ASSUR MER

Annexe au Règlement Intérieur

Charte d'usage et de sécurité du système d'information de l'entreprise ASSUR MER

ADOPTE EN CONSEIL D'ADMINISTRATION LE 2 NOVEMBRE 2022

ASSUR MER

➔ Table des matières

I. PRINCIPES GÉNÉRAUX

1.1. Préambule

La présente charte a pour objet de réglementer et d'encadrer l'accès et l'utilisation du matériel informatique mis à disposition du personnel de l'entreprise ASSUR MER. Elle a pour but de préciser la responsabilité des utilisateurs en accord avec la législation afin d'instaurer un usage correct des ressources informatiques mises à disposition.

Les règles de la présente charte s'appliquent quelle que soit ma situation de travail : dans les locaux à usage professionnel, en situation de déplacement ou en situation de télétravail.

Enfin, celle-ci ne me dispense pas du respect des réglementations existantes ou à venir.

1.2. Objet et champs d'application

Cette charte s'applique à l'ensemble des moyens de communication, des ressources informatiques, numériques et des utilisateurs.

Ensemble des ressources :

- Application métiers, bureautiques, messagerie, internet, intranet, extranet, VPN
- Données, adresse électronique, comptes réseaux
- Ordinateurs fixes, ordinateurs portables, photocopieurs, clés USB, …
- Téléphones fixes, mobiles, tablettes, fax

Liste non exhaustive qui évoluera en fonction des usages

1.3. Législation

Chaque utilisateur est personnellement responsable de son utilisation des moyens informatiques. A ce titre, il peut voir sa responsabilité individuelle engagée du fait d'une mauvaise utilisation.

Le présent article a pour objectif d'informer les utilisateurs des principaux textes législatifs et réglementaires définissant les droits et les obligations des personnes utilisant les moyens informatiques. Il ne s'agit en aucun cas d'une liste exhaustive.

- Le Code Pénal, notamment ses articles 323-1 à 323-7 relatifs à la fraude informatique.
- Le Code de la propriété intellectuelle qui reconnaît les logiciels comme œuvre de l'esprit et, à ce titre, les protège sans nécessité de dépôt ou d'enregistrement.

- Loi n°78-17 du 6 janvier 1978 modifiée, relative à l'informatique, aux fichiers et aux libertés, qui a notamment pour objet de protéger les libertés individuelles susceptibles d'être menacées par l'emploi de l'informatique et d'encadrer l'utilisation des données à caractère personnel dans les traitements informatiques.
- Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril, dit Règlement Général sur la Protection des Données (RGPD) qui constitue le texte de référence en matière de protection des données à caractère personnel.

II. UTILISATION DES RESSOURCES INFORMATIQUES ET NUMÉRIQUES

Tout utilisateur est responsable du bon usage des équipements mis à sa disposition. Il a aussi la charge, à son niveau, de contribuer à la sécurité générale du Système d'Information. L'utilisation des ressources doit être rationnelle et loyale afin d'éviter leur saturation ou leur détournement à des fins personnelles.

ASSUR MER met à la disposition de ses utilisateurs, différentes ressources tel que définies au chapitre 1.2 selon les modalités suivantes :

- Lorsque l'utilisation d'un code identifiant/mot de passe est requis, son utilisation est strictement personnelle. Il ne peut en aucune manière être cédé, même temporairement même à un tiers (y compris un collègue).
- Tout utilisateur est responsable de l'usage des ressources du système d'information auxquelles il a accès. En tant que contributeur clé à la sécurité générale, il doit utiliser ces ressources de façon rationnelle, loyale et conforme aux obligations légales afin d'en éviter la saturation ou le détournement abusif à des fins personnelles.

La protection du patrimoine informationnel d'ASSUR MER vise avant tout à assurer sa disponibilité, son intégrité, et sa confidentialité. Toute une infrastructure invisible pour l'utilisateur est aussi maintenue en état de fonctionnement.

Elle est constituée de :

- Serveurs hébergeant les fichiers et les applications métier.
- Réseaux locaux sur les différents sites.
- Dispositifs de contrôle et de lutte contre les menaces internes et externes.
- Téléphones fixes et mobiles.
- Dispositifs de sauvegarde.

2.1. Authentification

L'accès aux ressources informatiques repose sur l'utilisation d'un nom de compte (« login » ou identifiant) communiqué à l'utilisateur lors de son arrivée dans l'entreprise une fois la charte approuvée. Un mot de passe est associé à cet identifiant de connexion. Les moyens d'authentification sont personnels et confidentiels. Chaque utilisateur est responsable de l'utilisation qui peut être faite de ses identifiants. Pour des raisons de sécurité évidentes, la DSI se réserve le droit de modifier à tout instant les règles de complexité des mots de passe (nombre de caractère minimum, caractères spéciaux, etc.) et la durée de vie de ces derniers (renouvellement obligatoire tous les 90 jours).

