CHARTE D'UTILISATION DES RESSOURCES INFORMATIQUES DE LA SOCIETE LODI

Annexe n°1 du Règlement Intérieur

Sommaire

1. INTRODUCTION 2
2. RESPONSABILITES 2
3. MISE A DISPOSITION ET UTILISATION DES MOYENS MATERIELS INFORMATIQUES 2
Article A - Propriété des outils et données 2
Article B - Utilisation du matériel à disposition 3
Article C - Règles de protection du matériel 3
Article D - Télétravail 4
4. SECURITE DES RESEAUX ET ACCES 4
Article A - Gestion des accès 4
Article B - Règles de confidentialité 5
Article C - Gestion des départs 5
Article D - Virus, vers et autres programmes malveillants 6
Article E - Protection contre les attaques de phishing 6
5. REGLES D'UTILISATION D'INTERNET ET DE LA MESSAGERIE 7
Article A - Utilisation d'internet 7
Article B - Utilisation de la messagerie 8
Article C - Secret des correspondances 9
6. CONTROLE DE L'USAGE DES SYSTEMES D'INFORMATION (S.I.) 9
Article A - Objectifs 9
Article B - Fichiers de trace 10
Article C - Interventions de la société LODI 11
Article D - Contrôle de la société LODI 11
Article E - Protection des informations personnelles 12
Article F - Portée disciplinaire 13
7. TEXTES DE REFERENCE 13
8. ENTREE EN VIGUEUR 13

1. INTRODUCTION

Les Systèmes d'Information (SI) sont des outils informatiques modernes, qui, utilisés avec rigueur et précision soutiennent nos activités et nous permettent d'être chaque jour plus efficaces, dans nos communications internes mais aussi avec nos partenaires, prestataires et adhérents.

Cette charte présente les conditions d'utilisation du Système d'Information de la société LODI. A cette fin, elle a pour objet de préciser les droits, les devoirs et les responsabilités de chacun, en accord avec la législation en vigueur et la politique de sécurité du système d'information de la société LODI.

Le terme « Ressources Informatiques » désigne l'ensemble des moyens informatiques mis à disposition de manière directe ou indirecte par la société LODI (poste de travail, messagerie, applications, systèmes, bases de données, serveurs, réseau, Internet...).

2. RESPONSABILITES

La société LODI met à disposition des utilisateurs les ressources informatiques nécessaires à l'exécution de leurs missions et doit veiller à ce que leur utilisation demeure conforme aux lois et règlements en vigueur. Sa responsabilité tant civile que pénale pouvant être mise en cause en cas d'utilisation abusive ou répréhensible, elle met en place les dispositifs permettant de prévenir ce genre de situations.

La présente charte est annexée au Règlement Intérieur dont elle fait intégralement partie. Elle en a donc la même valeur et la même portée.

En conséquence, le non-respect des dispositions établies par le présent document est passible de sanctions disciplinaires, qui resteront en tout état en cause proportionnées à la gravité des infractions commises.

Elle s'applique à l'ensemble des personnels de la société LODI et des utilisateurs, permanents ou temporaires, tous statuts confondus (salariés, intérimaires, stagiaires, salariés d'entreprises extérieures, etc), ayant accès aux ressources du Système d'Information de la société LODI, désignés dans cette charte sous le terme « Utilisateurs ».

La société LODI garantit la disponibilité des données, l'efficience et la qualité des systèmes d'information mis à disposition des utilisateurs. Elle met en œuvre les dispositions permettant de maintenir un service de qualité à l'ensemble des utilisateurs avec des ressources optimisées.

La société LODI veille à la protection des informations et des données qui transitent, sont stockées ou proviennent des Systèmes d'Information ainsi que des outils et systèmes qui composent les Systèmes d'Information.

3. MISE A DISPOSITION ET UTILISATION DES MOYENS MATERIELS INFORMATIQUES

Article A - Propriété des outils et données

L'ensemble des matériels, outils et dispositifs mis à disposition de l'utilisateur demeure la propriété de la société LODI. Les données et informations créées ou disponibles à partir des systèmes d'information gérés par la société LODI demeurent la propriété de la société LODI. Les droits d'accès des utilisateurs ne peuvent leur conférer des droits de

propriété sur ces données. Le matériel fournit par le service informatique prend en compte les demandes « terrain » mais doit aussi répondre au cahier des charges du service informatique, ce dernier se réserve donc le droit de refuser toute demande spécifique.

Article B - Utilisation du matériel à disposition

Les Ressources Informatiques sont mises à la disposition de l'Utilisateur exclusivement pour un usage professionnel, en vue de la réalisation de ses missions. Néanmoins, la société LODI tolère une utilisation limitée des Ressources Informatiques à des fins personnelles, dans le cadre des nécessités de la vie courante dès lors que cet usage reste ponctuel, raisonnable et ne perturbe pas le bon fonctionnement du Système d'Information, et plus généralement la productivité et la bonne exécution des missions.

