

Charte informatique d'Antidote Expertise

L'organisme de formation Antidote Expertise, sis 8 rue du Faubourg Poissonnière – 75010 PARIS, enregistré sur le SIREN 528 832 983 au RCS de Paris, met en œuvre un système d'information et de communication nécessaire à son activité, comprenant notamment un réseau informatique et téléphonique. Il est représenté par sa Présidente Directrice générale, Mme Isabelle MADAULE.

Les salariés, dans l'exercice de leurs fonctions, sont amenés à utiliser les moyens de communication mis à leur disposition.

Cette charte a pour but de :

a) Sensibiliser les Utilisateurs sur les risques et conséquences pour l'entreprise et eux-mêmes d'une utilisation mauvaise, incontrôlée ou non-sécurisée, tels que :

- Le piratage des informations ou logiciels de l'Entreprise
- Les attaques virales
- Le préjudice à l'image de l'Entreprise
- Les indiscrétions
- La détention ou diffusion de données protégées par la loi
- La consommation exagérée de ressources

b) Informer formellement l'Utilisateur

c) Permettre, dans le cadre de la loi, les contrôles nécessaires de l'usage du poste de travail.

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 de communication de la Société.

1 Champ d'application

1.1 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, réseau informatique (serveurs, routeurs et connectique), photocopieurs, fax, téléphones, logiciels, services en ligne, fichiers, données et bases de données, système de messagerie, intranet, extranet, abonnements à des services interactifs (ci-après désignés collectivement par le terme « e-Ressources »).

Les e-Ressources de la Société sont fournies aux Utilisateurs en vue d'être utilisées uniquement pour des buts professionnels légitimes et en conformité avec les politiques, procédures, directives et instructions en vigueur dans la Société.

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 Utilisateurs concernés

Sauf mention contraire, la présente charte 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 ou même visiteurs occasionnels.

Les Utilisateurs 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 soit sur l'un des sites de l'Entreprise, soit à partir de tout lieu de travail déporté, notamment en cas de télétravail.

Chaque Utilisateur a la responsabilité de protéger la confidentialité des e-Ressources de la Société.

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. Il ne doit pas modifier les paramètres d'accès au réseau (adresses IP...).

L'Utilisateur ne doit pas s'approprier, modifier ou tenter de décrypter le mot de passe d'un autre Utilisateur.

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.

Lorsqu'ils sont choisis par l'Utilisateur, les paramètres doivent respecter un certain degré de complexité et être modifiés régulièrement. Les mots de passe doivent être conservés de façon strictement confidentielle. Ils ne doivent pas être évidents (pas de surnoms, de noms des enfants, d'initiales ni de mots d'un dictionnaire) et doivent être composés de lettres, numéros et/ou d'une ponctuation (6 caractères minimum).

L'Utilisateur ne doit pas utiliser de comptes autres que ceux auxquels il a légitimement accès.

L'Utilisateur ne doit pas masquer son identité par quelque façon que ce soit.

3 Accès aux données

3.1 Sécurisation des accès

L'entreprise met en œuvre les moyens humains et techniques appropriés pour assurer la sécurité matérielle et logicielle du système d'information et de communication. A ce titre, il lui appartient de limiter les accès aux ressources sensibles et d'acquiescer les droits de propriété intellectuelle ou d'obtenir les autorisations nécessaires à l'utilisation des ressources mises à disposition des Utilisateurs.

Les personnes ayant accès à des données confidentielles du fait de leur activité sur la maintenance des e-ressources sont assujetties à une obligation de confidentialité sur les informations qu'ils sont amenés à connaître. A ce titre, elles peuvent effectuer les opérations de sauvegarde et de duplication nécessaires prévues légalement par l'article L122-6 du code de la propriété intellectuelle.

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.

Les Utilisateurs doivent toujours activer un économiseur d'écran protégé par mot de passe lorsqu'ils laissent un ordinateur sans surveillance. A la fin de la journée, ils doivent sortir du système et mettre les ordinateurs hors tension avant de s'absenter.

En cas d'accès au système d'information avec du matériel n'appartenant pas à l'entreprise, l'Utilisateur doit obtenir une autorisation préalable et écrite (ou par mail) de la Direction.

3.2 Utilisation du matériel

Il appartient à l'Utilisateur de veiller à la sécurité du matériel utilisé et à son innocuité.

L'Utilisateur s'engage à prendre soin du matériel et des locaux informatiques mis à sa disposition. Il informe la Direction et le prestataire informatique assurant la maintenance de toute anomalie constatée. Une anomalie peut être l'indice d'une infection par un virus ou d'un autre problème de sécurité.

