

CHARTRE D'UTILISATION DES MOYENS INFORMATIQUES ET DES OUTILS NUMERIQUES
MISSION LOCALE HAUTE-GARONNE

SOMMAIRE

Préambule.....	2
Article 1 : Champ d'application.....	3
Article 2 : Objet.....	3
Article 3 : Conditions d'utilisation des Systèmes d'Information.....	4
Section 3.1 - Engagements des Missions Locales, des Utilisateur-trices et de l'Etat	4
Section 3.2 - Utilisation professionnelle / privée	5
Section 3.3 - Télétravail	6
Section 3.4 - Continuité de service : gestion des absences et des départs	6
Article 4 : Principes de sécurité	6
Section 4.1 - Règles de sécurité applicables	6
Section 4.2 - Devoirs de signalement et d'information	8
Section 4.3 - Mesures de contrôle de la sécurité	8
Section 4.4 - Personnels chargés de mission de contrôle de la sécurité du SI dans la Mission Locale.....	8
Article 5 : Communication électronique.....	8
Section 5.1 - Messagerie électronique	8
Section 5.2 - Internet	9
Section 5.3 - Téléchargements et Pare-feu	10
Article 6 : Respect de la propriété intellectuelle	11
Article 7 : Respect de la législation.....	11
Article 8 : Limitation des usages	12
Article 9 : Responsabilités- Sanctions	12
Article 10 : Entrée en vigueur de la Charte – Dépôt et publicité.....	12

Préambule

L'activité des Missions Locales implique de devoir gérer des données à caractère personnel, c'est-à-dire des informations qui permettent, sous quelque forme que ce soit, directement ou indirectement, l'identification des personnes physiques auxquelles elles s'appliquent.

Pour réaliser ses missions et gérer son activité, le réseau des Missions Locales s'est doté d'un Système d'Information I-MILO qui réalise des traitements automatisés sur des fichiers comportant des données à caractère personnel des jeunes accueillis dans les structures.

Les Missions Locales disposent également d'autres systèmes d'information tels que des systèmes d'information RH qui réalise des traitements automatisés sur des fichiers comportant des données à caractère personnel des salariés des structures.

Elles accèdent également à d'autres SI tels que notamment DUDE (Pôle emploi), Rio-suivi (Education nationale), système d'information CPF, où elles sont amenées à consulter et saisir des informations à caractère personnel. Elles peuvent également à partir de ces systèmes d'information éditer des listes. Les accès sont liés à des engagements (charte déontologique dans certains cas) entre chaque Mission Locale et l'autorité mettant à disposition son outil.

La loi n°78-17 du 6 janvier 1978 « Informatique et Libertés » régit l'utilisation des données à caractère personnel.

La loi n° 2018-493 du 20 juin 2018, promulguée le 21 juin 2018, a modifié la loi « Informatique et Libertés » afin de mettre en conformité le droit national avec le cadre juridique européen. Elle permet la mise en œuvre concrète du règlement européen 2016-679 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (RGPD).

Pour répondre aux exigences légales et européennes, les Missions Locales se dotent d'une charte d'utilisation des moyens informatiques. Cette charte a pour finalité de contribuer à la préservation de la sécurité du système d'information des Missions Locales et de faire de l'utilisateur-trice un acteur essentiel à la réalisation de cet objectif.

L'ensemble des utilisateur-trice-s et gestionnaires du système d'information sont tenus de se conformer aux dispositions de la présente charte.

Article 1 : Champ d'application

Le "Système d'Information" (SI) des Missions Locales recouvre l'ensemble des ressources matérielles, logicielles, applications, bases de données, équipements de reprographie et réseaux de télécommunications, pouvant être mis à disposition et utilisé par les Missions Locales.

Le terme « SI » vise donc indifféremment le système I-MILO ainsi que les autres systèmes d'information dont disposent les Missions Locales.

