questions relatives à cette charte seront communiquées aux salariés par courriel.

## 1.3. <u>Régime légal</u>

La présente charte informatique constitue une annexe du règlement intérieur.

Tout utilisateur qui agirait à l'encontre des règles et dispositions prévues dans la présente charte pourrait de manière cumulative ou alternative être soumis aux sanctions disciplinaires prévues dans le règlement intérieur et/ou se voir interdire l'accès au réseau et/ou matériel informatique. Il est précisé que la sanction disciplinaire pourrait aller jusqu'au licenciement pour faute grave.

Conformément aux articles L 1321-1 à L 1321-6 et R 1321-1 à R 1321-5 du Code du travail, le projet de la présente charte informatique a été soumis pour avis au délégué du personnel, le « date ».

Le projet de l'employeur et l'avis du représentant du personnel ont été transmis, en deux exemplaires, à l'inspecteur du travail le 26 février 2019. Il est ensuite déposé au

greffe du conseil des prud'hommes de Tours et affiché au sein des antennes de l'AGCSCDID sur le panneau réservé à cet effet et disponible sur le commun.

Elle peut être modifiée, notamment par des notes de service ou tout autre document comportant des obligations générales et permanentes sur les sujets abordés dans la présente charte informatique. Elle peut également être modifiée ou invalidée à la demande de l'inspecteur du travail ou d'un juge à la suite d'un litige.

La présente charte entrera en vigueur *(au moins 2 mois après l'accomplissement de la dernière des formalités de dépôt et de publicité).*

Conformément à la loi n°78-17 du 6 janvier 1978 à l'informatique, aux fichiers et aux libertés, les moyens de contrôle visés au sein de la présente charte ont été déclarés auprès de la CNIL.

## 2. Règles d'accès aux réseaux et/ou aux systèmes informatiques de l'AGCSCDID

### 2.1. L'obligation de signaler les risques de problèmes informatiques

Tout utilisateur appartenant à l'AGCSCDID a l'obligation de rapporter dès qu'il en a connaissance par écrit au Président, Docteur Jean-Pierre BONNEVILLE, par courriel, responsable de la sécurité informatique :

- La perte ou la divulgation d'une information secrète ou confidentielle ;
- Les fuites ou problèmes de sécurité, la constatation de faiblesses ou de menaces ;
- L'utilisation illicite du système informatique de l'AGCSCDID ;
- Le vol des informations ou des biens de l'AGCSCDID.

Que ces actes soient avérés, présumés ou suspectés.

Il est strictement interdit de rapporter un quelconque problème de sécurité ou faiblesse à un tiers n'appartenant pas à l'AGCSCDID, sans l'accord écrit de la direction.

L'AGCSCDID s'engage à protéger toute personne qui, de bonne foi, lui communique les infractions à toute loi ou règlementation applicable, ou l'informe de situations susceptibles de mettre en danger la sécurité et/ou la santé des travailleurs.

### 2.2. 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 être gardés confidentiels. Ils permettent en particulier de contrôler l'activité des utilisateurs.

Dans la mesure du possible, ces paramètres 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. Des consignes de sécurité sont élaborées par la direction afin de recommander les bonnes pratiques en la matière.

Les utilisateurs seront tenus pour responsables de toutes les manipulations effectuées sous leur propre nom d'utilisateur.

Le nom d'utilisateur attribué à une personne ne peut être utilisé que par celle-ci. Les utilisateurs ne peuvent autoriser d'autres personne à utiliser leur propre nom d'utilisateur pour accéder au système informatique, à un programme informatique ou exécuter une manipulation en utilisant le nom d'utilisateur appartenant à autrui.
La direction n'a pas un accès direct aux mots de passe des utilisateurs. A titre exceptionnel, elle peut être amenée à le modifier (pour une intervention technique sur son poste de travail par exemple). Toute modification imprévue concernant les mots de passe sera notifiée, par tous moyens, aux utilisateurs par la direction.

### 2.3. L'accès pour les tierces parties

Seule la direction est habilitée à donner à une tierce partie, l'accès au réseau ou aux systèmes informatiques de l'AGCSCDID.

