CHARTE INFORMATIQUE

SOMMAIRE

Préambule

La présente charte définit les règles d'usage et de sécurité du système d'information que les utilisateurs s'engagent à respecter. Elle précise les droits et devoirs de chacun. C'est un code de conduite dont l'objet est de définir les conditions générales d'utilisation des moyens de communication et outils informatiques mis en œuvre par Martinique Transport (MT).

Le terme « utilisateur » désigne toute personne ayant accès, dans le cadre de l'exercice de son activité professionnelle, aux ressources du système d'information qu'il soit agent de Martinique Transport ou d'un prestataire ayant un contrat avec l'établissement.

On désigne par système d'information (SI) l'ensemble des outils, progiciels, logiciels et tout autre matériel informatique mis à la disposition des utilisateurs (y compris le matériel personnel des utilisateurs connecté au réseau de l'administration) pour répondre à leurs besoins professionnels en matière de traitement des données, de circulation et de diffusion de l'information visant à améliorer la qualité de travail et de la prise de décision au sein de Martinique Transport.

Il est rappelé qu'en cas d'atteinte à l'un des principes protégés par la loi, la responsabilité administrative, pénale et/ou civile de l'agent ainsi que celle de l'établissement est susceptible d'être recherchée.

1. Objectif

La présente charte informatique est un code de déontologie qui vise à exposer les principales règles et précautions que tout utilisateur du SI de Martinique Transport doit respecter concernant l'utilisation des ressources informatiques mises à sa disposition.

La charte informatique a pour objectif de fixer les dispositions visant à assurer, l'efficacité et la sécurité du SI, la protection des données personnelles et de fournir aux utilisateurs les bonnes pratiques à observer dans le respect de leur vie privée.

2. Champs d'application

2.1. Utilisateurs concernés

Sauf mention contraire, la présente charte s'applique à l'ensemble des agents de Martinique Transport et des élus et/ou partenaires se connectant sur le réseau de Martinique Transport.

2.2. Système d'information et de communication

Le système d'information et de communication de Martinique Transport est notamment constitué des éléments suivants : ordinateurs (fixes ou portables), périphériques y compris clés USB, assistants personnels, réseau informatique (serveurs, routeurs et connectique), photocopieurs, télécopieurs, téléphones, smartphones, tablettes et clés 3G/4G, logiciels, fichiers, données et bases de données, système de messagerie, connexion internet, intranet, extranet, abonnements à des services interactifs. Pour des raisons de sécurité du réseau, est également considéré comme faisant partie du système d'information et de communication le matériel personnel des salariés connecté au réseau de l'entreprise, ou contenant des informations à caractère professionnel concernant l'entreprise.

2.3. Postes de travail

Un ensemble de matériel, système d'exploitation, logiciels est mis à disposition de l'agent lui permettant d'assurer ses missions.

Le matériel mis à disposition demeure la propriété de Martinique Transport.

L'agent n'exerçant plus de fonctions au sein l'établissement doit restituer le matériel qui lui avait été attribué. Un formulaire de restitution de ces matériels sera renseigné par ses soins et supervisé par la Direction des Systèmes d'Information.

2.4. Terminaux mobiles et téléphonie fixe

Des terminaux mobiles (téléphones, tablettes…) sont attribués sous justification et validation hiérarchique.

Toute utilisation de terminaux mobiles à des fins personnelles doit rester occasionnelle.

L'autorité territoriale peut vérifier qu'il n'est pas fait d'utilisation abusive des lignes téléphoniques professionnelles pour des appels personnels, dans le respect de la vie privée et libertés de l'agent. Les lignes attribuées aux représentants du personnel (délégués du personnel, délégués syndicaux, membres du comité d'entreprise, etc…) sont exclues de ces contrôles.

Le contrôle des appels émis pourra être effectué dans le cadre d'une procédure administrative ou d'une enquête judiciaire.

Deux techniques de contrôle peuvent être utilisés :

- Le serveur de téléphonie qui permet d'orienter les appels entrants et sortants et d'enregistrer les numéros de téléphone sortants. Il peut donc identifier les communications téléphoniques non professionnelles.
- Les relevés de téléphonie fixe ou mobile : l'opérateur transmet chaque mois les relevés téléphoniques à l'employeur. Celui-ci peut demander des relevés détaillés par poste et les numéros composés, **en cas d'utilisation manifestement abusive (harcèlement, appels de numéros surtaxés hors du cadre d'obligations de service, etc..)**.

2.5. Messagerie électronique

La messagerie électronique est un moyen d'amélioration de la communication au sein des organisations de travail et avec des tierces personnes.

La messagerie est accessible depuis tout équipement disposant d'un accès d'internet, personnel ou professionnel, à l'adresse suivante : https://portal.office.com

2.5.1. Utilisation professionnelle de la messagerie

Chaque utilisateur du SI dispose, pour l'exercice de son activité professionnelle, d'une adresse de messagerie électronique attribuée par la Direction des Systèmes d'Information. Cette messagerie est destinée à un usage strictement professionnel. En conséquence, dans le respect de la loi n° 91-646 du 10 juillet 1991 relative au secret des correspondances émises par la voie des communications électroniques, l'employeur est en droit d'y accéder si les nécessités du service l'exigent (à titre non exhaustif : absence prolongée de l'agent, recherche de virus, sous requête d'une autorité judiciaire…).