L'informatique nomade (tels que les assistants personnels, les ordinateurs portables, les téléphones, boîtiers de télégestion, ...), est également un des éléments constitutifs du Système d'Information Mission Locale.

La présente charte a été soumise à l'avis du CSE le 25 novembre 2022.

Par « Mission Locale » il faut entendre la Mission Locale Haute-Garonne

Le terme « Utilisateur-trice » recouvre :

- toute personne ayant accès, dans le cadre de l'exercice de son activité, aux ressources du SI quel que soit son statut : salarié, stagiaire, bénévole, partenaire...
- tout prestataire ayant contracté avec une structure une mission lui donnant accès à tout ou partie du SI.

Le terme Utilisateur-trice recouvre donc des Utilisateur-trice-s internes et externes au réseau des Missions Locales. Les Utilisateur-trice-s externes (prestataire, sous-traitant, partenaire etc.) s'engagent à respecter et/ou à faire respecter la Charte lorsque celle-ci est portée à leur connaissance par voie contractuelle notamment.

Le terme « donnée personnelle » : Toute information identifiant directement ou indirectement une personne physique (ex. nom, numéro d'immatriculation Sécurité sociale, numéro de téléphone, photographie, adresse mail, date de naissance, commune de résidence, empreinte digitale...).

Le droit d'accéder au SI des Missions Locales est un droit temporaire, individuel, lié à la mission et/ou fonction de l'Utilisateur-trice.

Article 2 : Objet

La charte a pour objet d'informer l'Utilisateur-trice sur :

- les usages permis des moyens informatiques mis à sa disposition,
- les règles de sécurité en vigueur,
- les mesures de contrôle prises par l'employeur,
- les sanctions encourues par l'utilisateur-trice.

Elle définit les règles d'usages et de sécurité que la Mission Locale et tout Utilisateur-trice s'engagent à respecter. Elle précise les droits et devoirs de chacun. ⁽¹⁾

La charte rappelle les droits et obligations de chaque Utilisateur-trice, ainsi que les précautions à respecter, concernant l'utilisation des ressources technologiques du SI afin de préserver la sécurité et

¹ Tout document relatif aux conditions d'utilisation du système d'information doit se conformer aux principes de la charte

la confidentialité et d'appeler l'attention des Utilisateur-trice-s sur certains comportements de nature à porter atteinte à l'intérêt collectif « du réseau » des Missions Locales.

La Charte précise qu'il incombe à chaque Utilisateur-trice de veiller à la sécurité des données et informations des Missions Locales.

L'Utilisateur-trice est personnellement responsable de l'usage qu'il fait des ressources technologiques. Il s'engage à une utilisation rationnelle et loyale des ressources technologiques auxquelles il a accès afin d'éviter la saturation de ces ressources et le détournement des données et informations qu'elles contiennent.

Article 3 : Conditions d'utilisation des Systèmes d'Information

Section 3.1 - Engagements des Missions Locales, des Utilisateur-trices et de l'Etat

Engagements de l'Etat :

Concernant I-MILO, l'Etat en sa qualité de responsable de traitement facilite l'accès des Utilisateur-trices aux ressources du Système d'Information dans le respect des règles de sécurité.

Engagements de la Mission Locale :

La Mission Locale met en œuvre les mesures nécessaires pour assurer la sécurité de son Système d'Information et la protection des données et des Utilisateur-trices.

Engagements de l'Utilisateur-trice :

Les ressources mises à la disposition de l'Utilisateur-trice sont dédiées à un usage professionnel.

L'Utilisateur-trice est responsable en tout lieu, de l'usage qu'il fait du Système d'Information ainsi que des ressources auxquelles il a accès.

Il doit en faire une utilisation loyale et rationnelle et ne doit pas mettre en péril la sécurité et l'intégrité du matériel informatique. Il a une obligation de réserve et de confidentialité à l'égard des informations et documents auxquels il accède. Cette obligation implique le respect des règles d'éthique professionnelle et de déontologie.

