Envoyé en préfecture le 14/08/2024
Reçu en préfecture le 14/08/2024
Publié le 14/08/2024
ID : 030-200066918-20240814-2024_0373D-AR

Alès Agglomération

RÉPUBLIQUE FRANÇAISE

2024 /0373

EXTRAIT DU REGISTRE DES DÉCISIONS D'ALÈS AGGLOMÉRATION

Service : Département TIC
Tél : 04 66 56 11 58
Réf : JN/2024_0605

Objet : Adoption de la charte pour le bon usage de l'outil informatique, des réseaux et de la téléphonie

Le président d'Alès Agglomération,

Vu le règlement européen (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 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, et abrogeant la directive 95/46/CE (règlement général sur la protection des données),

Vu le Code général des collectivités territoriales,

Vu le Code général de la fonction publique,

Vu le Code pénal,

Vu la loi n°78-17 en date du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés,

Vu la délibération C2024_03_17du conseil de communauté en date du 27 juin 2024 portant délégation du conseil de communauté au président en application des dispositions de l'article L5211-10 du Code général des collectivités territoriales,

Vu l'avis du comité social territorial en date du 11 juin 2024,

Considérant que le développement des technologies de l'information et de la communication se traduit par un recours généralisé à des moyens informatiques, téléphoniques et logiciels, tant entre le public et l'administration qu'au sein de l'administration ou entre cette dernière et ses prestataires,

Considérant que le règlement général de protection des données susvisé a, dans un objectif de protection des données personnelles des personnes physiques, créé de nouvelles obligations au regard des traitements de ces données pour les responsables de traitement, notamment pour la Communauté Alès Agglomération,

Considérant que les personnes publiques sont régulièrement la cible de cyberattaques susceptibles de perturber le fonctionnement des services publics ou d'induire des fuites de données préjudiciables aux usagers,

Envoyé en préfecture le 14/08/2024
Reçu en préfecture le 14/08/2024
Publié le 14/08/2024
ID : 030-200066918-20240814-2024_0373D-AR

Considérant la nécessité pour la communauté Alès Agglomération d'être en mesure de garantir un niveau de performance satisfaisant à tous les utilisateurs des ressources informatiques,

Considérant qu'il est nécessaire de faire adopter, par tous les utilisateurs d'outils composant le système d'information ou ayant accès à ce dernier, des bons comportements et d'interdire certains usages risqués pour réduire les vulnérabilités,

Considérant qu'il convient d'adopter une charte informatique afin d'atteindre ces objectifs,

DÉCIDE

ARTICLE 1 :

D'adopter la charte informatique, à compter du 1er juillet 2024 dont le texte intégral est joint à la présente décision.

ARTICLE 2 :

Monsieur le directeur général de la communauté Alès Agglomération et Monsieur le receveur communautaire sont chargés, chacun en ce qui le concerne, de l'exécution de la présente décision.

Alès, le 14 AOUT 2024

Le président

Christophe RIVENQ

921

ALES AGGLOMERATION

La présente décision, à supposer que celle-ci fasse grief, peut faire l'objet, dans un délai de deux mois à compter de sa notification ou de sa publication, d'un recours contentieux auprès du Tribunal Administratif de Nîmes ou d'un recours gracieux auprès du Président de la Communauté Alès Agglomération, étant précisé que celui-ci dispose alors d'un délai de deux mois pour répondre. Un silence de deux mois vaut alors décision implicite de rejet. La décision ainsi prise, qu'elle soit expresse ou implicite, pourra elle-même être déférée au Tribunal Administratif dans un délai de deux mois. Conformément aux termes de l'article R.421-7 du Code de Justice Administrative, les personnes résidant outre-mer et à l'étranger disposent d'un délai supplémentaire de distance de respectivement un et deux mois pour saisir le Tribunal. Le Tribunal Administratif peut aussi être saisi par l'application informatique "Télérecours citoyens" accessible par le site internet www.telerecours.fr.

Envoyé en préfecture le 14/08/2024
Reçu en préfecture le 14/08/2024
Publié le 14/08/2024
ID : 030-200066918-20240814-2024_0373D-AR

CHARTE
POUR LE BON USAGE DE L'OUTIL INFORMATIQUE, DES RÉSEAUX ET DE LA TÉLÉPHONIE de la Ville d'Alès, d'Alès Agglomération et du CCAS

Envoyé en préfecture le 14/08/2024
Reçu en préfecture le 14/08/2024
Publié le 14/08/2024
ID : 030-200066918-20240814-2024_0373D-AR

PRÉAMBULE

La présente charte s'applique aux Collectivités suivantes : la Ville d'Alès, la Communauté Alès Agglomération et le Centre Communal d'Action Sociale de la Ville d'Alès ont mutualisé leur système d'information auprès d'Alès Agglomération par le biais d'un service commun. Le système d'information est administré par le département Système d'Information ci-après nommé département T.I.C.
Cette mutualisation induit que les Collectivités utilisant ce système d'information adhèrent aux mêmes règles d'organisation telles que PSSI, charte...