L'accès à la messagerie sera supprimé pour un agent n'exerçant plus de fonctions au sein de l'établissement.

Les messages électroniques comportant un quelconque caractère contraire à la loi, à l'ordre public, à la morale, aux bonnes mœurs, à la réputation ou à la considération de l'établissement ou de toute autre personne sont strictement interdits.

L'adresse de messagerie de l'agent sera de la forme :

« prenom.nom@martiniquetransport.mq »

Le nom retenu par défaut est le nom patronymique sauf homonyme ou indication expresse contraire de l'agent. Il en sera de même pour le prénom qui sera par défaut le 1er prénom sauf indication expresse contraire de l'agent.

Les messages électroniques reçus sur la messagerie professionnelle font l'objet d'un contrôle antiviral et d'un filtrage anti-spam, ce qui n'exclut pas la vigilance des utilisateurs du SI.

Aux termes des articles 331-1 à 335-10 du code de la propriété intellectuelle, la liste de diffusion et l'annuaire électronique de l'ensemble du personnel, développés par l'établissement demeurent sa propriété exclusive et leur diffusion est interdite.

La diffusion de messages en masse n'est pas autorisée. Tout envoi exceptionnel de message à l'ensemble du personnel doit être préalablement autorisé par l'administration.

2.5.2. Exception à l'utilisation professionnelle de la messagerie

Les messages à caractère personnel sont tolérés, à condition que les messages envoyés soient signalés par la mention "Privé" dans leur objet et soient classés, dès l'envoi, dans un dossier lui-même dénommé " Privé ". Les messages reçus doivent être également classés, dès réception, dans un dossier lui-même dénommé " Privé ". En cas de manquement à ces règles, les messages sont présumés être à caractère professionnel. Cet usage à caractère exceptionnel, ne doit pas perturber l'activité professionnelle, ni entacher la réputation de l'établissement.

En cas d'usage privé abusif (fréquence des messages reçus ou envoyés, volume des données échangées, type-taille-format des pièces jointes, nombre de destinataires...) ou malveillant avéré de la messagerie, l'autorité territoriale peut procéder, à tout moment, à des restrictions d'usage (blocage de l'accès, limitation du nombre de destinataires...) sur les messages entrants ou sortants.

2.5.3. Utilisation de la messagerie sur mobile

En raison de la politique de sécurité de Microsoft, la configuration de la messagerie professionnelle sur un appareil nomade, professionnel ou personnel, permet aux administrateurs du SI d'effectuer des opérations techniques sur cet appareil (réinitialisation à distance, limitation de la diffusion de documents internes et aux "copier-coller" de texte aux seules applications professionnelles...). Cette manipulation peut être effectuée par l'agent avec le support de la Direction des Systèmes d'Information.

2.5.4. Spécificités applicables aux représentants du personnel et aux organisations syndicales

La messagerie électronique est réservée aux échanges de courriers. Toute transmission de documents, tracts ou textes quel que soit son format n'est autorisée qu'aux adhérents ou sympathisants qui en accepte l'envoi. Un espace de communication sur l'intranet est réservé à cet effet.

Conformément au décret n°85-397 du 3 avril 1985 et à la circulaire du 20 janvier 2016, l'autorité territoriale pourra utilement se référer aux dispositions prévues dans la fonction publique de l'Etat en application du décret n° 2014-1319 du 4 novembre 2014 relatif aux conditions d'accès aux technologies de l'information et de la communication et à l'utilisation de certaines données par les organisations syndicales et de son arrêté d'application du 4 novembre 2014.

La communication d'origine syndicale sur le réseau informatique du service doit être compatible avec les exigences de bon fonctionnement du réseau informatique et ne pas entraver l'accomplissement du service. Les échanges électroniques entre les agents et les organisations

syndicales sont confidentiels. Dans le respect des règles générales de sécurité du système d'information, les messages électroniques en provenance des organisations syndicales parviennent à leurs destinataires sans blocage ni lecture par un tiers. L'administration ne recherche pas l'identification des agents qui se connectent aux pages d'information syndicale accessibles sur le site intranet. Elle ne collecte pas de données à des fins de mesure d'audience sur ces pages.

Les conditions de mise à disposition de la messagerie électronique sont définies en fonction de l'architecture du réseau de l'établissement, ainsi que des impératifs techniques et de sécurité du système d'information qui peuvent nécessiter de contingenter les envois en nombre.

L'envoi d'E-pétition n'est pas autorisé.

2.5.5. Listes de diffusion : Groupes Office365 et équipes Teams

La Direction des Systèmes d'Information met à disposition des agents groupes Office365 ou des équipes Teams permettant d'envoyer un message à un groupe de personnes identifiées (DGA MT, Direction(s) MT, Chefs de service MT…).

Afin d'éviter les erreurs ou les abus, certaines listes de diffusion ne sont accessibles qu'à certains agents dûment identifiés.