La Mission Locale interdit à l'Utilisateur-trice toute cession, transmission ou location de fichiers à des tiers intéressés par son patrimoine informationnel.

De même, l'Utilisateur-trice doit signaler à la Mission Locale toute tentative de violation de son compte et, de manière générale, toute anomalie qu'il peut constater.

Il est strictement interdit à l'Utilisateur-trice de détenir et de conserver sur le matériel mis à sa disposition par la Mission Locale des données (photos, vidéos...) à caractère violent, pornographique, pédophile, raciste ou incitant à la haine raciale, révisionniste, offensant ou diffamatoire et, de manière générale, toute donnée à caractère illicite.

En tout état de cause, l'Utilisateur-trice est soumis au respect des obligations résultant de son statut ou de son contrat.

Section 3.2 - Utilisation professionnelle / privée

Le Système d'Information (incluant messagerie, internet...) est un outil de travail. L'utilisation des ressources informatiques et l'usage des services internet, ainsi que des réseaux permettant d'y accéder, sont réservés à la seule activité professionnelle des Utilisateur-trices, conformément aux lois et règlements en vigueur. Il est donc interdit d'utiliser ces ressources pour porter atteinte aux mœurs, à l'honneur, à la vie privée ou à l'intégrité morale d'une autre personne.

Usage professionnel :

Les ressources technologiques font partie du patrimoine de la Mission Locale. A cet égard, toutes les informations, données ou communications électroniques émises, reçues ou stockées au moyen de ces ressources, ainsi que tous les documents et fichiers enregistrés par l'Utilisateur-trice, notamment sur son poste de travail ou sur les serveurs de la Mission Locale sont présumés appartenir à la Mission Locale et avoir un caractère professionnel, sauf si l'Utilisateur-trice les identifie clairement comme étant personnels.

En cas d'absence ou de départ de l'Utilisateur-trice, quel qu'en soit le motif, l'Utilisateur-trice doit se conformer aux règles fixées à la section 3.04.

Usage personnel :

L'utilisation des ressources du système d'information et l'usage des services Internet sont autorisés dans le cadre de l'activité professionnelle et le cas échéant pour des besoins personnels à la condition que cet usage présente un caractère limité en nombre et en durée de connexions et qu'il ne soit pas porté atteinte à l'obligation d'exécution loyale du contrat de travail.

En revanche, un fichier ou un message électronique peut être identifié comme personnel lorsque son nom ou son objet, ou le dossier dans lequel il est enregistré, comporte clairement la mention : « personnel », « privé ». Les messages « personnels » relèvent alors du secret des correspondances.

A défaut de mention, les messages et fichiers seront considérés comme professionnels. Il appartient à l'Utilisateur-trice de procéder au stockage de ces données à caractère privé ou personnel dans un espace de données prévu explicitement à cet effet ou mentionnant le caractère privé de la ressource.

Les données personnelles de l'Utilisateur-trice ne doivent pas être sauvegardées sur les matériels de la Mission Locale et la politique de sauvegarde de la Mission Locale ne couvre pas les données personnelles de l'Utilisateur-trice.

Sauf en cas d'événement, de risque particulier susceptible de porter préjudice à la Mission Locale, à l'un de ses salariés ou à un tiers, ou de maintenance, la Mission Locale s'engage à n'accéder aux données et communications électroniques ayant été identifiées comme personnelles par un Utilisateur-trice, émises, reçues, transmises, téléchargées ou enregistrées par un Utilisateur-trice, sur le poste de l'Utilisateur-trice, sur un autre poste ou sur l'un des serveurs de la Mission Locale qu'en présence de l'Utilisateur-trice concerné ou qu'après l'avoir dûment informé.

A l'exclusion du SI I-MILO, l'utilisation du SI à titre privé doit respecter la réglementation en vigueur.