Les technologies de l'information et de communication (TIC) constituent pour la Ville d'Alès (ci-après dénommée « la Collectivité ») une ressource stratégique indispensable à la conduite des activités et de la satisfaction des services rendus aux citoyens et utilisateurs. Le personnel de la Collectivité est amené à utiliser dans l'exercice de ses fonctions l'outil informatique, les réseaux et les services de communication pour satisfaire ses missions. Or, cette utilisation comporte de nombreux risques en termes de sécurité (virus, vers, messages indésirables, piratages et fraudes informatiques, hameçonnage, etc.) et est encadrée par des exigences légales, réglementaires et contractuelles de plus en plus strictes.

Face à cela, une Politique de Sécurité des Systèmes d'Information (PSSI) d'Alès Agglomération, dont la présente charte est un des principaux éléments, a été définie. Cette dernière précise les rôles et responsabilités de chacun et institue des principes et des règles de sécurisation des Systèmes d'Information. Il est primordial que chaque utilisateur s'astreigne à respecter les règles d'utilisation de ces outils dont l'irrespect pourrait engager la responsabilité civile et/ou pénale de l'utilisateur et/ou celle de la Collectivité.

La Collectivité souhaite, grâce à l'exposé des différentes mesures de protection à mettre en œuvre, sensibiliser chacun à l'importance de respecter les règles de sécurité et de contribuer ainsi à la sauvegarde des Systèmes d'Information.

Chaque utilisateur est en effet responsable de l'usage des équipements qui lui sont mis à disposition et doit en assurer, à son niveau, la protection afin qu'ils demeurent disponibles, fiables et performants.

Pour la sécurité de tous, chacun doit respecter les règles et principes détaillés dans la présente charte et adopter un comportement professionnel et soucieux de la sécurité des Systèmes d'Information.

Il convient de préciser que les termes techniques utilisés sont définis dans un glossaire à la fin de ce document, qui aborde tant les termes techniques que certains termes dont l'usage est plus compréhensible pour les destinataires de la charte.

ARTICLE 1 – OBJET

La présente charte a pour objet de :

- sécuriser le système d'information
- assurer une parfaite information des utilisateurs vis-à-vis de leurs droits et devoirs en matière d'utilisation et d'accès aux ressources des systèmes d'information
- les sensibiliser aux exigences de sécurité
- appeler l'attention des utilisateurs sur les comportements de nature à porter atteinte à l'intérêt collectif
- protéger les personnes contre des utilisations déviantes des outils mis à leur disposition et rappeler les règles d'utilisation de ces outils,

- encadrer l'usage des outils dans des limites qui concilient usage professionnel et garantie des libertés individuelles.
- porter à la connaissance de chaque utilisateur les moyens utilisés pour assurer le contrôle de l'accès et de l'utilisation des ressources des Systèmes.

Ces recommandations sont en partie issues des référentiels de bonnes pratiques de sécurité publiés par l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI).

Les mesures énoncées dans la présente charte découlent de la PSSI (Politique de sécurité des Systèmes d'Information) en vigueur librement consultable sur l'intranet et décrivant les éléments stratégiques (enjeux, référentiels, principaux besoins de sécurité et menaces) et les règles de sécurité applicables à la protection du Système d'Information.

ARTICLE 2 - CHAMPS D'APPLICATION DE LA CHARTE

2.1 Utilisateurs concernés

Tout utilisateur du système d'information et de communication, permanent ou temporaire, quel que soit son statut, fonction et mission, et ayant accès aux ressources informatiques et/ou aux données personnelles utilisées par la Collectivité, est tenu de respecter la présente charte, ainsi que la législation en vigueur, notamment en matière de protection des droits de propriété intellectuelle et de protection des données à caractère personnel. Cela vise notamment, les agents des Collectivités, les agents des organismes ayant recours au système d'information (logiciel gestion des cantines, logiciel de système d'information géographique, etc) , les employés de sociétés prestataires, les intérimaires, les stagiaires, les apprentis, les visiteurs / occasionnels (utilisateurs Wifi, Wifi public...), etc.