Pour toute demande de création/modification/suppression de liste de diffusion, il y a lieu de contacter le support informatique.

Spécificités applicables aux représentants du personnel et organisations syndicales
Conformément à l'article 4-1 du Décret du 3avril 1985 (précité) modifié par le Décret n° 2014-1624 du 24 décembre 2014 relatif à l'exercice du droit syndical dans la fonction publique territoriale *« Les conditions d'utilisation par les organisations syndicales, au sein d'une collectivité ou d'un établissement, des technologies de l'information et de la communication ainsi que de certaines données à caractère personnel contenues dans les traitements automatisés relatifs à la gestion des ressources humaines, sont fixées par décision de l'autorité territoriale, après avis du comité technique, dans le respect des garanties de confidentialité, de libre choix et de non-discrimination auxquelles cette utilisation est subordonnée. »*

La liste de diffusion doit répondre aux obligations du Règlement Général de la Protection des Données personnelles (RGPD). Les syndicats devront donc se conformer aux préconisations du délégué à la protection des données (DPO).

L'établissement s'engage à n'exercer aucun contrôle sur les listes de diffusion ainsi constituées, garantissant ainsi le respect de l'opinion d'un agent à l'égard d'une organisation syndicale, de son appartenance, ou de son choix d'accepter ou non de recevoir des messages à caractère syndical.

2.5.6. Boîte de services

Pour des besoins de service, il est possible de créer des boîtes aux lettres de services disponibles pour les agents dûment identifiés (Support informatique, Communication Interne, Inscription Scolaire…).

Pour toute demande de création/modification/suppression de boîte aux lettres de services, contacter le support Informatique.

2.6 Support Web (Internet, Intranet, réseaux sociaux, Web TV)

Dans le cadre de leur activité, les utilisateurs du SI ont accès à Internet via un navigateur web (Edge, Firefox, Chrome, Safari…).

Il est rappelé que les utilisateurs du SI ne doivent en aucun cas se livrer à une activité illicite, ou sans lien avec l'activité professionnelle et/ou portant atteinte aux intérêts de l'établissement.

L'utilisation d'Internet est réservée à des fins professionnelles. Néanmoins, il est toléré en dehors des heures de travail un usage modéré de l'accès à Internet pour des besoins personnels à condition que la navigation n'entrave pas l'accès professionnel.

Les utilisateurs du SI s'engagent lors de leurs consultations Internet à ne pas se rendre sur des sites portant atteinte à la dignité humaine (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 leurs origines ou de leur appartenance ou non appartenance à une ethnie, une nation, une race ou une religion déterminée).

Pour des raisons de sécurité et de règlementation, certaines catégories de sites ou sites web sont inaccessibles sur le réseau de l'établissement : contenus liés aux drogues, à la pornographie, aux activités illégales, aux activités de piratages et aux sites de téléchargements de spywares, adwares ou virus.

Une liste des catégories additionnelles à proscrire sera soumise à l'avis du Comité Technique et la DSI sera en charge d'implémenter ces restrictions.

La contribution des utilisateurs du SI à des forums de discussion, systèmes de discussion instantanée, blogs, sites est interdite. Elle peut être autorisée, sous réserve d'autorisation préalable de la Direction Générale. Un tel mode d'expression est susceptible d'engager la responsabilité de l'établissement, une vigilance renforcée des agents est donc indispensable.

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.

Tout abonnement payant à un site web ou à un service via Internet, au nom de l'établissement, doit faire l'objet d'une autorisation préalable de l'autorité territoriale. Tout achat personnel en ligne générant des frais pour l'établissement est proscrit.

Pour éviter les abus, l'autorité territoriale peut procéder, à tout moment, au contrôle des connexions entrantes et sortantes des sites les plus visités.

Toute saisie d'information impliquant directement l'établissement sur un site Internet nécessite l'autorisation préalable de l'autorité territoriale.

Toute utilisation de ses coordonnées professionnelles sur Internet engage la responsabilité de l'utilisateur vis-à-vis de l'établissement sur les propos émis sauf usage de la mention : « Le contenu de ce message n'engage que son auteur et en aucun cas Martinique Transport ».

L'utilisation des services de messagerie instantanée est autorisée, sous réserve que les outils soient ceux installés par l'établissement.

L'établissement dispose par ailleurs de :

- un site Internet accessible à partir d'un navigateur web à l'adresse suivante : http://www.martiniquetransport.mq
- un site intranet accessible uniquement sur le réseau de l'établissement
- des pages sur les réseaux sociaux (Facebook, LinkedIn, Instagram...)
- une web tv, YouTube.

L'ensemble de ces moyens de communication sont sous la responsabilité de la Direction de la Communication. Aussi, pour toute remarque ou suggestion, il y a lieu de contacter la Direction de la Communication.

2.7 Espaces de stockage et de sauvegardes

Un groupe Office365 propre à chaque Direction dispose d'un espace de stockage, communément appelé partage réseau, dans lequel les fichiers sont organisés en répertoires et sous-répertoires. Les autorisations d'accès doivent être validées par le supérieur hiérarchique en fonction de l'organigramme.