La consultation, détention, diffusion et exportation d'images à caractère pédophile, ou la diffusion de contenus à caractère raciste ou antisémite est totalement interdite. Il est interdit de consulter des sites non autorisés par la Mission Locale, à caractère violent, pornographique, pédophile, raciste ou incitant à la haine raciale, révisionniste, offensant ou diffamatoire et, de manière générale, tout site à caractère illicite.

Section 3.3 - Télétravail

L'obligation de confidentialité est renforcée en raison du télétravail. Le salarié-e en télétravail doit s'assurer du respect de la confidentialité et de l'intégrité des informations et documents qui lui sont confiés et auxquels il a accès dans le cadre professionnel.

Le salarié-e télétravailleur s'engage à n'utiliser le matériel mis à disposition qu'à des fins professionnelles dans le cadre de l'exercice de ses fonctions professionnelles.

En tant qu'Utilisateur-trice, le salarié-e en situation de télétravail a les mêmes obligations que le salarié-e qui exécute son travail dans les locaux de la structure, notamment en ce qui concerne les principes de sécurité visés à l'article IV de la présente charte.

Section 3.4 - Continuité de service : gestion des absences et des départs

Aux seules fins d'assurer la continuité de service, l'Utilisateur-trice informe sa hiérarchie des modalités permettant, pendant son absence temporaire, de rendre disponible les ressources nécessaires au bon fonctionnement du service et mises spécifiquement à sa disposition, tout en préservant le niveau de sécurité et confidentialité conforme à la charte.

Dans le cas d'un utilisateur-trice quittant définitivement la Mission Locale, il est tenu de restituer à son responsable l'intégralité des outils informatiques et téléphoniques mis à sa disposition dans le cadre de l'exécution de sa mission.

Les accès de l'Utilisateur-trice au SI sont rendus inactifs à la date de son départ.

Le responsable de la structure (ou administrateur principal des comptes d'accès selon les outils) informe l'autorité des systèmes d'information mis à disposition du départ des salarié-e-s, comme prévu dans les conventions qui les lient.

Dès qu'il connaît la date de son départ, le cas échéant, l'utilisateur-trice peut demander, auprès de sa hiérarchie, à récupérer ou à supprimer les données identifiées comme personnelles. L'Utilisateur-trice s'interdit de supprimer toutes données professionnelles.

Les mesures de conservation des données professionnelles sont définies avec le responsable désigné au sein de la Mission Locale.

Article 4 : Principes de sécurité

Section 4.1 - Règles de sécurité applicables

La Mission Locale met en œuvre les mécanismes de protection appropriés sur les ressources informatiques mises à la disposition des Utilisateur-trices avec des procédures écrites et évaluées.

L'utilisateur-trice est informé que les identifiants et codes d'accès constituent une mesure de sécurité destinée à éviter toute utilisation malveillante ou abusive. ⁽²⁾

Les niveaux d'accès ouverts à l'Utilisateur-trice sont définis en fonction de la mission qui lui est confiée.

² Cette mesure ne confère pas aux outils informatiques protégés un caractère personnel.

La sécurité du SI mis à sa disposition lui impose :

- de respecter les consignes de sécurité, notamment les règles relatives à la gestion des codes d'accès évoquées ci-après;
- de garder strictement confidentiels ses codes d'accès et ne pas les dévoiler à un tiers. Effectivement, chaque Utilisateur-trice se voit attribuer une identification personnelle sous forme d'un login et d'un mot de passe. Il est responsable de l'utilisation qui peut en être faite et doit les garder secrets. Il ne doit en aucun cas les communiquer à un tiers. Si, pour des raisons exceptionnelles et ponctuelles, l'Utilisateur-trice se trouve dans l'obligation de communiquer son mot de passe à un tiers, il devra ensuite le modifier dès que possible. Chaque mot de passe doit obligatoirement être modifié tous les 3 mois. Un mot de passe doit être composé d'au minimum 8 caractères composés d'au moins 1 majuscule, 1 minuscule, 1 chiffre et un caractère spécial (@., ;: ...). Concernant les accès internet sur les SI partenaires, ces changements sont réglementés dans le cadre des conventions de mise à disposition (ex : DUDE oblige à un changement de MDP tous les mois). Les mots de passe sont réglementés par le fournisseur.
- de respecter la gestion des accès, en particulier ne pas utiliser les codes d'accès d'un autre Utilisateur-trice, ni chercher à les connaître, sauf cas exceptionnel spécifique au métier
- de verrouiller sa session lorsqu'il quitte son poste de travail ⁽³⁾.