Les Utilisateurs s'engagent à identifier clairement les données et fichiers relatifs à leur utilisation personnelle notamment en les stockant dans un dossier intitulé « **Personnel** ». Il est strictement interdit de dissimuler des données à caractère professionnel en les dénommant « Personnel » ou en les stockant dans un dossier «Personnel ».

Article C - Règles de protection du matériel

Chaque Utilisateur est responsable de l'utilisation des Ressources Informatiques et s'engage à ne pas les utiliser dans des conditions pouvant porter atteinte à la sécurité et à l'intégrité du système d'information. Il devra notamment respecter les règles suivantes sans que cette liste ne puisse être considérée comme exhaustive :

- L'Utilisateur s'engage à ne pas modifier sans accord préalable de la société LODI la configuration et le paramétrage des matériels et logiciels mis à sa disposition ou de tout autre matériel ou logiciel accessible depuis les Systèmes d'Information.
- L'Utilisateur s'engage à ne pas connecter au réseau des équipements autres que ceux autorisés expressément par la société LODI
- L'Utilisateur s'engage à limiter l'usage des supports amovibles de type clé USB, CDROM. Il veillera à réaliser une analyse anti-virus du support avant toute utilisation des données.
- L'Utilisateur s'engage à ne pas sortir de données appartenant à la société LODI, notamment des données clients, par quelque moyen que ce soit (support amovible, messagerie, etc...), et à protéger l'accès aux informations à l'aide des outils à sa disposition (protection par mot de passe en particulier).
- L'Utilisateur s'engage à mettre en œuvre toutes les mesures à sa disposition pour garantir la protection des matériels qui lui ont été confiés, en particulier contre les dégradations, le vol ou l'usure prématurée.

Il est strictement interdit de porter atteinte aux droits d'auteur, liés aux images, textes, vidéos, logiciels, etc en vigueur ou de se rendre coupable de contrefaçon, en particulier en faisant une copie d'un document ou d'un logiciel commercial pour quelque usage que ce soit. De même, il est interdit de transgresser le cadre juridique lié à la propriété intellectuelle. Nous vous rappelons que ces agissements sont passibles de sanctions pénales.

Nous rappelons que les Utilisateurs d'outils « nomades » (ordinateurs ou matériels portables) doivent s'assurer que leur outil est toujours en lieu sûr. L'attention des Utilisateurs est attirée sur le fait qu'il est interdit de laisser seul un outil « nomade » ou portable dans un véhicule.

Article D - Télétravail

Le télétravail est une pratique de plus en plus courante qui permet aux employés de travailler à distance, en dehors des locaux de l'entreprise. Cette modalité de travail nécessite des règles spécifiques pour assurer la sécurité des informations et des systèmes informatiques de l'entreprise.

- Les employés doivent utiliser des connexions Internet sécurisées pour accéder aux ressources de l'entreprise. Les réseaux Wi-Fi publics et non sécurisés sont à proscrire.
- Si un employé doit utiliser un réseau Wi-Fi public, il doit impérativement se connecter via un VPN (Virtual Private Network) pour sécuriser la transmission des données.
- Les équipements utilisés pour le télétravail doivent être protégés par des mots de passe robustes.
- Les dispositifs doivent être verrouillés lorsqu'ils ne sont pas utilisés pour empêcher tout accès non autorisé
- L'utilisation d'un VPN est obligatoire pour accéder aux systèmes et aux données de l'entreprise depuis un lieu externe.
- Le VPN crypte les communications entre l'ordinateur de l'employé et le réseau de l'entreprise, réduisant ainsi les risques d'interception et de piratage.
- Le département informatique de l'entreprise est responsable de fournir et de configurer les accès VPN pour les employés.
- Les instructions détaillées pour l'installation et l'utilisation du VPN doivent être fournies aux employés.
- Les données professionnelles doivent être stockées sur des serveurs sécurisés de l'entreprise et non sur des dispositifs personnels ou des services de stockage en ligne non autorisés.
- Les documents sensibles doivent être traités conformément aux politiques de protection des données de l'entreprise et au RGPD.