Il est recommandé de sauvegarder les fichiers de travail sur ces partages réseaux car seuls ceux-ci sont sauvegardés par la Direction des Systèmes d'Information.

Le respect de ces pratiques permettra à la DSI, en cas de perte de fichiers sur les partages réseaux, de restaurer ces données. Dans ces cas précis, il convient de contacter le support informatique.

Chaque agent dispose d'un partage réseau OneDrive personnel. Ces partages seront supprimés pour un agent n'exerçant plus de fonctions au sein de l'établissement.

De manière générale, il convient :

- d'enregistrer vos documents sur des partages réseaux sauvegardés.
- d'enregistrer les fichiers avec un nom clair, concis et significatif pour faciliter les recherches.

Les partages réseaux mis à disposition par la Direction des Systèmes d'Information sont exclusivement destinés à un usage professionnel. En cas de manquement à cette règle, la DSI pourra procéder à la suppression des fichiers non-professionnels sur le réseau.

2.8 Impression et Numérisation

Les imprimantes et photocopieurs réseaux sont la propriété de l'établissement. Sauf indication contraire, ils sont donc utilisables par tout personnel de l'établissement.

Le paramétrage des imprimantes et des photocopieurs est effectué par la Direction des Systèmes d'Information. Les équipes de la DSI configurent les impressions, depuis les postes informatiques appartenant au domaine de Martinique Transport, vers les matériels d'impression (photocopieurs multifonctions, imprimantes).

De manière générale, ce type de matériel est mutualisé et les attributions individuelles sont à proscrire. Sur certains équipements, la confidentialité des impressions est garantie par la fonction d'impression sécurisée (via un code PIN).

2.9 Travail collaboratif

Pour permettre le travail collaboratif, plusieurs solutions sont disponibles (Office 365, Teams, SharePoint…).

Seuls les outils mis à disposition par l'établissement peuvent être utilisés, car ils respectent la sécurité du SI. Le cas échéant, contacter le support Informatique en précisant votre besoin.

3. Règles générales d'utilisation du Système d'Information

Tout utilisateur du SI est responsable de l'utilisation qu'il fait des ressources informatiques, ainsi que du contenu de ce qu'il affiche, télécharge ou envoie et s'engage à ne pas effectuer d'opérations qui pourraient avoir des conséquences néfastes sur le fonctionnement du réseau. Il doit en permanence garder à l'esprit que c'est sous le nom de l'établissement qu'il se présente sur internet et doit se porter garant de l'image de l'institution.

3.1. Droits et devoirs des agents

3.1.1 Accès réglementé aux ressources

L'accès à certains éléments du Système d'Information (comme la messagerie électronique ou téléphonique, les sessions sur les postes de travail, le réseau, certaines applications ou services interactifs) est protégé par des paramètres de connexion (identifiant, mot de passe). Ces paramètres sont personnels à l'utilisateur et doivent être gardés confidentiels. Ils permettent en particulier de contrôler l'activité des utilisateurs. Ils ne doivent être communiqués à personne, ni responsable hiérarchique, ni informatique. Dans la mesure du possible, ces paramètres doivent être mémorisés par l'utilisateur et ne pas être conservés, sous quelque forme que ce soit. En tout état de cause, ils

ne doivent pas être transmis à des tiers ou aisément accessibles. Ils doivent être saisis par l'utilisateur à chaque accès et ne pas être conservés en mémoire dans le système d'information. Lorsqu'ils sont choisis par l'utilisateur, les paramètres doivent respecter un certain degré de complexité et être modifiés régulièrement. Des consignes de sécurité sont élaborées par la direction ou la direction informatique afin de recommander les bonnes pratiques en la matière. Aucun utilisateur ne doit se servir pour accéder au système d'information de l'entreprise d'un autre compte que celui qui lui a été attribué. Il ne doit pas non plus déléguer à un tiers les droits d'utilisation qui lui sont attribués.

3.1.2 Une déclaration des casses, pertes et vols

Dans le cas malheureux où un matériel fourni par MARTINIQUE TRANSPORT devait être perdu ou volé :