Le vol ou le détournement d'un ordinateur doivent être signalés aussi rapidement que possible au supérieur hiérarchique ainsi qu'à la Direction en fournissant le nom de l'Utilisateur directement concerné, le modèle du matériel, la nature des informations contenues, la date du vol, une copie de la déclaration à la police le cas échéant ainsi que toutes autres informations pertinentes relatives au vol.

L'Utilisateur doit enregistrer les données sur les serveurs prévus à cet effet, et ne stocker sur un support autre (ordinateurs fixes ou portables, téléphones mobiles, clés USB...) que le strict nécessaire. Ces fichiers doivent être enregistrés sur les serveurs dès que possible.

L'Utilisateur ne doit pas installer de logiciels, de copier ou d'installer des fichiers susceptibles de créer des risques d'atteinte à la sécurité au sein de l'Entreprise.

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.

L'Utilisateur ne doit ni lire, ni copier, ni tenter de lire ou copier les fichiers d'un autre Utilisateur sans son autorisation. Il ne doit également ni intercepter, ni tenter d'intercepter les communications privées entre Utilisateurs, qu'elles consistent en courrier électronique ou en dialogue direct.

L'Utilisateur ne doit copier aucun logiciel autre que ceux du domaine public libres de droit. Il ne pourra installer sur son poste de travail que les logiciels et/ou fichiers légalement obtenus ou ceux qui sont libres de tout droit.

L'Utilisateur doit veiller à l'utilisation professionnelle du matériel permettant une consommation raisonnable des ressources informatiques à disposition.

4 Utilisation d'internet

Dans le cadre de leur activité, les Utilisateurs ont accès à internet. Pour des raisons de sécurité, l'accès à certains sites peut être limité ou prohibé.

La Direction est habilitée 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 extérieurs à l'activité de l'Entreprise (tels que site communautaire), est interdite.

Les Utilisateurs ne doivent en aucun cas se livrer à une activité illicite ou portant atteinte aux intérêts ou à l'image de l'Entreprise avec les moyens qu'elle met à leur disposition, y compris sur internet.

Seuls ont vocation à être consultés les sites internet présentant un lien direct et nécessaire à l'activité professionnelle au regard des fonctions exercées.

En particulier, l'Utilisateur ne doit pas se connecter, sous peine de dénonciation aux instances judiciaires, sur des sites à caractères pornographiques mettant en cause des mineurs.

La transmission ou mise à disposition d'informations ou documents professionnels, par le biais d'internet ou de tout moyen de diffusion ou de stockage en ligne, est prohibée si elle ne sert pas directement l'activité professionnelle de l'Utilisateur.

5 Messagerie

5.1 Mise à disposition

Chaque Utilisateur dispose, pour l'exercice de son activité professionnelle, d'une adresse de messagerie électronique et d'un accès à la messagerie instantanée.

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

La transmission d'informations ou documents professionnels par courrier électronique ou messagerie instantanée à des fins ne servant pas directement l'activité professionnelle de l'Utilisateur est prohibée.

5.2 Utilisation professionnelle

Avant tout envoi, il est impératif de vérifier l'identité des destinataires du message et de leur qualité à recevoir communication des informations transmises.

L'Utilisateur doit faire preuve de la plus grande correction à l'égard de ses interlocuteurs.

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.

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, racistes, haineux, injurieux, contrefaisants ou susceptibles de constituer des actes de concurrence déloyale ou parasitaire.

Afin d'éviter l'engorgement du système de messagerie, l'Utilisateur doit s'assurer qu'il envoie des pièces avec une taille minimale, et doit utiliser des systèmes alternatifs d'envoi si la ou les pièces jointes est de taille significative et/ou doit être effectué envers un grand nombre de destinataires.

5.3 Utilisation personnelle

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. Ils doivent être utilisés dans une quantité suffisamment raisonnable pour ne pas nuire à l'activité professionnelle de l'Utilisateur ou celle des autres Utilisateurs.

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.

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 suppression 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 Contrôles manuels

En cas de dysfonctionnement constaté, il peut être procédé à un contrôle manuel et à une vérification de toute opération effectuée par un ou plusieurs Utilisateurs par une personne habilitée par la Direction.

Lorsque le contrôle porte sur les fichiers d'un Utilisateur, et sauf risque ou événement particulier, cette personne 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.

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 Utilisateur, 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 communiquée individuellement à chaque salarié.

9 Entrée en vigueur

La présente charte est applicable à compter du 20 mai 2018.