Tout tiers ayant, par contrat ou convention de prestation, accès aux réseaux, aux données, aux programmes informatiques ou autres moyens de la Collectivité, reçoit communication et s'engage à respecter pour lui-même, ses préposés et éventuels prestataires propres, la présente charte ainsi que les contraintes techniques et déontologiques liées à la politique de sécurité.

En cas de besoin pour des dispositions particulières de la charte, des sous-catégories spécifiques d'utilisateurs peuvent être considérées et notamment les utilisateurs agents publics, catégorie visant le personnel employé par les Collectivités en application de règles de droit public et ainsi concerné par des droits et obligations spécifiques.

2.2 Règles particulières

Les présentes règles sont applicables sans préjudice des règles particulières pouvant porter sur l'utilisation du système d'information et de communication par les institutions représentatives du personnel, sur l'organisation d'élections par voie électronique, sur un niveau de sécurité et de confidentialité particulièrement renforcé ou encore sur l'organisation du télétravail pour certaines catégories de personnel.

ARTICLE 3 – CONDITIONS GÉNÉRALES D'UTILISATION

Tout utilisateur est responsable du bon usage des équipements mis à sa disposition, de ses moyens d'accès / d'authentification au SI (mots de passe, badge, carte d'authentification, etc.), des certificats électroniques de transmissions ou de signature et autres habilitations.

Il a aussi la charge, à son niveau, de contribuer à la sécurité générale.

Envoyé en préfecture le 14/08/2024
Reçu en préfecture le 14/08/2024
Publié le 14/08/2024
ID : 030-200066918-20240814-2024_0373D-AR

A cet effet, il s'engage à ne pas effectuer d'opérations pouvant nuire au fonctionnement du réseau, à l'intégrité de l'outil informatique.

L'usage des ressources informatiques doit se faire dans le respect des dispositions législatives et réglementaires en vigueur.
Le déplacement de tout matériel hors UE peut être soumis à des conditions particulières et devra, dans tous les cas, être envisagé avec le Département TIC *a minima* 15 jours avant la date prévue pour le départ.

3.1 Utilisation du matériel et responsabilité d'utilisation

En protégeant les équipements qui lui sont confiés et en adoptant une attitude responsable, l'utilisateur favorise la sécurité des informations placées sous sa responsabilité.

Les équipements mis à disposition des utilisateurs sont configurés sous le contrôle exclusif du département TIC. Ces configurations ne doivent ni être modifiées ni altérées par l'utilisateur (sauf demande explicite du département TIC)
A titre d'exemple :

- L'utilisateur ne doit jamais ajouter ou retirer de composant matériel (disque dur, carte réseau, etc.) sans l'accord du département TIC.

Pour tout équipement non préconfiguré par le département TIC, sa connexion au système d'information requiert une autorisation de ce département.

3.2 Diffusion des documents liés à la sécurité de l'information

Les documents liés à la sécurité de l'information sont hébergés sur la GED. Les directives de sécurité de l'information sont décrites dans la « Politique de Sécurité du Système d'Information » et couvrent les aspects organisationnels, humains, de sécurité logique (immatérielle) et physique.

3.3 Signaler un incident ou formuler une demande

Le département TIC met à disposition des utilisateurs un service d'assistance et de support : les utilisateurs doivent signaler tout dysfonctionnement du système d'information dans les plus brefs délais, notamment pour minimiser les dommages subis par la Collectivité.

Les utilisateurs peuvent exprimer un besoin ou proposer une évolution du système d'information par ce même moyen.

La disparition, la perte ou le vol présumé d'une ressource et en particulier d'un ordinateur, d'un téléphone, d'un badge d'accès ou encore d'un périphérique de stockage est considéré comme un incident de sécurité et doit immédiatement être porté à la connaissance du :

- son supérieur hiérarchique,
- le département TIC (ticket GLPI, appel hotline)
- Le délégué à la protection des données

Les utilisateurs doivent alerter immédiatement le département TIC en cas d'activité suspecte, de tentative de violation du système d'information, et le DPO en cas de violation de données personnelles (fuites, pertes de confidentialité, d'intégrité ou de disponibilité) même si celle-ci a été avortée, et a fortiori en cas de violation avérée : cela peut concerner la détection d'un code malveillant, la suspicion d'usurpation d'identité, la disparition suspecte de documents, etc. ou tout évènement anormal ou inhabituel. Il est demandé aux utilisateurs d'être particulièrement attentifs à ce sujet.