- L'utilisateur doit commencer par établir l'inventaire de tout ce qui lui a été volé ou perdu ; non seulement son matériel privé ou de MARTINIQUE TRANSPORT (ordinateur, tablette, smartphone), mais également ses objets personnels, tels que cartes bancaires et de crédit, cartes d'identité, abonnements, objets de valeur, etc., puis déclarer sans délai le vol dans sa globalité à la police.
- Le vol, la casse ou la perte de matériel utilisé dans le cadre professionnel doit être communiqué sans délai à la DSI à l'adresse support.informatique@martiniquetransport.mq.
- La DSI commence par demander à l'utilisateur si d'autres utilisateurs de MT se sont connectés avec leur nom d'utilisateur ou ont utilisé la machine volée par le passé. Toute connexion laisse une trace numérique sur la machine (mots de passe en cache, cookies, etc.), qui peut être exploitée à mauvais escient. Dès lors, il est important de prendre les mesures appropriées, non seulement envers l'utilisateur principal de la machine volée, mais aussi envers les autres utilisateurs ayant utilisé cette machine.
- Une fois cette liste obtenue, la DSI vérifie auprès de l'utilisateur si des données personnelles au sens de la loi se trouvaient sur la machine au moment du vol. Si tel est le cas, l'information est transmise à la CNIL.
- La DSI va ensuite vérifier si le matériel volé fait partie de l'inventaire de la DSI. Si oui, il démarre la procédure de traitement de vol de matériel MT. Si non, il démarre la procédure de traitement de vol de matériel privé
- En cas de vol d'effets personnels, l'utilisateur ne doit pas oublier d'informer les organes compétents (par exemple, institutions financières pour bloquer les cartes bancaires et de crédit, autorités en cas de vol de cartes d'identité, etc.). L'utilisateur doit également informer toutes les personnes, de MT ou non, qui auraient pu utiliser la machine volée avec des données privées (par exemple, achat sur Internet avec paiement par carte de crédit). Enfin, la DSI informe également l'utilisateur de l'importance de changer tous les mots de passe de ses comptes privés (par exemple, Google, LinkedIn, Facebook, etc.).

En cas de casse, l'utilisateur se verra remettre un matériel de substitution qui pourra être temporaire ou définitif qui lui permettra d'assurer la continuité de ses missions. La DSI assistera l'utilisateur, sur la migration et la sauvegarde de données contenu sur le matériel cassé avant sa prise en charge pour une réparation ou une mise au rebut.

3.1.3 Traitement d'un vol/perte de matériel

Sitôt après réception de la liste des utilisateurs concernés, la DSI démarre la procédure de traitement du vol/perte :

- la DSI informe la Direction des Affaires Juridiques qui annonce le vol à la compagnie d'assurance avec laquelle travaille MARTINIQUE TRANSPORT (MT) et suit le traitement du cas, puis établit l'inventaire des licences logicielles de MT qui étaient activées sur la machine volée/perdue. A la fin du processus, la DSI met à jour son inventaire (mutation de la machine volée et saisie de la machine de remplacement) ;

- la DSI prépare une machine de remplacement pour l'utilisateur, selon la procédure d'installation standard ;

- sur la base des informations reçues, la DSI bloque temporairement le compte non seulement de l'utilisateur principal de la machine, mais aussi de chaque utilisateur s'étant servi de cette machine, afin que ces comptes ne puissent pas être utilisés à mauvais escient par la personne ayant volé/récupéré la machine. Le-s compte-s sont réactivé-s dès que le-s utilisateur-s ont changé leur mot de passe. Le Support DSI se tient à disposition des employés, pour les aider dans cette procédure. Le cas échéant, la machine volée est également sortie du domaine MT ;

- sur la base des informations reçues, la DSI active une alarme sur la MAC address WiFi de la machine volée/perdue. Si d'aventure la machine est détectée et/ou localisée par ce biais, elle pourra en informer la justice et les services compétents ;

- sur la base de la modification d'état de la machine dans l'inventaire, la DSI sort la machine du réseau câblé de MT.

Ce n'est qu'une fois toutes ces tâches réalisées que la DSI peut livrer la machine de remplacement à l'utilisateur, puis fermer le cas.

La procédure reste valable dans le cas d'un salarié en télétravail.

3.1.4 Traitement d'un vol/perte de matériel privé (contenant des données de l'entreprise)

L'utilisateur ne doit pas oublier d'annoncer le vol à sa compagnie d'assurance privée. Ensuite, la DSI démarre la procédure de traitement du vol :

- la DSI commence par établir l'inventaire des licences logicielles de MT qui étaient activées sur la machine volée/perdue.

- sur la base des informations reçues, la DSI bloque temporairement le compte non seulement de l'utilisateur principal de la machine, mais aussi de chaque utilisateur s'étant servi de cette machine, afin que ces comptes ne puissent pas être utilisés à mauvais escient par la personne ayant volé/récupéré la machine. Le-s compte-s sont réactivés-s dès que le-s utilisateur-s ont changé leur mot de passe. Le Support DSI se tiennent à disposition des employés, pour les aider dans cette procédure.

- si l'utilisateur est en mesure de communiquer la Mac address WiFi de la machine volée/perdue, la DSI active une alarme sur cette MAC address. Si d'aventure la machine est détectée et/ou localisée par ce biais, elle pourra en informé la justice et les services compétents.

Ce n'est qu'une fois ces tâches réalisées que la DSI ferme le cas.

3.1.5 Données

Chaque utilisateur est responsable pour ce qui le concerne du respect du secret professionnel et de la confidentialité des informations qu'il est amené à détenir, consulter ou utiliser. Les règles de confidentialité ou d'autorisation préalable avant diffusion externe ou publication sont définies par la direction et applicables quel que soit le support de communication utilisé. L'utilisateur doit être particulièrement vigilant sur le risque de divulgation de ces informations dans le cadre d'utilisation d'outils informatiques, personnels ou appartenant à l'entreprise, dans des lieux autres que ceux de l'entreprise (hôtels, lieux publics…)

3.2 Droits et devoirs de MARTINIQUE TRANSPORT

3.2.1 Protection des données personnelles

La protection des données personnelles est encadrée par la loi du 6 janvier 1978 dite « Informatique et libertés ».
La loi du 20 juin 2018 relative à la protection des données personnelles a modifié la loi « Informatique et Libertés » pour l'adapter aux dispositions du Règlement Général sur la Protection des Données (RGPD), applicable partout en Europe depuis le 25 mai 2018.
Ce nouveau cadre juridique renforce les droits de chaque citoyen européen sur la protection de leurs données personnelles et responsabilise les acteurs traitant ces données.