4. SECURITE DES RESEAUX ET ACCES

Article A - Gestion des accès

L'Utilisateur s'engage à appliquer les recommandations de la société LODI relevant de la politique de gestion des accès et en particulier, sans que cette liste soit considérée comme exhaustive, les dispositions suivantes :

- L'Utilisateur est personnellement responsable de l'utilisation des comptes et mots de passe qui lui sont attribués de manière nominative dans le cadre de ses fonctions pour accéder au système d'information ;
- L'Utilisateur doit respecter la gestion des accès et en particulier ne pas masquer sa véritable identité en se connectant sous le nom ou avec le mot de passe d'un autre Utilisateur (sauf en cas de suppléance avec l'accord écrit du mandataire pour la période de suppléance), ni tenter d'outrepasser les limitations des accès associées à son identifiant (ou login), ni se connecter via un identifiant générique ou collectif en dehors des cas d'utilisation prévus pour celui-ci ;
- L'Utilisateur s'engage à ne pas tenter de modifier ou détruire des informations (données, fichiers, etc.) sans disposer des motifs et des prérogatives permettant de le faire ;
- Les mots de passe des Utilisateurs doivent rester confidentiels. A ce titre, l'Utilisateur s'engage à ne pas divulguer ses mots de passe que ce soit en les notant sur papier, ou en les divulguant à l'oral à d'autres personnes, sauf en cas de maintenance ou de dépannage informatique auxquels cas il est recommandé de changer le code d'accès après l'intervention ;

- L'Utilisateur s'engage à respecter les règles de constitution de mots de passe qui lui sont communiquées (nombre minimum de caractères, utilisation de majuscules, minuscules, chiffres, etc.) ;
- L'Utilisateur s'engage à changer ses mots de passe d'accès régulièrement ou à la demande de la société. De plus, l'employé doit également changer ses mots de passe après remise du matériel, lors de son arrivée.
- L'Utilisateur doit verrouiller son poste de travail lorsqu'il s'absente, même momentanément ;

Dans le cadre de leurs interventions et notamment pour l'assistance aux utilisateurs, le responsable informatique peut être amené à utiliser des logiciels de prise en main à distance des postes informatiques. Cette intervention de prise en main à distance des postes informatiques doit se dérouler avec l'acceptation par l'Utilisateur de la prise en main à distance. Il est déconseillé aux Utilisateurs de s'absenter pendant une telle intervention.

Afin d'assurer la continuité de l'activité du service, et plus particulièrement en cas d'absence, planifiée ou non, l'Utilisateur doit permettre à sa hiérarchie d'avoir accès aux informations (données, fichiers, etc.) liées à ses missions en toute circonstance, notamment en cas d'absence, planifiée ou non. Il pourra par exemple utiliser les serveurs partagés ou les boîtes aux lettres partagées.

Pour les personnes disposants de données a caractère sensible , il est possible de mettre en place une authentification à double facteur à savoir : Lors de la connexion, après avoir entré le mot de passe, l'utilisateur doit fournir un deuxième facteur d'authentification. Cela peut être un code envoyé par SMS, une notification push sur une application d'authentification, une clé de sécurité physique ou une donnée biométrique.Les messageries des postes de direction sont soumises par défaut à cette double authentification.Les utilisateurs disposant de données sensibles doivent se rapprocher du service informatique afin de mettre en place ce type de sécurité.

En cas de perte ou de vol d'un dispositif utilisé pour la MFA, l'utilisateur doit immédiatement informer le service informatique. Ce dernier prendra les mesures nécessaires pour sécuriser le compte affecté, notamment en désactivant l'ancien dispositif et en enregistrant un nouveau.

Article B - Règles de confidentialité

L'Utilisateur peut être amené à traiter dans le cadre de son activité professionnelle des informations ou données confidentielles de la société LODI et/ou des clients. Il doit mettre en œuvre tous les moyens à sa disposition pour s'assurer de la préservation de cette confidentialité. Il s'interdit de les divulguer à tout tiers non autorisé par la société LODI et ceci conformément aux dispositions de son contrat de travail et aux règles qui régissent sa profession.

De tels agissements pourraient nuire gravement à l'image et à l'activité de la société LODI et l'exposeraient à des poursuites judiciaires de la part de tiers. Ils ne pourront donc être tolérés et seront systématiquement sanctionnés.

Article C - Gestion des départs

Lors de son départ de la société LODI, quelle qu'en soit la cause, l'Utilisateur devra restituer l'ensemble des outils qui ont été mis à sa disposition par la société au moment de son embauche. Ces outils donneront lieu à un recensement puis un archivage par le service informatique après émargement « Remis en main propre contre décharge » du collaborateur.

Afin de permettre l'accès aux informations professionnelles stockées sur les différents outils aux personnes habilitées et pour permettre la maintenance des matériels (ou tout autre intervention relevant de leur responsabilité),

l'Utilisateur veillera à supprimer toutes les informations à caractère privé (messages, fichiers, dossiers, ...) contenues sur les outils qui étaient à sa disposition.