Par ailleurs, la sécurité des ressources mises à la disposition de l'Utilisateur-trice nécessite plusieurs précautions :

De la part de la Mission Locale :

- veiller à ce que les ressources sensibles ne soient accessibles qu'aux personnes habilitées ⁽⁴⁾
- limiter l'accès aux seules ressources pour lesquelles l'Utilisateur-trice est expressément habilité ;

De la part de l'Utilisateur-trice :

- s'interdire d'accéder ou de tenter d'accéder à des ressources du Système d'Information pour lesquelles il n'a pas reçu d'habilitation explicite ;
- verrouiller son ordinateur dès qu'il quitte son poste de travail ;
- ne pas connecter directement aux réseaux locaux des matériels autres que ceux confiés ou autorisés par la Mission Locale ou ceux dont la liste a été précisée dans un guide d'utilisation établi par le service ou l'association ;
- ne pas installer, télécharger ou utiliser sur le matériel de la structure, des logiciels ou progiciels, des fichiers audio, vidéo ou films, sans autorisation de sa hiérarchie ou ne provenant pas de sites dignes de confiance, ou non conformes aux préconisations de la Mission Locale ;
- ne pas supprimer ou modifier des informations qui ne lui appartiennent pas ;
- se conformer aux dispositifs mis en place par la Mission Locale pour lutter contre les virus et les attaques par programmes informatiques.

³ Verrouillage de session WINDOWS (raccourci : clavier Windows + L) ou mise en veille avec obligation de se ré-authentifier ou mise hors tension en fin de journée ou pendant la pause méridienne

⁴ En dehors des mesures d'organisation de la continuité du service mises en place par la hiérarchie

Section 4.2 - Devoirs de signalement et d'information

L'Utilisateur-trice doit avertir sa hiérarchie dans les meilleurs délais de tout dysfonctionnement constaté ou de toute anomalie découverte (par exemple une intrusion dans le SI).

Il signale également à la personne responsable du site toute possibilité d'accès à une ressource qui ne correspond pas à son habilitation.

L'utilisateur-trice a pour obligation de signaler au service informatique la perte ou le vol de tout matériel mis à sa disposition (ordinateur portable et téléphone portable) **dès que constaté**.

Section 4.3 - Mesures de contrôle de la sécurité

L'Utilisateur-trice est informé :

- que pour effectuer la maintenance préventive, curative ou évolutive, la Mission Locale se réserve la possibilité de réaliser des interventions (le cas échéant à distance ⁽⁵⁾) sur les ressources mises à sa disposition ;

- que toute information bloquante pour le système ou générant une difficulté technique d'acheminement à son destinataire, sera isolée ; le cas échéant rendue inaccessible depuis le SI ou supprimée.

La Mission Locale informe l'Utilisateur-trice que le Système d'Information donne lieu à une surveillance et un contrôle à des fins statistiques, de traçabilité réglementaire ou fonctionnelle, d'optimisation, de sécurité ou de détection des abus, dans le respect de la législation applicable.

Section 4.4 - Personnels chargés de mission de contrôle de la sécurité du SI dans la Mission Locale

Le personnel chargé des opérations de contrôle des Systèmes d'Information sont soumis au secret professionnel.