Envoyé en préfecture le 14/08/2024
Reçu en préfecture le 14/08/2024
Publié le 14/08/2024
ID : 030-200066918-20240814-2024_0373D-AR

ARTICLE 4 - ACCÈS AUX RESSOURCES

4.1 Attribution et retrait des accès aux ressources

Les ressources informatiques, l'usage des services Internet/Intranet et du réseau pour y accéder, ainsi que les moyens téléphoniques et matériels, sont mis à disposition des utilisateurs, tels que définis dans la présente charte, pour l'exercice des activités de la Collectivité ou des services offerts à la population, voire des prestations demandées par la Collectivité à ses prestataires, même occasionnels (ex : stagiaires).

L'accès aux ressources est justifié par, et uniquement par, les besoins de chaque utilisateur, par exemple l'exercice d'une fonction, l'accomplissement des missions en tant qu'employé, la réalisation d'un service en tant que prestataire, etc.
Il en résulte que tous les différents accès aux ressources, que ce soit la mise à disposition de moyens informatiques ou téléphoniques, l'attribution de compte, d'identifiant, etc, sont temporaires et en lien avec la qualité de chaque utilisateur.
Ainsi, aucun accès ne peut être conservé dès que le besoin n'est plus présent, ce qui a notamment pour conséquence :
- la restitution, par l'utilisateur, de tout équipement individuel lui ayant été attribué de quelque manière que ce soit,
- l'arrêt de l'utilisation de tous les identifiants et comptes permettant l'accès aux ressources jusqu'à leur suppression par le Département TIC.

Les accès aux ressources sont définis dans le cadre de la mission de l'utilisateur et sont personnels, confidentiels et non transmissibles.

Toute demande d'accès au système d'information doit être soumise à l'autorisation écrite préalable des supérieurs hiérarchiques, notamment pour l'accès :

- aux moyens informatiques (hors vidéoprojecteurs)
- aux moyens téléphoniques
- au / aux réseaux
- aux sites internet
- aux logiciels métiers tels que la Gestion Financière, Gestion des Ressources Humaines...,
- aux données partagées.

La création ou la fermeture des accès lors du gain ou de la perte de la qualité d'utilisateur, notamment cas d'arrivée ou de départ d'un agent ou de modification des missions, est à l'initiative de la personne chargée du contrôle ou responsable de l'activité de l'utilisateur, par exemple le supérieur hiérarchique pour l'arrivée, le départ ou la modification des missions d'un agent, le référent du marché pour un prestataire, etc.

4.2 Attribution de compte nominatif pour tout accès aux ressources

Chaque personne ayant accès aux ressources doit utiliser un compte ou une session de travail nominative et personnelle, protégée par un identifiant (nominatif) et un mot de passe. Les sessions partagées ou communes sont donc proscrites.

Les comptes et postes de travail doivent être protégés par un mot de passe robuste composé, au minimum, de 10 caractères, mélangeant des lettres majuscules et minuscules, des chiffres et des caractères spéciaux.

Pour une confidentialité et une sécurité optimale, les mots de passe doivent être modifiés régulièrement, **a minima deux fois par an.**
Pour des raisons de sécurité, le département TIC se réserve le droit d'imposer tout changement de mots de passe.

Envoyé en préfecture le 14/08/2024
Reçu en préfecture le 14/08/2024
Publié le 14/08/2024
ID : 030-200066918-20240814-2024_0373D-AR

Tous les mots de passe sont personnels, confidentiels et incessibles. L'emploi de mots de passe communs à plusieurs personnes est donc interdit.
Ils ne doivent, à titre non-exhaustif :
- ni être notés sur des supports potentiellement accessibles à autrui (par exemple sur un cahier, un post-it ou un fichier non chiffré),
- ni être enregistrés dans le navigateur (hors coffre-fort de mots de passes validé par l'autorité) mais ressaisis à chaque connexion,
- ni être communiqués, y compris au département TIC, à ses collaborateurs ou à sa hiérarchie,
- ni être faciles à deviner par une personne mal intentionnée (pas de prénoms ou dates de naissance de proches, de nom usuel, par exemple).

Ainsi, à titre d'exemple :

- tout stockage de mot de passe sur un support physique externe ou en mémoire dans le système d'information et/ou le terminal de connexion est interdit, à l'exception des coffre-forts de mots de passe sécurisés validés par le département TIC (exemple : KeePass).
- l'utilisateur ne communiquera aucun mot de passe au téléphone s'il n'est pas absolument sûr de l'identité et de l'habilitation de son interlocuteur. En cas de doute, il devra rappeler la personne au département TIC (numéro interne), pour poursuivre l'opération.