Un mot de passe doit, pour être efficace, comporter 12 caractères alphanumériques comprenant des majuscules, des minuscules, des chiffres et des caractères spéciaux à choisir dans une liste d'au moins 37 caractères spéciaux possibles. Il ne doit pas être, notamment, identique au login, même en inversant les caractères, comporter le nom et/ou prénom de l'utilisateur ou de membres de sa famille, le numéro de téléphone, la marque de la voiture ou toute référence à quelque chose appartenant à l'utilisateur, être un mot ou une liste de mots du dictionnaire ou un nom propre, nom de lieu, être écrit sur un document et être communiqué à un tiers.

Pour certains services des solutions d'authentification forte ou à plusieurs facteurs seront systématiquement mise en place :

- Connexion à Windows : utilisation de la carte à puce contenant vos certificats personnels, l'utilisation de l'identifiant et du mot de passe restera possible.
- Connexion au VPN d'entreprise : utilisation obligatoire du certificat personnel de sécurité.
- Connexion à la messagerie professionnelle : authentification forte avec code de confirmation SMS à saisir.

2.2. Sécurité des données et du réseau

Tout utilisateur s'engage à respecter les règles suivantes :

- Usurpation d'identité : Ne pas tenter de masquer sa véritable identité ou d'usurper l'identité d'une autre personne pour accéder à ses informations.
- Respect des données d'autrui : Ne pas tenter de lire, modifier, copier ou détruire des données autres que les siennes même si celles-ci ne sont pas explicitement protégées exception faite des données diffusées dans des dossiers publics ou partagés clairement identifiés.
- Accès aux postes de travail : Ne pas laisser les ressources accessibles à des tiers en cas d'absence du poste de travail : verrouiller le poste avant de s'absenter même momentanément. En outre, il convient de rappeler que les visiteurs ne sont pas autorisés à accéder au Système d'Information sans accord préalable de la DSI.
- Téléchargement et installation de logiciels : Ne pas télécharger, installer, utiliser ou contourner l'utilisation d'un logiciel pour lequel la DSI n'a pas acquis de licence. Seuls les agents de la DSI sont habilités à installer des logiciels, y compris des logiciels libres.

- Equipements étrangers : Ne pas connecter sans autorisation, à un poste ou au réseau, un équipement étranger à l'entreprise et susceptible de provoquer des dysfonctionnements ou d'introduire des virus informatiques. Toute connexion d'un nouveau matériel doit se faire avec l'autorisation de la DSI.
- Virus : L'utilisateur s'engage à ne pas perturber volontairement le bon fonctionnement des systèmes informatiques et les réseaux, que ce soit par des manipulations anormales du matériel ou par l'introduction de logiciels parasites (virus, chevaux de Troie, ransomware, etc.). Des comportements inhabituels d'un logiciel ou d'un ordinateur tels que l'ouverture intempestive de fenêtres, l'activité inexpliquée du disque dur ou la dégradation importante des performances peuvent traduire la présence d'n logiciel parasite : contacter la DSI.
- Antivirus : La DSI installe sur chaque ordinateur un logiciel destiné à vous protéger des programmes malveillants. Il est absolument interdit de désinstaller cet outil ou de tenter d'en modifier le paramétrage. Le logiciel antivirus vous avertit en cas de détection de virus : vous devez en informer la DSI immédiatement.

2.3. Partage des ressources

Les utilisateurs disposent d'espace de stockage sur les réseaux informatiques : bases de données, serveurs de messagerie, serveurs de fichiers, etc. Les documents traités par les services et les données traitées par les différents progiciels sont stockés sur des serveurs accessibles via le réseau local ou des réseaux interconnectés.

L'accès à ces serveurs est limité par des droits donnés par l'administrateur à un utilisateur suite à la demande écrite de son responsable de service ou au responsable fonctionnel d'une application métier.

Ces autorisations sont liées à un compte utilisateur nominatif.

Ces ressources étant partagées, l'utilisation abusive par un utilisateur d'espace ou de connexions pénalise l'ensemble des autres utilisateurs.