Il ne peut divulguer les informations qu'ils sont amenés à connaître dans le cadre de leurs fonctions dès lors que ces informations sont couvertes par le secret des correspondances ou identifiées comme telles, elles relèvent de la vie privée de l'Utilisateur-trice.

Il est assujéti au devoir de réserve et est tenu de préserver la confidentialité des données qu'il est amené à connaître dans le cadre de leurs fonctions.

En revanche, il doit communiquer ces informations si elles mettent en cause le bon fonctionnement technique des applications ou leur sécurité, ou si elles tombent dans le champ de l'article 40, alinéa 2 du code de procédure pénale (obligation de dénonciation de tout acte délictueux constaté).

Article 5 : Communication électronique

Section 5.1 - Messagerie électronique

L'utilisation de la messagerie constitue l'un des éléments d'optimisation du travail, de mutualisation et d'échange de l'information au sein de la structure.

Adresses électroniques :

En fonction des besoins, la Mission Locale s'engage à mettre à la disposition de l'Utilisateur-trice une boîte à lettres électronique professionnelle nominative lui permettant d'émettre et de recevoir des messages électroniques.

⁵ Une maintenance à distance est précédée d'une information de l'Utilisateur-trice

L'utilisation de cette adresse nominative est ensuite de la responsabilité de l'Utilisateur-trice. L'utilisation de la messagerie électronique à des fins personnelles est tolérée, dans des proportions raisonnables et à la condition que cela n'affecte pas le trafic normal des messages professionnels.

La gestion d'adresses électroniques correspondant à des listes de diffusion institutionnelles, désignant une catégorie ou un groupe d'« utilisateur-trice-s », relève de la responsabilité exclusive de la Mission Locale : ces listes ne peuvent être utilisées sans son autorisation explicite.

Contenu des messages électroniques :

Sont interdits les messages comportant des contenus à caractère illicite quelle qu'en soit la nature ⁽⁶⁾.

Émission et réception des messages :

L'Utilisateur-trice doit s'assurer de l'identité et de l'exactitude des adresses des destinataires des messages. En cas d'envoi du même message à plusieurs personnes, il utilise « la copie cachée » sauf à avoir demandé préalablement l'autorisation de communiquer l'adresse de messagerie des tiers.

Il doit veiller à ce que la diffusion des messages soit limitée aux seuls destinataires concernés afin d'éviter les diffusions de messages en masse, l'encombrement inutile de la messagerie ainsi qu'une dégradation du service.

Statut et valeur juridique des messages :

Les messages électroniques échangés avec des tiers peuvent, au plan juridique, former un contrat ⁽⁷⁾.

L'Utilisateur-trice doit, en conséquence, être vigilant sur la nature des messages électroniques qu'il échange au même titre que pour les courriers traditionnels.

Stockage et archivage des messages :

Les messages électroniques sont conservés sur le serveur de messagerie de l'entreprise pendant toute la durée du contrat de travail + 30 jours.

L'utilisation de la messagerie électronique à des fins personnelles est tolérée, dans des proportions raisonnables et à la condition que cela n'affecte pas le trafic normal des messages professionnels.

Chaque Utilisateur-trice doit organiser et mettre en œuvre les moyens nécessaires à la conservation des messages pouvant être indispensables ou simplement utiles en tant qu'éléments de preuve.

Section 5.2 - Internet

Il est rappelé que les connexions établies grâce à l'outil informatique mis à disposition par la Mission Locale sont présumées avoir un caractère professionnel. L'utilisation d'Internet à des fins privées est tolérée dans des limites raisonnables, à condition que la navigation n'entrave pas l'accès professionnel.

⁶ Il s'agit notamment des contenus contraires aux dispositions de la loi sur la liberté d'expression ou portant atteinte à la vie privée d'autrui (par exemple : atteinte à la tranquillité par les menaces, atteinte à l'honneur par la diffamation, atteinte à l'honneur par l'injure non publique, protection du droit d'auteur, protection des marques...).