4.3 Centralisation des données sur les partages réseaux

Sauf cas particuliers, aucune donnée de travail courant ne doit être stockée localement sur le disque dur des postes de travail.

Le département TIC s'engage sur la pérennité des données à condition que ces données aient été sauvegardées sur les serveurs identifiés et validés et non sur les postes.

Les données présentes sur le disque local de la machine ne sont pas intégrées dans le plan de reprise d'activité et ne bénéficient donc pas de la sauvegarde centralisée.

Les utilisateurs peuvent toutefois effectuer une demande de sauvegarde sur serveur de leurs données (ou d'une partie de celles-ci) stockées sur leur poste, qui leur paraissent stratégiques.
A noter que, pour la sécurité du SI, les techniciens du département TIC analysent le contenu des données (type, taille des fichiers) ainsi sauvegardées.

Il convient d'effectuer régulièrement la sauvegarde serveur ou sur un système d'archivage électronique de ses données dans un but d'archivage légal, au même titre que les documents papier.

La sauvegarde de fichiers professionnels, sur des sites extérieurs comme GoogeDrive, We-Transfert, divers clouds, ainsi que sur une solution de messagerie autre que Zimbra, est interdite.
Les dérives dues à l'utilisation de ces solutions ne sauraient donc engager la responsabilité de la Collectivité et du département TIC.

4.4 Gestion des supports amovibles

Tout support amovible (clés USB, disques durs externes, téléphones portables, outils de connexion réseau, etc ...) est un moyen privilégié de propagation des codes malveillants et de fuite de données.

Envoyé en préfecture le 14/08/2024
Reçu en préfecture le 14/08/2024
Publié le 14/08/2024
ID : 030-200066918-20240814-2024_0373D-AR

À ce titre, la connexion sur un équipement de travail ou sur le réseau d'un support amovible ayant été connecté sur un équipement externe est strictement interdite. Cette mesure inclut le chargement de téléphone portable, de cigarette électronique, lecteur MP3, montre connectée, etc...
Des supports amovibles contrôlés sont fournis par les techniciens du département TIC en cas de besoin particulier d'utilisation.

4.5 Badges d'accès

L'accès aux locaux non-ouverts au public est limité uniquement aux personnes autorisées (agents, prestataires, élus) à condition qu'il soit porteur d'un badge d'identification personnel, fourni par la Collectivité, et précisant le nom, le prénom, la photo de l'agent ainsi que le numéro d'identification., Un badge « prestataire » est fourni aux intervenants externes réalisant des prestations sans être accompagnés par un agent.

Le badge est personnel et incessible.

Tout badge perdu ou égaré doit être signalé immédiatement au département TIC.

Les visiteurs ne sont pas autorisés à circuler seuls dans les locaux non-ouverts au public et doivent être accompagnés.

ARTICLE 5 - SÉCURITÉ DU POSTE DE TRAVAIL

5.1 Droits administrateur sur le poste

L'accès aux fonctions d'administration du poste de travail, permettant les modifications et installations potentiellement risquées, est strictement limité aux techniciens du département TIC. Des droits étendus peuvent être accordés à certains profils utilisateurs ayant des besoins particuliers.

5.2 Verrouillage et extinction du poste de travail

Les ressources ou services ne doivent pas être accessibles à des tiers y compris en cas d'absence du poste de travail : il convient alors de verrouiller son poste avant de s'absenter, même momentanément.

Pour rappel, le titulaire du compte utilisateur est responsable de tout acte de malveillance opéré depuis son poste en cas de négligence.

Pour les ordinateurs, la mise en fonction automatique de l'économiseur d'écran, au bout de quelques minutes d'inactivité, est obligatoire, avec saisie obligatoire d'un mot de passe pour quitter la veille.

A la fin de la journée, sauf besoin exceptionnel, le poste de travail doit être éteint et connecté au réseau local afin de procéder aux différentes mises à jour de sécurité.

5.3 Exploitation de logiciels « à jour » sur le poste de travail

Les mises à jour du système d'exploitation sont nécessaires et obligatoires. Une stratégie de déploiement via l'Active Directory a été mise en place. Après validation par le département TIC, elles sont installées automatiquement au redémarrage du poste. D'autre part, un agent logiciel est déployé sur chacun des postes afin de faciliter la gestion centralisée.

Les utilisateurs ayant des droits étendus, au sens de l'article 5.1, sont responsables de la mise à jour des logiciels installés sur le poste de travail (notamment du navigateur web) et doivent obligatoirement effectuer les mises à jour demandées par les techniciens du département TIC.

