Charte d'utilisation des moyens informatiques et des réseaux et des moyens de communication

Vu loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés ;
Vu loi n°83-634 du 13 juillet 1983 portant droits et obligations des fonctionnaires ;
Vu la loi n°84-53 du 26 janvier 1984 relative à la fonction publique territoriale ;
Vu la loi n°2000-230 du 13 mars 2000 portant adaptation du droit de la preuve aux technologies de l'information et relative à la signature électronique ;
Vu loi n° 94-665 du 4 août 1994 relative à l'emploi de la langue française ;
Vu le décret n°88-145 du 15 février 1988 pris pour l'application de l'article 136 de la loi du 26 janvier 1984 modifiée portant dispositions statutaires relatives à la fonction publique territoriale et relatif aux agents contractuels de la fonction publique territoriale ;
Vu le Code des relations entre le public et l'administration ;
Vu le Code Pénal, pris notamment en ses articles 226-1 à 226-7, 226-15, 323-1 à 323-7 et 432-9 ;
Vu le Code Civil, pris notamment en ses articles 1363 à 1368 ;
Vu le Code de la Propriété Intellectuelle ;

Article 1 : Préambule

Le SMiTU met en œuvre des moyens d'information et de communication nécessaires à son activité, comprenant notamment des réseaux informatiques et téléphoniques.
Les agents, dans l'exercice de leurs fonctions, sont conduits à accéder à ces moyens et à les utiliser dans un cadre professionnel territorial.

Dans un but de transparence à l'égard des utilisateurs, de promotion d'une utilisation optimale, responsable et sécurisée des systèmes d'information, la présente charte pose les règles relatives à l'utilisation de ces ressources.
Cette dernière définit les obligations et les responsabilités des utilisateurs pour assurer le bon usage des systèmes informatiques (matériels) et des outils d'information et de communication (connexions et accès aux réseaux et bases de données du SMiTU) dans le respect des lois, de la confidentialité, du respect d'autrui et de l'intérêt du SMiTU.

Cette charte a pour fonction d'informer et de sensibiliser les agents sur les risques juridiques, économiques et techniques, que peuvent générer une mauvaise utilisation ou une utilisation imprudente de ces ressources.

La rédaction de cette charte doit donc réaliser la nécessaire conciliation entre les obligations auxquelles sont tenus le SMiTU vis-à-vis de ses agents et les obligations qui lui incombe en ce qui concerne le contrôle de leurs activités et la sécurité de leur service.

Article 2 : Objet

La présente charte est un code de déontologie formalisant les règles légales et de sécurité relatives à l'utilisation des moyens informatiques et des réseaux de communications au sein du SMiTU.

Cette charte s'applique à toute personne utilisant les moyens informatiques, y compris ceux dont le SMiTU autorise l'accès à distance (titulaire/non titulaire, stagiaire et élu).
Celle-ci s'applique également à tout prestataire extérieur ayant accès aux données et aux outils informatiques du SMiTU. Tout contrat avec un prestataire extérieur devra faire référence et comporter comme annexe la présente charte.

La charte s'applique à l'utilisation des ressources informatiques et téléphoniques fournis au personnel :

- Ordinateurs (fixes et portables)
- Tablettes
- Téléphones (fixes et portables)
- Système de messagerie
- Réseaux informatiques (serveurs, routeurs et connectique)
- Internet
- Photocopieurs et imprimantes
- Machine pour affranchir
- Fax
- Périphériques
- Logiciels
- Fichiers et base de données
- Badges

Article 3 : Droit et devoirs des agents

Tout agent travaillant au SMiTU dispose d'un droit d'accès au système d'information. Ce droit est strictement personnel et incessible.
Ces droits d'accès peuvent être modifiés ou retirés à tout moment, selon les besoins du service, et prennent fin lors de la cessation d'activité professionnelle.

L'utilisateur est responsable des ressources qui lui sont confiées dans le cadre de l'exercice de ses fonctions. Il doit concourir à la protection des dites ressources, en faisant preuve de prudence.
Tout agent s'engage à ne pas manipuler le matériel de façon anormale, ni d'introduire des « ressources extérieures » matérielles ou logicielles qui pourraient porter atteinte à la sécurité du système informatique.

L'usage de ces outils de communication ne modifie en rien les obligations de validation et d'information vis-à-vis de la hiérarchie.

L'agent doit respecter l'intégrité et la confidentialité des données et ne pas perturber la disponibilité du système informatique. 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, le droit à l'image des personnes, l'exposition des mineurs aux contenus préjudiciables...

La continuité du service étant une priorité, l'agent s'interdit d'appliquer des mesures de sécurité non validées par la Direction Générale et qui auraient pour conséquence de rendre inaccessibles des informations intéressant le bon fonctionnement du SMiTU.