En plus du RGPD, l'Union européenne a adopté la directive (UE) du 27 avril 2016 dite "Directive Police Justice" relative aux traitements de données personnelles en matière pénale. Ces deux textes constituent "le paquet européen" sur la protection des données.

Le RGPD s'applique à tout traitement de données personnes, c'est-à-dire :

- Toute opération ou ensemble d'opération appliquées à des données (collecte, conservation...) quel que soit le procédé utilisé (collecte, enregistrement organisation, conservation, adaptation, modification, extraction consultation, utilisation, communication par transmission ou diffusion ou toute autre forme de mise à disposition, rapprochement).
-
- Qui se rapportent à une personne physique, directement ou indirectement identifiable (nom, prénom, numéro d'identifiant, numéro de téléphone, email, adresse postale....).

Certaines données sont considérées comme sensibles, à savoir celles qui révèlent :

- Les données de santé ou liées au handicap
- Les croyances religieuses ; les convictions politiques ou l'appartenance syndical
- L'origine ethnique
- Les infractions pénales

- Les données sur la vie privée issues d'un profilage

L'utilisation de ces données impliquent des mesures de sécurité adaptées.

Les principes concernant le traitement des données sont les suivants :

- Les finalités doivent être déterminées au préalable (nécessaire à l'exécution d'une mission d'intérêt public)
- La collecte des données doit être proportionnée aux finalités
- L'information des personnes est indispensable
- La durée de conservation est encadrée
- Le niveau de sécurité doit être approprié
- L'exercice des droits des personnes doit être garantie

Les personnes publiques doivent :

- Garantir la sécurité maximale des données personnelles
- Être transparente dans le traitement des données – c.à.d. une obligation d'information et de conseil des personnes concernées
- Respecter les droits de la personne concernée lors du traitement des données
- Tenir un registre des traitements de données
- Nommer un délégué à la protection des données (DPO)
- Effectuer des Analyses d'impact préalable aux traitements des données personnelles permettant de gérer au préalable les risques éventuels lors du traitement (une fuite des données par exemple)

La personne publique doit avoir une relation continue et intense avec la CNIL pour une information fluide et rapide de l'autorité de contrôle en cas de violation des données personnelles.

L'agent doit s'assurer de respecter les conditions d'utilisation des données personnelles qu'il est amené à utiliser dans le cadre de ses missions. En cas de doute, il doit impérativement et avant toute action, se tourner vers le DPO ou la Direction des Systèmes d'Information.

En effet, chacun des utilisateurs du SI doit s'astreindre à les respecter et à se conformer aux préconisations du DPO. Ainsi, en cas de création ou de constitution de fichiers contenant des données personnelles, l'utilisateur et/ou son responsable hiérarchique devront se rapprocher du DPO afin de s'assurer de la conformité du RGPD.

Les sollicitations du DPO sont à faire à l'adresse : dpo@martiniquetransport.mq

3.2.2 Disponibilité et intégrité du SI

L'établissement s'engage à :

- Mettre à disposition les ressources informatiques matérielles et logicielles nécessaires au bon déroulement de la mission des utilisateurs du SI et ce dans le respect du code de la commande publique

- Informer les agents des diverses contraintes d'exploitation (interruption de service, maintenance…) susceptibles d'occasionner une perturbation
- Respecter la confidentialité des données et assurer leur protection

4. Accès aux ressources informatiques

L'accès sécurisé aux ressources informatiques de l'établissement est possible quel que soit le lieu sous-réserve d'une configuration particulière des postes, dès lors qu'ils sont connectés à internet.

Il en est ainsi de la messagerie électronique, accessible via n'importe quel navigateur et poste disposant d'une connexion à internet.

En fonction des droits d'accès aux applications (financière, rh, courriers…) et aux partages réseaux paramétrés sur le réseau interne de l'établissement, il est également possible de se connecter à l'extérieur des locaux de l'établissement (accès distant).

Pour activer l'accès à distance, l'agent doit en faire la demande au support informatique qui lui configurera son accès et lui communiquera la procédure à suivre pour se connecter.

Lors de cet accès à distance, les bonnes pratiques de sécurité d'utilisation du SI sont applicables.

5. Télétravail

Le télétravail est une forme d'organisation du travail qui permet à l'agent de travailler ailleurs que dans son service ou ses locaux habituels en utilisant les technologies de l'information et de la communication (TIC).

Le télétravail est mis en place à la demande de l'agent conformément aux termes du protocole d'accord relatif à la mise en œuvre du télétravail à MARTINIQUE TRANSPORT en vigueur

En position de télétravail, toutes les bonnes pratiques de sécurité et d'utilisation du SI restent applicables.