5.4 Protection contre les virus

L'utilisateur s'engage à ne pas apporter volontairement des perturbations au bon fonctionnement des systèmes informatiques et des réseaux, que ce soit par des manipulations anormales du matériel ou par l'introduction de logiciels parasites connus sous le nom générique de virus, chevaux de Troie, bombes logiques, etc...

Le département TIC installe sur les machines des outils destinés à protéger des programmes malveillants.
Ces outils ne doivent en aucun cas être désinstallés, et ils sont paramétrés pour se mettre à jour régulièrement (reconnaissance de nouveaux virus).
Le paramétrage ne doit donc pas être modifié.
Il est recommandé aux utilisateurs d'ordinateurs portables de se connecter régulièrement (fréquence hebdomadaire) au réseau informatique pour que cette mise à jour puisse être effectuée.

5.5 Téléchargements et installation de logiciels

Seules les personnes du département TIC sont habilitées à installer ou faire installer (par des tiers) sous leur contrôle des logiciels, y compris des logiciels libres.

Tous les logiciels doivent faire l'objet d'une demande officielle d'installation au département TIC qui en définira les modalités.

La propriété industrielle d'un *logiciel* est définie par un accord de licence indiquant les modalités et les conditions d'utilisation.
Il n'est pas autorisé de télécharger, installer, utiliser, copier ou contourner les restrictions d'utilisation d'un logiciel pour lequel la Collectivité n'a pas acquis de licence (pour le respect des droits de propriété).

Le non-respect de la licence peut entraîner des pénalités allant d'une simple amende à l'emprisonnement et engager la responsabilité de l'utilisateur ainsi que celle de la Collectivité.
L'installation de *logiciel* piraté est strictement interdite.
La copie d'un *logiciel* professionnel pour une utilisation personnelle est illégale.

ARTICLE 6 – PROTECTION ET ACCÈS AUX INFORMATIONS

6.1 Documents et communications privés et professionnels

Par défaut, les communications et documents créés, ouverts, modifiés, réalisés ou conservés en utilisant du matériel et/ou un système d'information mis à disposition par la Collectivité à titre professionnel pour l'accomplissement des missions de l'utilisateur sont présumés être à caractère professionnel.

L'utilisateur doit veiller à distinguer clairement les documents, courriers, messages ... qu'il considère comme personnels, des documents professionnels, en les rangeant dans des dossiers distincts nommés « **PRIVE** » **sous le répertoire « mes documents »**, et/ou en faisant figurer « **PRIVE** » en tête du nom des documents et de l'objet des **mails**.

Seul le département TIC est habilité à définir la taille de l'espace consacré aux données privées.
Tout document ou courriel ne respectant pas cette règle sera considéré comme relevant de la sphère professionnelle.

Les mails identifiés par leur expéditeur comme « privés » sont protégés par le secret des correspondances.

Il est admis que, si un mail n'est pas identifié comme « privé » et est donc par défaut présumé comme « professionnel », son accès par un technicien du département TIC dans le cadre des missions du département TIC telles que mentionnées à l'article 12 est possible.
Dans l'éventualité où le contenu d'un mail présumé professionnel s'avérait être personnel, le technicien du département TIC l'ayant consulté en tout ou partie dans le cadre de ses missions prévues à l'article 12 ne le retiendra pas dans les étapes ultérieures du contrôle mis en place et aura obligation de ne pas le divulguer.

Il est à noter qu'il est interdit de faussement (re)qualifier de « privé » un mail ou document professionnel afin de le soustraire au contrôle de la Collectivité.

Il est également à noter que, sans prendre connaissance du contenu des mails « privés », un contrôle de l'usage de la messagerie professionnelle peut mener le département TIC à déceler une utilisation excessive de la messagerie professionnelle à titre personnel et ainsi caractériser un dépassement de l' « usage raisonnable » évoqué à l'article 8.

De même, le poids et/ou le nombre de fichiers contenu dans un dossier « personnel » ou « privé » sur le disque dur d'un poste de travail pourront amener à la même conclusion, notamment si cela amène à une baisse de performance du poste de travail.

6.2 Respect de la confidentialité et de l'intégrité des données

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 sanctionné disciplinairement et pénalement.

En particulier, il est strictement interdit de modifier des fichiers contenant des informations comptables ou d'identification, ou tenter de prendre connaissance d'informations détenues par d'autres utilisateurs, même si ceux-ci ne les ont pas explicitement protégées, exception faite des données diffusées dans des dossiers publics ou partagés qui sont clairement identifiés.