La DSI assure la sauvegarde de toutes les informations stockées sur les ressources prévues à cet effet et uniquement celles-ci. Ainsi, la sauvegarde des fichiers stockés sur le poste de travail de l'utilisateur est de la responsabilité de ce dernier. En outre, il est rappelé que la sauvegarde de fichiers professionnels sur des supports personnels ou sur des sites extérieurs à l'entreprise est strictement prohibée.

Il est impératif :

- de ne conserver sur les serveurs mis à votre disposition que les données directement liées à l'activité professionnelle.
- de ne pas utiliser, même temporairement, l'infrastructure informatique d'ASSUR MER pour copier transférer ou traiter des données personnelles. Toutes les données identifiées comme privées ou personnelles sur ces espaces sont susceptibles d'être purement et simplement supprimées sans préavis. Si des fichiers personnels devaient être stockés, ils le seront dans le répertoire « Mes documents » de son poste de travail avec la mention « perso » ou « personnel » figurant explicitement dans le nom du dossier correspondant.

III. MATERIEL MIS A DISPOSITION

L'attribution de moyens de communication ou d'outils informatiques dépend de ma fonction et de mes missions. Ces moyens (ordinateur de bureau, PC portable, tablette, téléphone fixe, mobile intelligent, …) évoluent avec le temps et les technologies.

Je suis personnellement responsable de ces équipements et de leur restitution. Leur usage est professionnel ; il doit rester conforme aux règles définies par la DSI. Je suis responsable de l'usage des ressources informatiques et du réseau auxquels j'ai accès. Je dois être rationnel dans l'utilisation de ces ressources afin d'éviter la saturation ou le détournement à des fins non professionnelles.

Les matériels informatiques et téléphoniques qui me sont confiés sont fragiles, je dois prendre soin d'eux.

Seuls les agents de la DSI sont autorisés à intervenir sur le matériel informatique ou télécom tant physiquement que logiciellement.

3.1. Utilisation professionnelle

L'utilisation des équipements informatiques et téléphoniques de l'entreprise est limitée à un usage professionnel. L'utilisation à titre privé est tolérée, mais doit demeurer très occasionnelle et ne doit pas être en contradiction avec les principes déontologiques rappelés dans la charte.

3.2. Equipement personnel

Pour des raisons de sécurité du Système d'Information, ASSUR MER proscrit formellement tout type d'équipement personnel sur le réseau de l'entreprise. La DSI n'assure aucun support ni aucune maintenance sur les équipements personnels.

IV. INTERNET

Comme pour l'ensemble des moyens mis à ma disposition, Internet est destiné à un usage professionnel.

L'usage privé doit rester accessoire. Tout abus sera sanctionné. Je dois faire preuve, sur Internet comme dans l'exercice de mes fonctions, de professionnalisme, de discernement, de bon sens, de courtoisie et de prudence.

4.1. Téléchargements

Les téléchargements peuvent sérieusement perturber le fonctionnement du Système d'Information (accès ralentis pour les autres utilisateurs, impact possible sur l'utilisation d'applications métiers, conséquences sur les espaces disques, incompatibilité avec d'autres logiciels, introduction de virus, etc.). Par ailleurs, les données circulant sur Internet peuvent être réglementées en termes d'utilisation ou être protégées par un droit de propriété intellectuelle.

Un téléchargement est un vecteur de transmissions important de virus ; en cas d'incident, je contacte la DSI.

4.2. Filtrage internet

L'accès Internet est un outil professionnel. Dans ce cadre, ASSUR MER permet seulement les accès aux sites liés à mes missions.

Seuls ont vocation à être consultés les sites Internet ayant un lien direct et nécessaire avec mon activité professionnelle et présentant une utilité au regard des fonctions à exercer.

Une consultation ponctuelle et raisonnable des sites Internet dont le contenu n'est pas contraire à l'ordre public et qui ne mettrait pas en cause les intérêts et les règles éthiques et déontologiques de l'entreprise est tolérée.

La loi interdit l'accès à des sites de nature diffamatoire, discriminatoire, raciste, sexiste, révisionniste, pédophile ou incitant à la violence ou à la haine raciale ; en cas d'agissements de cette nature, ma responsabilité pénale personnelle peut être engagée, indépendamment des sanctions disciplinaires qui pourraient être prises.

La DSI contrôle et limite les accès aux sites qui sont classifiés par catégorie. Je peux demander le droit d'accès à un site bloqué en contactant le support technique de la DSI et en justifiant le besoin professionnel. Si j'ai besoin d'un logiciel ou d'une mise à jour spécifique, je contacte la DSI.

V. REGLES D'UTILISATION DE LA MESSAGERIE ELECTRONIQUE

La messagerie est destinée à un usage professionnel.