L'utilisateur doit respecter les obligations de réserve, de discrétion et de secret professionnel conformément aux droits et obligations des agents publics tels que définis par la loi du 13 juillet 1983 portant droits et obligations des fonctionnaires et la loi du 26 janvier 1984 relative à la fonction publique territoriale.

Article 4 : Engagements de la collectivité et du prestataire

Le personnel habilité doit veiller à assurer le fonctionnement normal et la sécurité des réseaux et systèmes. Ces personnes peuvent être conduites par leurs fonctions à avoir accès à l'ensemble des informations relatives aux utilisateurs, y compris celle qui sont enregistrées sur le disque dur du poste de travail dans le respect du secret professionnel. Un tel accès n'est contraire à aucune disposition de la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.
Ils doivent respecter la confidentialité des « données utilisateurs » auxquelles ils pourraient être amenés à accéder, avec l'accord de l'utilisateur, pour diagnostiquer ou corriger un problème spécifique, ainsi que des fichiers, courriers et sorties imprimantes lors de leurs tâches d'administration.

Le SMiTU doit mettre à disposition les ressources informatiques matérielles et logicielles nécessaires au bon déroulement de la mission des agents.
Il doit effectuer les mises à jour nécessaires des matériels et des logiciels composant le système informatique afin de maintenir le niveau de sécurité en vigueur.
Le SMiTU doit assurer la sauvegarde de l'ensemble des données ainsi que des ressources.
Pour finir, il doit faire respecter les droits et responsabilités des agents sur ces dernières.

L'accès à la salle technique informatique est strictement réservé à la direction. Tout prestataire devant intervenir dans cette salle devra obligatoirement être accompagné d'un membre de ce service.

Article 5 : Modalités d'usage

Il est toléré un usage raisonnable des ressources à des fins personnelles, à la condition expresse de respecter les dispositions de la présente charte. Cet usage personnel des ressources ne pourra être qu'occasionnel et limité dans le temps et par son objet.

L'utilisateur veille à distinguer clairement les documents, courriers, messages... qu'il considère comme personnels, des documents professionnels, notamment en les rangeant dans des dossiers distincts nommés « Privé », « Personnel » ou « Confidentiel » et/ou en faisant figurer ce mot en tête du nom des documents et de l'objet des courriels.
Tout document ou courriel ne respectant pas cette règle sera considéré comme professionnel.

En cas d'absence de l'agent, la continuité du service doit être assurée. L'agent doit veiller à ce que le service puisse accéder aux documents, logiciels et dossiers indispensables à l'activité.
En cas de départ définitif ou de mutation, le successeur récupère les documents de travail ainsi que les messages, à l'exception des documents et messages privés.

Article 5-1 : Les postes informatiques

Un système informatique est mis à disposition de chaque utilisateur (matériel, système d'exploitation et logiciels). Le matériel informatique est fragile, il faut donc en prendre soin.
Toute installation logicielle sera à la charge de la personne compétente et désignée par l'autorité territoriale.
L'utilisateur doit signaler tous dysfonctionnements ou anomalies à la direction.

En cas d'absence, même momentanée, l'utilisateur doit quitter les applications et verrouiller systématiquement son PC.
A la fin de la journée de travail, l'utilisateur doit quitter les applications, arrêter le système, éteindre l'écran et l'imprimante.
L'utilisateur doit procéder régulièrement à l'élimination des fichiers non-utilisés et à l'archivage dans le but de préserver la capacité de mémoire.
L'utilisateur doit conserver ses fichiers sur les espaces réseaux qui lui sont attribués. Aucun fichier ne doit être conservé sur le disque dur du poste de travail. L'employeur ne peut pas prendre connaissance des fichiers ou dossiers portant la mention « privé », « confidentiel » ou « personnel » (Cass 28 octobre 2006 n°04-47400).

L'employeur peut avoir accès au contenu d'une clé USB personnelle connectée à l'ordinateur professionnel. En effet, dès lors qu'elle est connectée à un outil informatique mis à la disposition de l'agent par la collectivité, la clé USB appartenant à l'agent est présumée utilisée à des fins professionnelles, de sorte que l'employeur peut avoir accès aux fichiers non-identifiés comme personnels qu'elle contient, hors la présence de l'agent. Telle est la solution inédite retenue par la chambre sociale de la Cour de cassation dans un arrêt n°11-28649 du 12 février 2013.

Il est interdit d'effectuer des copies de logiciels pour quelque usage que ce soit, hormis une copie de sauvegarde dans les conditions prévues par le code de la propriété intellectuelle, ou de contourner les restrictions d'utilisation de ce logiciel.
Aucune installation de logiciel n'est de principe, autorisée, en dehors des autorisations accordées par la direction générale.