⁷ Sous réserve du respect des conditions fixées par les articles 10 1369-1 à 1369-11 du code civil.

L'utilisation d'Internet (par extension intranet) constitue l'un des éléments essentiels d'optimisation du travail, de mutualisation et d'accessibilité de l'information au sein et en dehors du réseau de la Mission Locale.

Chaque Utilisateur-trice doit prendre conscience des risques que comporte Internet en matière de sécurité et de confidentialité.

Il est donc interdit de :

- communiquer à des tiers des informations techniques relatives au matériel de l'entreprise ;
- diffuser sur Internet des informations relatives à l'entreprise sauf les salarié-e-s ayant besoin de le faire dans le cadre de leur mission ;
- participer à des forums, à l'exception des forums professionnels ;
- participer à des conversations en ligne (chat) à l'exception des « chats professionnels ».

Il est interdit de consulter des sites non autorisés par la Mission Locale, à caractère violent, pornographique, pédophile, raciste ou incitant à la haine raciale, révisionniste, offensant ou diffamatoire et, de manière générale, tout site à caractère illicite.

Toute publication de pages d'information sur les sites internet ou intranet de la Mission Locale doit être validée par un responsable de site ou responsable de publication nommément désigné ⁽⁸⁾.

La Mission Locale se réserve le droit de filtrer ou d'interdire l'accès à certains sites, de procéder au contrôle a priori ou a posteriori des sites visités et des durées d'accès correspondantes. Cet accès n'est autorisé qu'au travers des dispositifs de sécurité mis en place par la Mission Locale ⁽⁹⁾.

Un système de sauvegarde des données est mis en place dans la Mission Locale. En conséquence, la suppression de données par l'Utilisateur-trice n'est pas absolue. Il en reste donc une copie :

- sur les dispositifs de sauvegarde ;
- sur les serveurs de traitement des données ;
- sur les pare-feux ;
- chez les fournisseurs d'accès

La Mission Locale se réserve le droit, à tout moment, de contrôler les connexions Internet des Utilisateur-trices.

Les règles de contrôle font l'objet d'une discussion avec les représentants du personnel.

Section 5.3 - Téléchargements et Pare-feu

Tout téléchargement de fichiers, notamment de sons ou d'images, sur Internet doit s'effectuer dans le respect des droits de la propriété intellectuelle tels que définis à l'article VI de la présente charte.

La Mission Locale se réserve le droit de limiter le téléchargement de certains fichiers pouvant se révéler volumineux ou présenter un risque pour la sécurité (virus susceptibles d'altérer le bon fonctionnement du système d'information, codes malveillants, programmes espions, ...).

La Mission Locale s'est dotée d'un « pare-feu » permettant de contrôler tout le trafic entrant et sortant (Internet et messagerie) et enregistrant toutes les traces des activités qui transitent par lui : sites

⁸ Aucune publication de pages d'information à caractère privé (pages privées ...) sur les ressources du système d'information de la Mission Locale n'est autorisée.

⁹ Des règles de sécurité spécifiques peuvent être précisées, s'il y a lieu, dans un guide d'utilisation établi par le service ou l'association.

internet visités, heure et durée de la visite, liste et nature des éléments téléchargés (textes, photos, vidéos, logiciels), messages transmis et reçus via la messagerie, texte du message, destinataire, objet, nature de la pièce jointe.

Le pare-feu filtre également les URL des sites définis comme non autorisés par la Mission Locale (voir point 4.1 - Règles d'utilisation).

Article 6 : Respect de la propriété intellectuelle

La Mission Locale rappelle que l'utilisation des ressources informatiques implique le respect de ses droits de propriété intellectuelle ainsi que ceux de ses partenaires et plus généralement, de tous tiers titulaires de tels droits.