Depuis son domicile, il est plus que nécessaire de ne pas laisser son poste de travail connecté au réseau de la collectivité sans supervision directe. Il est recommandé de le verrouiller si l'on est amené à se déplacer loin de son poste de travail.

6. Assistance, support aux agents

Pour toute demande ou incident d'utilisation de moyens informatique l'agent doit effectuer une déclaration par mail à : support.informatique@martiniquetransport.mq

Cette déclaration permet à la DSI de centraliser dans un outil unifié l'ensemble des demandes de service et des déclarations d'incidents.

Cet outil permet à la DSI de planifier et d'apporter un meilleur suivi aux actions qui seront à réaliser et de nous assurer que l'ensemble des sollicitations qui nous parviennent soient effectivement bien traitées.

En résumé, transmettre vos demandes via cette adresse :

- Garantie que votre demande sera traitée par la DSI.

- Permet d'être automatiquement informé par mail de l'agent qui sera en charge de vous répondre.
- Permet d'automatiquement informé par mail des différentes étapes du traitement de votre demande.

7. Sécurité informatique

Nous sommes tous concernés par la sécurité. Chacun est responsable à son niveau de la sécurité de l'information dans l'établissement. Nous nous devons d'avertir la Direction des Systèmes d'Information lors de la détection d'un problème de sécurité.

Les principaux objectifs de la sécurité :

- L'intégrité, garantie l'exactitude et l'entièreté des données relatives à l'information. Elle fait en sorte que les données ne puissent être corrompues, volées ou perdues ;

- La confidentialité : seules les personnes autorisées peuvent avoir accès aux informations qui leur sont destinées (notions de droits ou permissions). Tout accès indésirable doit être empêché.

- La disponibilité, permet de maintenir le bon fonctionnement du système d'information et de protéger les données à tout instant en veillant à ce que les dispositifs de sécurité ne perturbent pas les conditions de travail ;

- L'authentification : les utilisateurs doivent prouver leur identité par l'usage de droit d'accès. Il ne faut pas mélanger identification at authentification : dans le 1er cas, l'utilisateur n'est reconnu que par son identifiant, tandis que dans le 2ème cas, il doit fournir un mot de passe

7.1 Les commandements de la sécurité

1. Suivez les règles et procédures de la sécurité de l'information
Consultez régulièrement les règles et procédures disponibles sur l'intranet ou transmises par mail.

2. Protégez vos mots de passe
Ne relevez jamais vos mots de passe. Si quelqu'un vous les demande, refusez. Notre sécurité implique de ne jamais donner vos mots de passe, ni de les noter sur un support en évidence.

3. Bloquez l'accès à votre ordinateur
Si vous quittez votre bureau, bloquez l'accès à votre ordinateur en verrouillant votre session (CTRL+ALT+SUPP puis sélectionner l'option « Verrouiller » ou appuyer simultanément sur Windows + L).

4. Sauvegardez correctement vos données
Stocker vos données sur les partages réseaux qui sont sauvegardés régulièrement sur les serveurs de Martinique Transport. Appliquer ces consignes vous permettra de récupérer vos données si elles ont été perdues et d'y avoir accès à tout moment.

5. Assurez-vous de l'identité de vos interlocuteurs
Lors d'une conversation par e-mail ou par téléphone, assurez-vous de l'identité de votre interlocuteur. Soyez prudents à chaque fois que l'on vous demande des informations personnelles, confidentielles, ou importantes au niveau de l'établissement.

6. Soyez attentifs à vos mails
Les e-mails peuvent représenter une menace pour votre ordinateur et pour l'ensemble du réseau informatique. Ne répondez jamais aux e-mails vous demandant des informations personnelles et/ou confidentielles. Vérifiez la provenance, l'innocuité et l'intégrité de chaque pièce jointe.

7. Utilisez intelligemment Internet
L'utilisation d'internet est limitée pour des raisons de sécurité. L'accès est restreint mais suffisant pour votre usage professionnel. Téléchargez uniquement des fichiers nécessaires à votre travail et soyez attentifs aux fichiers reçus.

8. Utilisez votre antivirus
L'établissement met à disposition un antivirus qu'il convient d'utiliser pour analyser toutes sources de données qui peuvent représenter un risque.

9. Utilisez les logiciels déployés par la DSI
N'installez jamais de logiciels non autorisés. Utilisez uniquement ceux mis à votre disposition par votre organisation. Si vous avez besoin d'un logiciel, formulez une demande d'installation à la Direction des Système d'Information.

10. Prenez soin du matériel
Chaque utilisateur du SI est responsable du matériel mis à sa disposition.

11. Eteignez votre poste de travail
Eteignez votre ordinateur à la fin de votre journée de travail, sauf contre-indication de la DSI.

12. Signalez les incidents
Tout incident doit être signalé au plus vite à la DSI. Cela peut prévenir d'autres incidents similaires.

7.2 Mesures de sécurité

Les risques liés à une infection sont la perte pure et simple de vos données et celles de vos collègues.