Article 5-2 : La messagerie électronique

Une équivalence juridique est établie entre le courrier électronique et le courrier sur support papier (Code des relations entre le public et l'administration). Ils doivent en conséquence être traités dans les mêmes délais.

Chaque agent dispose d'une adresse électronique professionnelle déterminée.
L'utilisation de la messagerie est réservée à des fins professionnelles. Néanmoins, il est toléré un usage modéré de celle-ci pour des besoins personnels et ponctuels.
L'utilisateur est tenu de la consulter au minimum une fois par jour, hormis en période d'absence, et se doit de les traiter.
Chacun est responsable des messages envoyés ou reçus, et doit utiliser la messagerie dans le respect des missions et fonctions qui lui sont dévolues et des règles élémentaires de courtoisie et de bienséance.
Une signature personnelle est attachée à chaque courrier. Celle-ci comporte :

- Les nom et prénom de l'expéditeur
- La qualité
- Le numéro de téléphone et son adresse mail
- Les coordonnées postales du SMiTU

Tout courrier électronique est réputé professionnel et est donc susceptible d'être ouvert par l'autorité territoriale ou le référent informatique. Les courriers à caractère personnel doivent expressément porter la mention « personnel », « confidentiel » ou « privé » dans leur objet. Ces derniers ne pourront alors être ouverts par l'autorité territoriale ou le référent informatique, que pour des raisons exceptionnelles de sauvegarde de la sécurité ou de préservation des risques de manquement de droit des tiers ou à la loi (Cour d'Appel de Rennes, 14 janvier 2010, n°08/02209).
En revanche, l'Autorité territoriale ne peut consulter les emails provenant de l'adresse mail personnel de l'agent même si cette messagerie est accessible sur l'ordinateur professionnel (Cass soc 7 avril 2016, n°14-27949).

L'utilisateur s'engage à ne pas diffuser d'informations pouvant porter atteinte à la dignité humaine ou à la vie privée ou aux droits et image de chacun ou faisant référence à une quelconque appartenance à une ethnie, religion, race ou nation déterminée.

L'utilisateur doit éviter de surcharger le réseau d'informations inutiles. Les messages importants sont à conserver et/ou à archiver, les autres à supprimer. Le dossier « éléments supprimés » doit être vidé périodiquement.

En cas d'absence prévisible, l'utilisateur devra mettre en place un message automatique indiquant la date de retour prévue, ainsi que les coordonnées de la personne à contacter en cas d'urgence. Un agent du service doit pouvoir gérer les messages pendant son absence.

Les courriels sont notamment protégés par le secret de la correspondance. Nul ne peut en prendre connaissance sans autorisation de l'émetteur ou du destinataire, à l'exception d'un juge d'instruction ou d'un officier de police judiciaire, qui peut, en cas de plainte, procéder à la saisie des données nécessaires à la manifestation de la vérité.

Un message électronique peut constituer une preuve, et peut engager fermement son expéditeur et son destinataire. Il existe un risque réel pour qu'un agent prenne des engagements qu'il faudra ensuite respecter.

Avant tout envoi, il est nécessaire de vérifier l'identité des destinataires du message et de leur qualité à recevoir communication des informations transmises
Pour une question de sécurité, il est impératif de ne pas ouvrir de pièce jointe d'un courriel dont on n'est pas absolument certain de sa provenance.

Article 5-3 : Internet

L'utilisation d'internet est réservée à des fins professionnelles. Néanmoins, il est toléré un usage modéré de l'accès à internet pour des besoins personnels, en dehors du temps de travail, à condition que la navigation n'entrave pas l'accès professionnel.
Seuls ont vocation à être consultés les sites internet présentant un lien direct et nécessaire avec l'activité professionnelle.

L'utilisateur s'engage lors de ses consultations Internet à ne pas se rendre sur des sites portant atteinte à la dignité humaine (pédophilie, pornographie, apologie des crimes contre l'humanité et provocation à la discrimination, à la haine ou à la violence à l'égard d'une personne ou d'un groupe de personnes à raison de leur origine ou de leur appartenance ou non à une ethnie, une nation, une race ou une religion déterminée...).
Le téléchargement, en tout ou partie de données numériques soumis aux droits d'auteurs ou à la loi du copyright (fichiers musicaux, logiciels propriétaires...) est strictement interdit.
Pour éviter les abus, l'autorité territoriale peut procéder, à tout moment, au contrôle des connexions entrantes et sortantes et des sites les plus visités (Cass soc 9 juillet 2008 n°06-45-800).

L'utilisation des réseaux sociaux est réservée à des fins professionnelles aux agents qui ont été habilités à parler au nom de la collectivité.