Après le départ du salarié, les données et informations relatives à son compte utilisateur, et notamment les éléments de sa messagerie, continuent d'être archivées et stockées selon les règles de sécurité et les durées habituelles.

Afin d'assurer la continuité de l'activité du service, un accès temporaire et occasionnel à la messagerie du salarié pourra être accordé à un collaborateur après le départ du salarié.

Article D - Virus, vers et autres programmes malveillants

Il est strictement interdit aux Utilisateurs de désactiver la protection anti-virus du poste de travail mis à leur disposition.

Chaque Utilisateur doit rester vigilant en veillant à ne pas propager volontairement de virus, vers informatiques ou tout autre programme malveillant. Il se montrera particulièrement prudent face aux pièces jointes des messages reçus d'origine inhabituelle ou d'objet non professionnel.

En effet, des virus peuvent être transportés dans les pièces jointes et peuvent très rapidement nuire au bon fonctionnement des Systèmes d'Information et de la société LODI.

Si l'Utilisateur constate ou soupçonne l'existence d'un virus ou autre programme malveillant sur son équipement, il doit cesser toute utilisation et informer au plus vite par téléphone le service informatique de la société LODI. Il se conformera alors aux instructions et consignes qui lui seront transmises.

Article E - Protection contre les attaques de phishing

- Le phishing est une technique de cyberattaque où des attaquants se font passer pour des entités de confiance pour inciter les victimes à divulguer des informations sensibles telles que des mots de passe, des numéros de carte de crédit, ou d'autres données personnelles.
- Les employés doivent suivre des formations régulières pour reconnaître les emails et messages suspects. Ils doivent être capables d'identifier les signes typiques de phishing, comme les fautes d'orthographe, les adresses email inhabituelles, et les liens douteux.
- Des campagnes de sensibilisation périodiques doivent être organisées pour rappeler les bonnes pratiques de sécurité.
- Avant de cliquer sur un lien ou d'ouvrir une pièce jointe, les employés doivent vérifier l'authenticité de l'expéditeur. En cas de doute, ils doivent contacter directement la personne ou l'organisation par un moyen de communication fiable.
- En cas de réception d'un email suspect, les employés doivent immédiatement le signaler au département informatique et ne pas cliquer sur les liens ou ouvrir les pièces jointes.
- Si un employé pense avoir divulgué des informations sensibles, il doit immédiatement en informer le service informatique pour prendre des mesures correctives.
- Les mises à jour des logiciels incluent souvent des correctifs de sécurité essentiels qui protègent contre les vulnérabilités récemment découvertes. Ne pas mettre à jour les logiciels expose l'entreprise à des risques de sécurité accrus.

- Dans la mesure du possible, les mises à jour des systèmes d'exploitation et des applications doivent être configurées pour s'installer automatiquement. Cela réduit le risque d'oubli et assure que tous les dispositifs disposent des derniers correctifs de sécurité.
- Le département informatique doit régulièrement vérifier que toutes les mises à jour critiques sont installées sur les systèmes de l'entreprise. Cela inclut les systèmes d'exploitation, les logiciels antivirus, les applications métier, et les firmwares des équipements réseau.
- Des audits de sécurité réguliers doivent être effectués pour vérifier que tous les systèmes et logiciels sont à jour. Les résultats des audits doivent être documentés et les actions correctives prises en cas de non-conformité.

5. REGLES D'UTILISATION D'INTERNET ET DE LA MESSAGERIE

Article A - Utilisation d'internet

L'utilisation d'internet est réservée à un usage professionnel, en vue de la réalisation des missions du collaborateur. Seuls les sites présentant un lien direct et nécessaire avec l'activité professionnelle ont vocation à être consultés, sauf urgence de nature familiale.

Néanmoins, la société LODI tolère une utilisation limitée d'internet à des fins personnelles, dans le cadre des nécessités de la vie courante dès lors que cet usage reste ponctuel, raisonnable et ne perturbe pas le bon fonctionnement du Système d'Information, et plus généralement la productivité et la bonne exécution des missions du service.

Cette tolérance ne doit pas amener à une utilisation régulière ou prolongée d'internet à des fins personnelles. Tout usage abusif, pourra être passible de sanctions disciplinaires.

Les employés doivent éviter d'utiliser les réseaux Wi-Fi publics et non sécurisés pour accéder aux systèmes de l'entreprise ou pour transmettre des informations sensibles.

Lorsqu'ils travaillent à distance, les employés doivent utiliser des réseaux Wi-Fi sécurisés, tels que leur réseau domestique protégé par un mot de passe fort.

Lorsqu'il est nécessaire d'utiliser un réseau Wi-Fi public, les employés doivent se connecter via un VPN pour chiffrer leurs communications et protéger leurs données.