Il est précisé que les salariés d'entreprise extérieures sous-traitantes, présents dans l'entreprise, sont des tierces parties et qu'ils peuvent avoir accès aux réseaux en vertu des contrats de prestation de services.

Il est interdit à une tierce partie de se connecter au réseau de l'AGCSCDID avec son propre matériel. Exceptionnellement, une telle connexion peut être autorisée par la direction.

Les utilisateurs sont assujettis à une obligation de confidentialité sur les informations qu'ils sont amenés à connaître.

### 2.4. Protection des ressources sous la responsabilité de l'utilisateur

L'AGCSCDID 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.

Il relève également de la responsabilité de l'AGCSCDID de prévoir un plan de continuité du service.

Le Président de l'AGCSCDID est responsable du contrôle du bon fonctionnement du système d'information et de communication. Il veille à l'application des règles de la présente charte en concertation avec les membres du bureau.

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 desdites 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 effectue des sauvegardes régulières des fichiers dont il dispose sur le matériel mis à sa disposition.

L'utilisateur doit éviter d'installer des logiciels, de copier ou d'installer des fichiers susceptibles de créer des risques de sécurité au sein de l'AGCSCDID. Il doit dans tous les cas en alerter le Président.

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. Il ne doit en aucun cas 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.

### 2.5. Les virus

## 3. 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 Président . 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.

La contribution des utilisateurs à des forums de discussion, systèmes de discussion instantanée, blogs, sites, est interdite, sauf autorisation expresse du Président.

Un tel mode d'expression étant susceptible d'engager la responsabilité de l'entreprise, une vigilance renforcée des utilisateurs est donc indispensable.

La contribution des utilisateurs à des forums de discussion, systèmes de discussion instantanée, blogs, sites, est autorisée.

Un tel mode d'expression étant susceptible d'engager la responsabilité de l'entreprise, une vigilance renforcée des utilisateurs est donc indispensable.

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.

## 4. 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 attribuée par la Direction.

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 la Directioon des dysfonctionnements qu'ils constatent dans le dispositif de filtrage.

### 4.1. 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.

L'envoi de messages électroniques à des tiers obéit aux mêmes règles que l'envoi de correspondances postales, en particulier en termes d'organisation hiérarchique. En cas de doute sur l'expéditeur compétent pour envoyer le message, il convient d'en référer à l'autorité hiérarchique.

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.

La vigilance des utilisateurs doit redoubler en présence d'informations à caractère confidentiel. Les messages doivent, dans ce cas, être cryptés, conformément aux recommandations légales en vigueur.

Le risque de retard, de non remise et de suppression automatique des messages électroniques doit être pris en considération pour l'envoi de correspondances importantes. Les messages importants sont envoyés avec accusé réception. Ils doivent, le cas échéant, être doublés par des envois postaux.

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 la Direction, notamment en ce qui concerne la mise en forme et la signature des messages.
La Direction doit être informée de toute absence supérieure à 2 jours, afin de mettre en place un répondeur automatique.

### 4. 2 Limites techniques

Pour des raisons techniques, l'envoi de messages électroniques n'est possible, directement, que vers un nombre limité de destinataires fixé par la direction . Cette limite est susceptible d'être levée temporairement ou définitivement sur demande adressée au Président.

De même, la taille, le nombre et le type des pièces jointes peuvent être limités par 10 MO pour éviter l'engorgement du système de messagerie.
Les messages électroniques sont conservés pendant une durée d'un an . Passé ce délai, ils sont automatiquement archivés.

Si le salarié souhaite conserver des messages au-delà de ce délai, il lui appartient d'en prendre copie.

### 4.3. Utilisation personnelle de la messagerie

Les messages à caractère personnel sont tolérés, à condition de respecter la législation en vigueur, de ne pas perturber et de respecter les principes posés dans la présente charte.

Les messages envoyés doivent être signalés par la mention « Privé » dans leur objet et être classés dès l'envoi dans un dossier lui-même dénommé « Privé ».

Les messages reçus doivent être également classés, dès réception, dans un dossier lui-même dénommé « Privé ».

En cas de manquement à ces règles, les messages sont présumés être à caractère professionnel.