Article 5-5 : Téléphone

L'utilisation des téléphones fixes et portables est réservée à des fins professionnelles. Néanmoins, un usage ponctuel du téléphone pour des communications personnelles locales est toléré, à condition que cela n'entrave pas l'activité professionnelle.
L'autorité territoriale peut procéder au contrôle de l'ensemble des appels émis.
L'utilisation des téléphones portables personnels doit rester occasionnelle et très discrète. Celle-ci ne doit pas gêner le travail des autres agents.

Il n'est pas obligatoire de répondre aux appels ou aux mails reçus sur un téléphone portable professionnel en dehors du temps de travail (soir, week-end et congés).
L'agent quittant définitivement la collectivité doit restituer le téléphone portable professionnel.

Article 6 : Mesures de surveillance et sanctions

Le directeur général pourra requérir de l'administrateur des mesures de surveillance particulières portant sur les ressources informatiques ou téléphoniques lorsque des dérives de nature à porter préjudice à l'intérêt de la structure sont constatées, sans porter atteinte toutefois aux informations personnelles de l'utilisateur et dans le respect des lois en vigueur.

L'utilisateur est informé que sa propre responsabilité, celle de son chef de service, et la responsabilité du SMiTU peuvent être engagées civilement et pénalement du fait de son comportement. Il veillera donc à respecter les lois et règlements en vigueur, ainsi que les règles d'utilisation, de sécurité et de bon usage décrites dans la présente charte.

L'agent est informé que tout abus de l'utilisation non professionnelle pourra faire l'objet de sanctions. Tout utilisateur ne suivant pas les règles et obligations rappelées dans cette charte pourra se voir suspendre l'accès aux ressources informatiques, téléphoniques, ou à certains services (internet, messagerie...).

En cas de manquement grave et d'intention manifeste de nuire au bon fonctionnement des ressources ou à l'activité des services, il sera passible de sanctions administratives disciplinaires proportionnelles à la gravité des manquements constatés. Celui-ci est informé par sa hiérarchie dans un bref délai des faits qui lui sont reprochés, sauf risque ou évènement particulier.
Tout utilisateur n'ayant pas respecté les lois pourra être poursuivi civilement et/ou pénalement.

Pour des nécessités de sécurité, de maintenance et de gestion technique, l'utilisation des ressources matérielles ou logicielles ainsi que les échanges via le réseau peuvent, sous le contrôle du responsable informatique et de l'autorité territoriale, être analysés et contrôlés dans le respect de la législation applicable et notamment de la loi relative à l'informatique, aux fichiers et aux libertés. La prise de contrôle des postes de travail pour détecter et réparer à distance les pannes éventuelles peut être pratiquée par la collectivité ou le prestataire.

Il est expressément rappelé qu'accéder sans autorisation à des informations d'autres utilisateurs, les copier, les divulguer, les modifier ou les effacer, peut être sanctionnée pénalement.

Article 7 : Modalités d'application

Cette charte est un élément du règlement intérieur. Ce règlement s'applique à l'ensemble des agents, tous statuts confondus, aux élus, stagiaires, visiteurs, et plus généralement à tous les utilisateurs des moyens informatiques et téléphoniques du SMiTU.

Dès l'entrée en vigueur de la présente charte, chaque agent de la collectivité s'en verra remettre un exemplaire, il devra en prendre immédiatement connaissance et devra s'engager à la respecter (cf récépissé) et sera tenu sans délai au respect des règles qui y sont édictées.

Afin de recueillir une adhésion forte et une efficacité renforcée de la charte, celle-ci sera accompagnée d'une démarche pédagogique auprès du personnel concerné, accompagnée d'une large diffusion tant collective qu'individuelle, par tout moyen utile afin que nul ne puisse en ignorer son existence et son contenu.

Touchant à l'organisation des services, elle a été adoptée par délibération du Comité syndical, après consultation du Comité technique du Centre de gestion de la Moselle.
Elle pourra être complétée ou modifiée par l'autorité territoriale, l'avis du Comité technique sera à nouveau demandé.

Il sera fait mention de cette charte dans les contrats de travail au titre du respect du règlement intérieur.

Chaque nouvelle version sera validée et diffusée de la même manière. La version en vigueur sera la plus récente.

Le Président du SMiTU

1A av. Gabriel Lippmann 57970 YUTZ
SYNDICAT MIXTE DES TRANSPORTS URBAINS THIONVILLE FENSCH
SMITU

Monsieur Jean-Marie MIZZON

Récépissé de la charte informatique

Je soussigné(e)

Nom :

Prénom :

Service :

Fonction :

Utilisateur des moyens informatiques et réseaux du SMiTU, déclare avoir pris connaissance de la présente charte et m'engage à la respecter.

Fait à Yutz, le
(En deux exemplaires : un pour l'agent et un pour la collectivité).

Signature