L'Utilisateur se devra de respecter les restrictions suivantes :

- Il est strictement interdit de tenter d'accéder à des systèmes ou données internes ou externes sans autorisation (intercepter des données, pénétrer des réseaux ou serveurs sécurisés, attaquer des systèmes informatiques, ...) ;
- Il est strictement interdit de consulter des sites dont le contenu est illicite ou pouvant générer un risque pour la sécurité du Système d'Information ou pour l'image de la société LODI. En particulier et sans que cette liste soit exhaustive, il est interdit de consulter des sites à caractère pédophile, pornographique, antisémite, raciste ou de quelque nature que ce soit qui soit contraire aux bonnes mœurs et à l'ordre public. Les actes liés à la constitution, la diffusion, au soutien de ce type de support ou à leur participation sont répréhensibles pénalement et sanctionnables par des peines aggravées pouvant aller jusqu'à 5 ans d'emprisonnement et 75 000 € d'amendes ;
- Il est interdit de créer ou gérer un site Internet personnel ou un blog personnel en utilisant les ressources et outils informatiques de la société LODI.

- Il est interdit de diffuser ou de télécharger pour un usage personnel des jeux, images, vidéos, musiques ou tout autre document multimédia. Par ailleurs, il est rappelé que l'échange et le partage à titre personnel de ces documents sont volumineux sur le réseau informatique et nuisent au bon fonctionnement des réseaux.
- Il est interdit d'accéder à des forums, chats ou comptes de réseaux sociaux sur Internet sauf dans le cas où ces services correspondent à une nécessité professionnelle, auquel cas leur utilisation doit rester proportionnelle au besoin.
- Il est interdit d'introduire, installer et utiliser un logiciel, y compris un logiciel libre, freeware ou shareware sans autorisation préalable du service informatique.
- Il est formellement interdit de diffuser et d'échanger des informations ou données confidentielles ayant trait à l'activité de la société LODI vers l'extérieur. Dans tous les cas où un Utilisateur participerait à un forum, un chat ou toute autre plate-forme d'échanges, il serait pleinement responsable des propos et des messages émis et échangés tant à l'égard de la société LODI qu'à l'égard des tiers.

Article B - Utilisation de la messagerie

L'utilisation de la messagerie est réservée à un usage professionnel, en vue de la réalisation des missions du collaborateur. Néanmoins, est tolérée une utilisation limitée de la messagerie à des fins personnelles, dans le cadre des nécessités de la vie courante dès lors que cet usage reste ponctuel, raisonnable et ne perturbe pas le bon fonctionnement du Système d'Information, et plus généralement la bonne exécution des missions du service.

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.

En cas d'absence supérieure ou égale à 8 jours ouvrables, le collaborateur a l'obligation de mettre un message d'absence sur sa messagerie.

Toutes les correspondances d'ordre non professionnel devront comporter dans leur objet la mention «**PERSONNEL**» de manière à ce qu'elles soient distinctes des correspondances professionnelles.

De la même façon, l'Utilisateur veillera à classer ces messages reçus dans un répertoire prévu spécifiquement à cet effet et intitulé «**PERSONNEL**». Il est en revanche strictement interdit de classer des messages à caractère professionnel dans le répertoire «PERSONNEL».

L'émission d'e-mails depuis la messagerie de la société LODI engage la responsabilité tant civile que pénale et l'image de la société LODI. L'Utilisateur devra avoir une vigilance et une prudence particulières lors de tout envoi de message électronique depuis sa messagerie professionnelle.

Chaque Utilisateur s'engage à faire un usage de la messagerie qui demeure respectueux des personnes. Il s'engage notamment à ne pas porter atteinte à l'intégrité, la dignité et la sensibilité d'un autre Utilisateur, notamment par l'intermédiaire de messages, textes ou images provocants.

Les Utilisateurs sont avertis que les contenus suivants sont considérés comme inacceptables :

- Tout message pouvant être perçu comme harcèlement ou dénigrement sur le sexe, la race, le comportement sexuel, l'âge, la nationalité d'origine, un handicap, la religion, l'appartenance politique ou sur tout autre critère relevant de la discrimination ;
- Les messages, images, caricatures ou plaisanteries comportant un caractère sexuel, diffamatoire ou insultant
- Les injures, jurons, obscénités, calomnies ou diffamations insultants

- Les messages qui pourraient être perçus comme le dénigrement de la société LODI, d'un de ses membres ou de ses partenaires.

La société LODI attire l'attention des utilisateurs sur le fait que tout e-mail émis ou reçu, transitant par la boite e-mails Outlook sera automatiquement sauvegardé et conservé en « cloud » da ns la limite de la capacité de stockage alloué par boite mail (actuellement 60 Go).