La seule solution à ce jour est une restauration de vos fichiers à une date antérieure. De ce fait, cela entrainera incontestablement une perte d'information (perte des mises à jour effectuées entre la date de l'infection et la date de la restauration).

En cas d'infection, suivre les recommandations suivantes :
- Débranchez immédiatement le câble réseau derrière votre poste ou éteignez-le,
- Contactez la DSI : support.informatique@martiniquetransport.mq.

8. Revue des fichiers d'activités

8.1. Revues des fichiers automatisées

Pour des nécessités de maintenance et de gestion technique, de traçabilité, de sécurité ou de détection des abus, l'utilisation des ressources informatiques et des services internet, ainsi que les échanges via le réseau peuvent être analysés et contrôles dans le respect de la législation (loi n°2018-133 du 26 février 2018 portant diverses dispositions d'adaptation au droit de l'Union Européenne dans le domaine de la sécurité).

Le système d'information s'appuie sur des fichiers d'enregistrement d'activités dits « logs », créés automatiquement.

Ils permettent d'assurer le bon fonctionnement du système, en protégeant la sécurité des informations, en détectant des erreurs matérielles ou logicielles et en examinant les accès et l'activité des utilisateurs du SI (données de connexion, espace de stockage, volume de données échangées, sites visités...).

Les agents sont informés que de multiples traitements sont réalisés afin de sécuriser l'activité du SI.

Sont notamment enregistrées les données relatives :

- A l'utilisation des logiciels applicatifs, pour contrôler l'accès, les modifications et suppression de fichiers
- Aux connexions entrantes et sortantes au réseau interne, à la messagerie et à Internet, pour détecter les anomalies liées à l'utilisation de la messagerie et surveiller les tentatives d'intrusion et les activités, telles que la consultation de sites web ou le téléchargement de fichiers.

8.2. Procédure de revues de fichiers

En cas de dysfonctionnement constaté par la Direction des Systèmes d'Information, il peut être procédé à un examen manuel et à une vérification de toute opération effectuée par un ou plusieurs agents. Lorsque cette vérification porte sur les fichiers d'un utilisateur du SI, la Direction des Systèmes d'Information ne peut ouvrir les fichiers, identifiés comme privés, qu'en présence de ce dernier. Tous les autres fichiers peuvent être ouverts par la DSI pour vérification.

9. Information des agents

La présente charte est disponible sur l'intranet de l'établissement.

Une communication interne (par mail et via les afficheurs numériques) sera réalisée à chaque mise à jour ultérieure du document.

10. Bases légales

Sur le plan juridique, il importe que chaque agent respecte les règles d'utilisation de la Charte afin de se prémunir d'actions susceptibles d'engager outre sa responsabilité disciplinaire, sa responsabilité civile et/ou pénale.

En effet, la quantité et la facilité de circulation des informations et des contenus sur les réseaux informatiques, notamment l'internet, ne doivent pas faire oublier la nécessité de strictement respecter la législation en vigueur d'une part, et l'ensemble des obligations déontologiques qui s'applique à tout fonctionnaire d'autre part, au premier rang desquelles, l'obligation de réserve.

10.1 Déontologie – Ethique – Droit disciplinaire

Chaque utilisateur s'engage à respecter les règles de déontologie informatique dans l'esprit des principes généraux fixés par le statut des fonctionnaires.

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 n°84-53 du 26 janvier 1984 relative à la fonction publique territoriale, l'agent doit respecter les obligations de réserve, de discrétion et de secret professionnel.

10.2 Sanctions applicables

Il est rappelé qu'en cas d'atteinte à l'un des principes protégés par la loi, la responsabilité administrative, pénale et/ou civile de l'agent ainsi que celle de l'établissement est susceptible d'être recherchée.

Tout manquement aux règles définies dans cette charte est susceptible d'entraîner, en cas d'abus, des sanctions de type :

- Modification/suppression d'habilitation aux logiciels
- Limitation/suppression d'accès à certains sites/à internet, à certaines applications
- Non remplacement d'un matériel en mauvais état
- Mesures disciplinaires…

La DSI est chargée de vérifier l'utilisation du SI dans le respect des règles et de saisir l'administration en cas de dysfonctionnements ou d'utilisation contraire aux termes de la charte.

Dès lors qu'une sanction disciplinaire est susceptible d'être prononcée à l'encontre d'un agent, celui-ci est informé conformément aux dispositions règlementaires.

Par ailleurs, les articles 226-16 à 226-24 du code pénal précisent les atteintes aux droits de la personne résultant des fichiers ou des traitements informatiques. Tandis que les articles 323-1 à 323-7 du même code portent sur les atteintes aux systèmes de traitement automatisé de données.

11. Opposabilité de la charte

La présente charte a été présentée en Comité Technique, le 17 mai 2021.
Elle a été adoptée par le Conseil d'Administration le 31 mai 2021.
La charte sera affichée et disponible sur l'intranet.
Elle est rendue opposable dès sa notification à chaque utilisateur valant acceptation entière de ses termes.

Le Président du Conseil d'Administration
de Martinique Aéroport

10 JUIN 2021

Alfred MARIE-JEANNE