Les utilisateurs sont invités, dans la mesure du possible, à utiliser leur messagerie personnelle *via* un client en ligne pour l'envoi de message à caractère personnel.

### 4.4 Suppression de compte

En cas de départ définitif d'un salarié, son compte de messagerie sera placé sur répondeur pendant une durée de 6 mois.

Passé ce délai, le compte de messagerie sera supprimé. L'entreprise se réserve le droit de consulter les messages à caractère professionnel avant la suppression du compte.

### 4.5 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.

## 5. Données à caractère personnel

La loi n° 78-17 du 6 janvier 1978 modifiée, relative à l'**informatique**, aux fichiers et aux libertés, définit les conditions dans lesquelles des traitements de données personnelles peuvent être opérés. Elle institue au profit des personnes concernées par les traitements des droits que la présente invite à respecter, tant à l'égard des utilisateurs que des tiers.

Des traitements de données automatisés et manuels sont effectués dans le cadre des systèmes de contrôle prévus dans la présente **charte**. Ils sont, en tant que de besoin, déclarés conformément à la loi du 6 janvier 1978 et du RGPD.

## 6. Contrôle des activités

### 6.1. Contrôles automatisés

Le système d'information et de communication s'appuie sur des fichiers journaux (« *logs* »), créés en grande partie automatiquement par les équipements informatiques et de télécommunication. Ces fichiers sont stockés sur les postes informatiques et sur le réseau. Ils permettent d'assurer le bon fonctionnement du système, en protégeant la sécurité des informations de l'entreprise, en détectant des erreurs matérielles ou logicielles et en contrôlant les accès et l'activité des utilisateurs et des tiers accédant au système d'information.

Les utilisateurs sont informés que de multiples traitements sont réalisés afin de surveiller l'activité du système d'information et de communication. Sont notamment surveillées et conservées les données relatives :

- à l'utilisation des logiciels applicatifs, pour contrôler l'accès, les modifications et suppressions de fichiers ;
- aux connexions entrantes et sortantes au réseau interne, à la messagerie et à internet, pour détecter les anomalies liées à l'utilisation de la messagerie et surveiller les tentatives d'intrusion et les activités, telles que la consultation de sites web ou le téléchargement de fichiers.

L'attention des utilisateurs est attirée sur le fait qu'il est ainsi possible de contrôler leur activité et leurs échanges. Des contrôles automatiques et généralisés sont susceptibles d'être effectués pour limiter les dysfonctionnements, dans le respect des règles en vigueur.

### 6.2. Procédure de contrôle manuel

En cas de dysfonctionnement constaté par la Direction , 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, la Direction 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.

Le contenu des messages à caractère personnel des utilisateurs (tels que définis au point 3 des présentes), ne peut en aucun cas être contrôlé par la Direction, à moins d'avoir l'autorisation expresse du collaborateur ou d'être dument habilité à le faire par décision de justice.

## 7. 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.

## 8. Information des salariés

La présente charte est affichée publiquement en annexe du règlement intérieur. Elle est communiquée individuellement à chaque salarié.

La charte informatique est à la disposition des salariés pour leur fournir toute information concernant l'utilisation des NTIC. Il informe les utilisateurs régulièrement sur l'évolution des limites techniques du système d'information et sur les menaces susceptibles de peser sur sa sécurité.

La présente charte et l'ensemble des règles techniques sont disponibles sur l'intranet de l'AGCSCDID.

Des opérations de communication internes seront organisées, de manière régulière, afin d'informer les salariés sur les pratiques d'utilisation des NTIC recommandées.

Chaque utilisateur doit s'informer sur les techniques de sécurité et veiller à maintenir son niveau de connaissance en fonction de l'évolution technologique.

## 9. Formation des salariés

Les salariés seront formés pour appliquer les règles d'utilisation prévues par la présente charte. Ils trouveront notamment une formation en ligne sur l'intranet de l'entreprise, concernant la sécurité de leur poste informatique.

## 10. Entrée en vigueur

La présente charte est applicable à compter du 1er janvier 2019.

Elle a été adoptée après information et consultation du délégué du personnel le 11 décembre 2018.