La société LODI a également mis en place des systèmes de filtrage permettant d'identifier les documents et pièces jointes qui seraient trop volumineux (images, photos, vidéos, ...), ainsi que les messages contenant certains mots clé jugés illicites, les spams et autres publicités non sollicitées.

Le service informatique, après accord de la Direction, se réserve le droit de les analyser, de les recycler convenablement voire de les supprimer s'ils portent atteinte à la sécurité et au bon fonctionnement des Systèmes d'Information.

Article C - Secret des correspondances

Le secret des correspondances défini par l'article 226-15 du Code Pénal s'applique aux courriers électroniques et stipule qu'il est interdit sous peine de poursuites de consulter, intercepter, détourner, supprimer ou retarder des correspondances adressées à des tiers. Il est également interdit de divulguer ou d'utiliser le contenu de ces correspondances.

Les messages à caractère non professionnel classés dans un répertoire intitulé « PERSONNEL » et identifiés comme tels sont couverts par le secret des correspondances y compris sur le lieu de travail, de sorte que l'employeur ne peut y accéder en dehors de la présence du salarié.

Dans le cadre du contrôle de l'activité de ses salariés, l'employeur a la possibilité d'accéder à l'ensemble des messages professionnels émis et reçus par les salariés sur leur poste de travail en leur présence.

6. CONTROLE DE L'USAGE DES SYSTEMES D'INFORMATION (S.I.)

Article A - Objectifs

La politique de sécurité mise en place par la société LODI vise en particulier à assurer la disponibilité, la confidentialité, l'intégrité et la traçabilité des données.

Pour des raisons de sécurité et de bon fonctionnement des ressources informatiques, la société LODI se réserve le droit de mettre en place des moyens permettant de surveiller l'utilisation des réseaux informatiques mis à disposition des Utilisateurs afin de les protéger contre des saturations éventuelles ou des utilisations détournées.

Il est précisé que les moyens de contrôle et de protection mis en œuvre par la société LODI répondent aux objectifs suivants :

- Assurer la permanence du fonctionnement des Systèmes d'Information, notamment en contrôlant et en optimisant l'exploitation des outils, en réalisant des sauvegardes régulières et en cas de panne en procédant aux opérations de maintenance corrective et de restauration nécessaires ;
- Assurer le maintien des performances des Systèmes d'Information ;

- Garantir la sécurité et le bon fonctionnement des Systèmes d'Informations au travers de systèmes de filtrage et d'audit qui se composent notamment d'anti-virus, de passerelles, de pare-feu, de filtrage, d'anti-spam et de sonde de détection d'intrusion ;
- Garantir aux clients et aux partenaires de la société LODI un traitement des données qui assure leur disponibilité, leur confidentialité, leur intégrité et leur traçabilité ;
- Assurer la confidentialité, la sécurité et l'intégrité des données notamment en interdisant ou autorisant l'accès aux Systèmes d'Information, pour des opérations et des fonctions définies, selon des critères spécifiques conformément à la politique de sécurité de la société LODI (gestion des habilitations, des environnements et de la messagerie) ;
- Permettre d'identifier les personnes qui accèdent aux Systèmes d'Information (par l'utilisation d'identifiant et de mot de passe dont ils n'en seraient pas les détenteurs) ;
- Vérifier le respect des règles régissant l'utilisation des Systèmes d'Information et notamment le respect de la présente charte ;
- Assurer l'évolution dans le temps (maintenance évolutive et corrective) des Systèmes d'Information ;
- Mettre à disposition les moyens d'appliquer la présente charte.

Nous attirons l'attention des Utilisateurs sur les moyens de contrôle, de surveillance et de protection suivants mis en œuvre, sans que cette liste ne soit exhaustive :

- Filtrage des sites web dont la société LODI autorise l'accès
- Vérification et contrôle des informations et données téléchargées à partir d'Internet ;
- Contrôle du volume et de la taille des messages émis et reçus et suppression des messages bloquants ou susceptibles de porter atteinte à l'intégrité du système ;
- Modification de la priorité d'une tâche ou annulation d'une tâche des Utilisateurs, après les en avoir avertis, si celle-ci nuit aux autres utilisateurs ou à l'activité de la société LODI;

Article B - Fichiers de trace

→ **Information des utilisateurs**

L'ensemble des services informatiques utilisés génèrent, à l'occasion de leur emploi, des « fichiers de trace ». Ces fichiers sont essentiels à l'administration des Systèmes d'Information. Ils servent à remédier aux dysfonctionnements des services ou systèmes informatiques utilisés. Ces fichiers conservent des informations par exemple concernant la messagerie (expéditeurs, destinataires, date ...) mais aussi heures de connexion aux applications de gestion, connexions à distance, numéro de la machine utilisée, identifiant utilisé, ...