Je ne dois pas tenter de lire ou copier les courriels d'un autre utilisateur sans son autorisation expresse. Je m'abstiens également de toute tentative d'interception sans autorisation de courriels entre utilisateurs.

L'utilisation de la messagerie à des fins privées, lorsqu'elle est rendue nécessaire par les impératifs de la vie courante et familiale, est tolérée si elle n'affecte pas le trafic normal de la messagerie professionnelle. Par défaut, tout courriel reçu ou envoyé à partir du poste de travail mis à ma disposition par l'entreprise est considéré comme professionnel.

En cas d'absence prolongée, et pour les besoins du service, ASSUR MER peut accéder à ma messagerie. Cet accès peut être ouvert à mon responsable hiérarchique, après avis du délégué à la protection des données (DPO).

Seuls mes courriels privés identifiés comme tels sont protégés au titre du respect de ma vie privée et du secret de mes correspondances : ASSUR MER ne peut pas accéder à mes courriels privés, sauf dans le cadre d'une procédure d'enquête judiciaire ou sur autorisation d'un juge.

Pour que mes courriels privés soient protégés, je dois les identifier comme tels, par exemple : - En précisant dans leur objet « Personnel » ou « Privé », - En les stockant dans un répertoire intitulé « Personnel » ou « Privé ».

VI. DROIT A LA DECONNEXION

Je dispose d'un « droit à la déconnexion », c'est-à-dire de la possibilité de ne pas me connecter aux outils numériques de l'entreprise (outils collaboratifs, applications métier) et de ne pas être contacté par mon employeur en-dehors de mon temps de travail (téléphone, courriel). Ce droit s'exerce en dehors des heures correspondant à ma formule de travail hebdomadaire, définie avec ma hiérarchie.

VII. TELETRAVAIL

Afin de faciliter l'accès des salariés qui le souhaitent au télétravail, un document spécifique au télétravail définira ses modalités de mise en œuvre :

- Les activités éligibles au télétravail,
- Le temps possible de télétravail,
- Les règles à respecter en matière de sécurité des systèmes d'information et de protection des données, de temps de travail, de sécurité et de protection de la santé.
- Les modalités de contrôle et de comptabilisation du temps de travail ;
- Les modalités de prise en charge, par l'employeur, des coûts découlant directement de l'exercice du télétravail, notamment ceux des matériels, logiciels, abonnements, communications et outils ainsi que de la maintenance de ceux-ci,
- Les modalités de formation aux équipements et outils nécessaires à l'exercice du télétravail.

VIII. TRAÇABILITE DES CONNEXIONS

ASSUR MER trace tous les accès au système d'information à des fins de sécurité, de statistique et de maintenance. Lorsqu'un poste de travail accède au Système d'Information, les données suivantes sont enregistrées :

- L'identifiant de l'utilisateur,
- La date et l'heure de connexion,
- L'adresse IP et le nom du poste de travail,
- Les applications auxquelles il a accédé,
- Le nombre de sessions ouvertes par l'utilisateur,
- La durée totale de l'activité de l'utilisateur,
- Durée de conservation : 36 mois maximum.

Lorsqu'un poste de travail accède à Internet, depuis les locaux professionnels ou via un VPN, le serveur de connexion enregistre :

- L'identifiant de l'utilisateur,
- L'adresse du site web visité,
- Le nombre d'accès à ce site par l'utilisateur,
- Le nombre de sessions ouvertes par l'utilisateur,
- La durée totale de l'activité de l'utilisateur,
- Le volume des données transmises par l'utilisateur,
- L'adresse IP et le nom de l'équipement utilisé,
- Les dates et heures des accès,
- Durée de conservation : 36 mois maximum.

IX. PROTECTION DES DONNEES PERSONNELLES

ASSUR MER, qui est mon employeur, collecte et traite des données à caractère personnel me concernant.

Je dispose, dans certaines conditions, de droits sur ces données à caractère personnel : accès, rectification, effacement, limitation, portabilité et opposition.

Pour tout renseignement sur les modalités d'exercice de ces droits, je peux saisir le délégué à la protection des données (DPO – Data Protection Officer) d'ASSUR MER (dpo@assur-mer.fr).

Je peux également introduire une réclamation auprès de la CNIL (www.cnil.fr).

CONTACTS

Pour contacter l'assistance informatique de DSI :

- Ouverture d'un ticket sur GLPI : http://helpdesk.intra.assur-mer
- Par courriel : dsi-helpdesk@assur-mer.fr
- Par téléphone : au poste 8978 ou 04.91.45.89.78