Pour rappel, tous les documents professionnels sont la propriété de la Collectivité. Ils ne doivent donc être ni altérés ni supprimés.

En vue d'en assurer leur pérennité, les données professionnelles sensibles des utilisateurs et les données partagées doivent systématiquement être stockées sur les serveurs de données (GED ou dossiers partagés) et non sur les postes.

La pérennité des données privées ne relève pas du département TIC a contrario des données professionnelles.

6.3 Informations confidentielles et données à caractère personnel

6.3.1 Protection de l'information

Aucun utilisateur ne doit divulguer des informations confidentielles ou des données à caractère personnel à des tiers qui ne doivent pas les connaître.
De plus, l'utilisateur ne doit pas :

- détourner ou utiliser des informations propres à la Collectivité pour son usage personnel ou celui d'un tiers
- émettre de fausses déclarations ou fournir de fausses informations visant à falsifier les données des Collectivités
- supprimer ou modifier des données au détriment des Collectivités

6.3.2 Protection des données personnelles

La collecte de données et l'obtention de renseignements de la part de personnes physiques menant à des traitements automatisés et manuels et notamment création de fichiers concernant des informations relatives à des personnes (nom, prénom, mail, etc.,) doivent prévoir une information préalable quant aux finalités exactes des traitements, la liste des destinataires des diverses informations, ainsi que leur durée de conservation. En effet, la réglementation française et européenne de protection des données à caractère personnel définit les conditions dans lesquelles des traitements de données à caractère personnel peuvent être effectués et crée au profit des personnes physiques concernées par les traitements des droits que la présente charte invite à respecter, tant à l'égard des utilisateurs que des tiers.

Il est rappelé aux utilisateurs que tous les traitements de données à caractère personnel doivent être recensés par le Délégué à la protection des données personnelles (DPO). Par exemple, créer un simple fichier Excel peut constituer un nouveau traitement de données à caractère personnel.
Les utilisateurs souhaitant réaliser un nouveau traitement de données personnelles doivent prendre contact avec le Délégué à la protection des données personnelles (DPO) avant d'y procéder comme prévu à l'article 13.

Un délégué à la protection des données (ou DPO pour Data Protection Officer) veille au sein de la Collectivité à la bonne application de la réglementation française et européenne relative auxdits traitements.

Toute demande adressée par un utilisateur ou un tiers (prospects, clients, partenaires, fournisseurs, etc.) qui serait relative à des données à caractère personnel doit lui être immédiatement transférée.

ARTICLE 7 – UTILISATION DU MATÉRIEL ET RESPONSABILITÉ D'UTILISATION

7.1 Respect des consignes de Sécurité du Système d'Information

Tous les utilisateurs de la Collectivité s'engagent à respecter les consignes diffusées par le département TIC, afin de garantir le bon fonctionnement des outils informatiques et numériques.

Envoyé en préfecture le 14/08/2024
Reçu en préfecture le 14/08/2024
Publié le 14/08/2024
ID : 030-200066918-20240814-2024_0373D-AR

7.2 Respect du matériel

Chaque utilisateur doit :

- prendre soin du matériel et informer un technicien du département TIC de toute anomalie constatée ainsi que de toute perte ou vol, avéré ou suspecté, de matériel qui lui avait été attribué ou dont il avait l'usage à titre personnel ou collectif ;
- ne pas interrompre le fonctionnement normal du réseau ou saturer les ressources ;
- respecter les consignes de sécurité du réseau ;
- lors de la restitution du matériel, supprimer ce qui est contenu dans les dossiers privés.

Hormis le matériel affecté à un utilisateur à titre permanent, il est obligatoire de :

- réserver tout matériel numérique avant de l'emprunter pour son utilisation. Une note de service est à disposition afin de gérer les emprunts de matériel.

7.3 Usurpation d'identité

Aucun utilisateur ne doit tenter de masquer sa véritable identité ou d'usurper l'identité d'une autre personne pour essayer d'accéder à ses informations ou ses traitements.

7.4 Accès distants et VPN

Les documents copiés en local doivent être sécurisés par un système de sécurisation par mot de passe (de type BitLocker) mis en place par le département TIC avant toute mise à disposition d'ordinateur portable.

Une attention particulière doit être portée sur les risques de vol, aussi l'équipement ne doit pas être laissé sans surveillance.

Tout accès distant aux SI de la collectivité doit impérativement se faire via un tunnel sécurisé (VPN) fourni par le département TIC.

Les accès VPN ne sont autorisés que sur demande via le logiciel de ticketing GLPI.