Ce type de trace existe pour l'ensemble des services informatiques et fait donc partie intégrante des dispositifs de contrôle et de protection mis en place par la société LODI. Ces fichiers ne sont utilisés que pour un usage technique et conservés pour une durée définie adaptée à chaque application.

Les fichiers de trace sont conservés sur le poste dans la limite de capacité de stockage du poste. Pour l'application X3, la durée de conservation des fichiers et limitée à 3 mois.

→ **Données sensibles**

La société LODI est responsable des données qu'elle utilise et met à disposition des utilisateurs. Certaines applications permettent l'accès et l'utilisation de données particulièrement sensibles, notamment concernant la santé et la vie privée des clients, les données financières des entités etc.

Afin de garantir la sécurité et la confidentialité de ces informations et d'en prévenir toute utilisation détournée, les fichiers de trace générés par ces applications sont conservés de façon systématique pour une durée adaptée à la sensibilité des applications et des données concernées et dans le respect des prescriptions légales.

Article C - Interventions de la société LODI

La société LODI s'engage à n'utiliser les moyens de contrôle et de protection mis en œuvre de façon conforme et proportionnée aux buts et objectifs précisés ci-dessus.

Dans le cadre de leur mission, les salariés de la société LODI sont soumis au **secret professionnel** qui leur interdit de révéler les informations qu'ils pourraient être amenés à connaitre à cette occasion.

Le service informatique affecté à l'exploitation des Systèmes d'Informations est susceptible d'informer la Direction de la société LODI de tout message électronique ou utilisation des outils et des Systèmes d'Information qui peuvent mettre en cause le bon fonctionnement technique de ces derniers ou porter atteinte à sa sécurité ou aux intérêts de la société LODI.

Il a en charge d'assurer le fonctionnement optimal des ressources informatiques, d'en assurer la sécurité et de préserver les informations qu'elles contiennent.

De ce fait, le service informatique dispose d'accès étendus à l'ensemble des données et systèmes du Système d'Information et peut être amené à accéder à l'ensemble des informations stockées ou transitant sur les Systèmes d'Information. Ce service est tenu de respecter les règles de confidentialité quant aux informations dont il pourrait avoir connaissance dans le cadre de sa mission.

Article D - Contrôle de la société LODI

En application de l'article 1384 du Code Civil, la responsabilité des membres de la société LODI en tant qu'employeur peut être engagée en cas d'usage irrégulier, voire illicite par un Utilisateur des matériels mis à sa disposition pour un usage professionnel.

La société LODI a donc le devoir de prévenir la mise en cause de sa responsabilité et s'appuiera sur les dispositifs de contrôle mis en place par la société LODI pour s'assurer de l'usage régulier des Systèmes d'Information par ses salariés.

Par ailleurs, il est rappelé que les dossiers et fichiers de chaque Utilisateur, stockés sur l'outil informatique mis à disposition pour l'exécution de leur mission, sont présumés avoir un caractère professionnel de sorte que l'employeur peut y avoir accès hors de sa présence, sauf si l'utilisateur les identifie comme « Personnel ».

L'ensemble des ressources matérielles, logicielles et réseaux peuvent faire l'objet de surveillance, d'analyse et de contrôle, dans le respect de la législation en vigueur et notamment de la loi « Informatique & Libertés » du 6 janvier 1978, y incluant ses modifications ultérieures.

A titre indicatif, les moyens automatisés de surveillance, d'analyse et de contrôle peuvent notamment être les suivants :

- Journaux de connexion : ils permettent de retracer les accès passés ou en cours, et plus particulièrement la connexion des Utilisateurs aux éléments suivants :
  - Réseaux et ressources informatiques de la société LODI, dont la messagerie électronique
- Journaux d'activité : ils permettent de retracer certaines actions effectuées dans le Système d'Information.
- Contrôles de contenu : ils permettent de vérifier, en temps réel ou a posteriori, qu'un contenu (par exemple un fichier accédé ou stocké) est conforme à la politique de sécurité de la société LODI, ou n'est pas porteur d'un risque pour la société LODI (ex. : virus).
- Contrôles des communications téléphoniques : ces contrôles visent à optimiser la gestion des moyens de communication et à permettre une certaine maîtrise des dépenses liées à l'utilisation des services de téléphonie.

S'il dispose d'un motif légitime, l'employeur pourra accéder aux dossiers et fichiers qualifiés de « Personnel » des Utilisateurs en respectant les conditions de procédure suivantes :

- L'Utilisateur concerné devra être présent et/ou pourra désigner puis demander la présence d'un tiers, salarié de la société LODI, en qualité de témoin pendant la durée du contrôle ;
- Le contrôle effectué devra être respectueux de la dignité des personnes et notamment ne pas divulguer les informations collectées.