En conséquence, chaque Utilisateur-trice doit :

- utiliser les logiciels dans les conditions des licences souscrites ;
- ne pas reproduire, copier, diffuser, modifier ou utiliser les logiciels, bases de données, pages web, textes, images, photographies ou autres créations protégées par le droit d'auteur ou un droit privatif, sans avoir obtenu préalablement l'autorisation des titulaires de ces droits.

Article 7 : Respect de la législation

L'utilisateur-trice est informé de la nécessité de respecter les dispositions légales ainsi que le règlement européen 2016-679 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données en particulier lors de la création de fichiers et de la collecte de données.

Chaque responsable de traitement se doit d'être en conformité avec la législation en matière de protection des données.

Conformément à la législation en matière de protection des données à caractère personnel, toute personne concernée par un traitement dispose, sous certaines conditions, d'un droit de rectification, d'effacement de ces informations, ou du droit de s'opposer ou de limiter leur utilisation. Droits qui peuvent s'exercer en s'adressant à la Mission Locale ou directement au Délégué à la Protection des Données (DPO) désigné par le responsable de traitement ou son représentant : dpo@ml31.org

La collecte des données à caractère personnel par le SI est guidée par le respect de deux principes protecteurs :

1-Le principe de transparence ou d'information des Utilisateur-trices selon lequel les Utilisateur-trices doivent être clairement informés des objectifs poursuivis lors de la mise en place d'outils de collecte de données les concernant, des destinataires des données et des modalités d'exercice de leurs droits d'accès et de suppression au titre de la loi Informatique et Libertés.

2-Le principe de proportionnalité qui n'autorise le contrôle des données émises par les Utilisateur-trices ou destinées aux Utilisateur-trices qu'à condition qu'il soit nécessaire à l'objectif poursuivi (sécurité, respect des droits et intérêts de la Mission Locale, prévention d'infractions pénales).

Article 8 : Limitation des usages

En cas de non-respect des règles définies dans la Charte et des modalités définies dans les guides d'utilisation établis par le service ou l'association, la 'personne juridiquement responsable' ⁽¹⁰⁾ pourra, sans préjuger des poursuites ou procédures de sanctions pouvant être engagées à l'encontre des Utilisateur-trices, limiter les usages par mesure conservatoire.

Tout abus dans l'utilisation des ressources mises à la disposition de l'Utilisateur-trice à des fins extraprofessionnelles est passible de sanctions.

Article 9 : Responsabilités- Sanctions

Le non-respect des dispositions contenues dans la présente charte entraîne la responsabilité personnelle de l'Utilisateur-trice s'il est prouvé que les faits fautifs lui sont personnellement imputables. Il est donc passible de sanctions disciplinaires telles qu'elles sont définies par l'article V-13 de la convention collective nationale des Missions Locales et par le règlement intérieur de la Mission Locale.

Le non-respect des lois et textes applicables en matière de sécurité des Systèmes d'Information est susceptible de sanctions pénales prévues par la loi.

Article 10 : Entrée en vigueur de la Charte – Dépôt et publicité

La Charte constitue une annexe au règlement intérieur. Elle a été soumise à la consultation préalable du CSE le 25 novembre 2022.

La charte est diffusée à l'ensemble des utilisateur-trices par note de service, affichée sur chaque site d'activité et, à ce titre, mise à disposition sur l'extranet. Tout nouvel utilisateur-trice-trice en est informé.

Elle sera communiquée à l'Inspection du travail d'ici le **30 novembre 2022**, déposée au secrétariat du Conseil des Prud'hommes de Toulouse et affichée à la même date.

Elle entre en application le **1er janvier 2023**.

Pour la Mission Locale Haute-Garonne
Madame Nadège CARREL
Directrice



¹⁰ Par « personne juridiquement responsable », il faut entendre toute personne ayant la capacité de représenter la Mission Locale