Face à un danger sérieux et imminent pour la société LODI, l'employeur pourra accéder aux dossiers et fichiers qualifiés de « Personnel » des Utilisateurs en dehors de sa présence ni même dûment prévenu si les conditions suivantes sont réunies :

- Le contrôle est justifié par un risque ou évènement particulier ;
- Le contrôle est justifié par l'urgence ;
- Le contrôle est indispensable et l'employeur ne dispose pas d'alternative moins intrusive.
- Le contrôle effectué devra être respectueux de la dignité des personnes et notamment ne pas divulguer les informations collectées.

Ces contrôles ne pourront être exercés que par un ou des représentant(s) de l'employeur, éventuellement accompagné(s) d'un salarié de la société LODI.

Ces dispositions n'empêchent aucunement l'employeur de se faire autoriser par un juge ou toute autorité compétente l'accès aux fichiers et dossiers qualifiés de « Personnel » dans le cadre d'une procédure juridique, qu'elle soit civile ou pénale.

Article E - Protection des informations personnelles

La mise en œuvre des procédures visées dans la présente Charte peut entraîner la collecte et le traitement de données personnelles, au sens de la loi « Informatique & Libertés » du 6 janvier 1978 telle que modifiée par la loi du 6 août 2004, suivant une finalité de sécurité du Système d'information de la société.

Le cas échéant, ces collectes et traitements, qui ont pour principale finalité d'assurer la sécurité du Système d'information de la société et l'optimisation de leur traitement, sont effectués en conformité avec la loi précitée dans sa version en vigueur, et font en tant que de besoin l'objet de déclarations auprès de la Commission Nationale de l'Informatique et des Libertés (CNIL).

Conformément à la loi précitée, l'Utilisateur bénéficie d'un droit d'opposition au traitement des données personnelles le concernant s'il justifie d'un motif légitime.

Le traitement, la durée de conservation des données, et la personne auprès de qui peut s'exercer le droit d'accès prévu par la loi, sont publiés. L'Utilisateur peut exercer ces droits en adressant une demande officielle et écrite au responsable désigné du traitement concerné.

Article F - Portée disciplinaire

Le respect de la présente Charte Informatique peut faire l'objet de contrôles sans préavis. Les dispositions de la présente charte s'imposent à tout utilisateur du réseau, salarié permanent ou temporaire, lié ou non par un contrat de travail.

Tout manquement, tout abus ou utilisation non conforme de la présente charte peut faire l'objet de sanctions disciplinaires à l'encontre des intéressés.

Ces sanctions disciplinaires sont prévues par le règlement intérieur, elles pourront aller de l'avertissement à la rupture des relations contractuelles, selon les circonstances.

La violation de tout ou partie des dispositions de la présente Charte Informatique par l'Utilisateur peut entraîner la mise en œuvre de sa responsabilité civile et/ou pénale.

7. TEXTES DE REFERENCE

En complément du présent document, vous pourrez trouver dans les textes de lois et sources suivants de nombreuses informations portant sur la réglementation en vigueur et sur les usages et pratiques en matière de systèmes d'information :

- Secret des correspondances – Articles 226-15 et 432-9 du Code Pénal
- Respect de la vie privée – Article 9 du Code Civil
- Loi Informatique et Libertés du 6 janvier 1978
- Respect du droit d'auteur et de la propriété intellectuelle – Articles L 335-4 et suivants du Code la Propriété Intellectuelle
- Site internet de la CNIL www.cnil.fr
- Rapport de la CNIL « La cyber surveillance sur les lieux de travail »
- Commission nationale de l'informatique et des libertés (Rapport annuel – 2023) https://www.cnil.fr/sites/cnil/files/2024-05/cnil_44e_rapport_annuel_2023.pdf
- Le règlement général sur la protection des données (RGPD) https://www.cnil.fr/fr/reglement-europeen-protection-donnees

8. ENTREE EN VIGUEUR

La présente charte est annexée au Règlement Intérieur, dont elle est un élément à part entière.

Elle a été transmise à l'Inspecteur du travail, déposée au greffe du Conseil de prud'hommes de Rennes et a fait l'objet d'un affichage en date du 1er octobre 2024.

Elle entrera en vigueur un mois après l'accomplissement de ces formalités. Elle est communiquée lors de son introduction dans la société LODI ou lors de l'embauche, à tout salarié ou toute personne concernée.

La société LODI informera, selon les dispositions légales et selon les mêmes modalités de consultation et d'information, les Utilisateurs et toutes les parties prenantes en cas de modification de cette charte.

Alexis LOCKMAN

Président