7.5 Copieurs numériques multifonctions

Du fait de leurs fonctionnalités étendues, les copieurs numériques constituent un périphérique dont la sécurité doit être assurée comme celle des postes de travail informatiques. Dès lors que des informations à protéger transitent par ce type d'appareil, l'ensemble des recommandations et réglementations relatives aux systèmes d'informations s'appliquent.

Tous les points d'impression sont isolés d'internet ce qui empêche notamment l'envoi de mail vers l'extérieur.

Lors de la numérisation de documents, les utilisateurs doivent s'assurer que la destination des fichiers ainsi générés est accessible aux seules personnes habilitées à accéder à ces informations.

Les utilisateurs doivent s'abstenir de reproduire, copier, diffuser des pages web, images, photographies, textes ou toutes autres créations protégées par des droits d'auteur dans des conditions ne respectant pas ces derniers.

Envoyé en préfecture le 14/08/2024
Reçu en préfecture le 14/08/2024
Publié le 14/08/2024
ID : 030-200066918-20240814-2024_0373D-AR

ARTICLE 8 - MESSAGERIE ÉLECTRONIQUE

La messagerie électronique est un outil d'échange d'Informations, mais peut également être le vecteur de propagation de virus ou d'informations inutiles voire fausses (ex : canulars), ce qui peut se traduire par des pertes de temps et de productivité pour les utilisateurs.

Afin d'assurer la sécurité de cet outil ; certaines règles spécifiques sont à respecter, notamment :

- il est obligatoire d'utiliser Zimbra, la messagerie actuellement gérée par la Collectivité. L'utilisation, à titre professionnel, d'autres comptes de messagerie non validés par le département TIC est strictement interdite. En tout état de cause, l'usage de ces solutions ne saurait engager la responsabilité de la Collectivité et du département TIC, quant aux risques inhérents. De plus, le département TIC ne saurait en assurer la maintenance et la compatibilité avec les systèmes en place.
- les messages électroniques ne doivent comporter aucun élément illicite, tel que des propos diffamatoires, injurieux, contrefaisants ou susceptibles de contrevenir aux obligations des fonctionnaires (dignité, impartialité, intégrité, probité et neutralité)
- l'espace de stockage de la messagerie est limitée. Des dépassements de seuil peuvent être autorisés de manière dérogatoire
- sauf autorisation du département TIC, la messagerie électronique ne doit pas être utilisée pour des envois en nombre pouvant encombrer le réseau (notamment lors de l'utilisation inappropriée de listes de diffusion). En effet, l'anti-spam mis en œuvre par le département TIC pourrait bloquer leurs envois.
- l'utilisateur doit s'assurer du bien-fondé des messages qu'il émet vers ses correspondants et rester vigilant, et ainsi ne pas transmettre en connaissance de cause de fausses alertes ou canulars circulant par messagerie ;
- la vigilance des utilisateurs doit redoubler en présence d'informations confidentielles : les envois via messagerie électronique doivent être évités en faveur d'une transmission via support de stockage chiffré (via les plateformes de transfert de gros fichiers mises à disposition par le département TIC par exemple). L'utilisateur doit veiller à la protection des informations diffusées par messagerie. Il est rappelé que la confidentialité des échanges n'est pas techniquement assurée par la messagerie électronique en elle-même. En conséquence, celle-ci ne doit pas être utilisée sans sécurisation appropriée pour les échanges d'Informations ou de documents à caractère confidentiel ou sensible, même à titre de projets, ainsi que de transfert de données personnelles sensibles ou en masse. Par sécurisation, on entend des outils supplémentaires, fournis et maîtrisés par le département TIC. Chaque utilisateur qui diffuse ou transfère des messages par courrier électronique est entièrement responsable du respect de la confidentialité qui y est attachée ;
- l'utilisateur ne doit, en aucun cas, activer le reroutage automatique de ses messages vers une adresse de messagerie externe à la Collectivité, afin d'éviter que des messages sensibles se trouvent envoyés sur Internet à l'insu de l'émetteur ;
- en cas d'absence d'un utilisateur et pour des raisons de continuité de service, la boîte de réception de sa messagerie peut être amenée, sur décision de la personne responsable concernée et après validation du département TIC, à être partagée avec un ou plusieurs autres utilisateurs ; dans ce cas, une information ultérieure sera délivrée à l'utilisateur concerné.
- l'utilisateur doit faire preuve de vigilance vis-à-vis de l'identité des auteurs des messages reçus, notamment de correspondants extérieurs. En effet, la falsification de l'identité de l'auteur d'un message est facilement réalisable sur Internet
- l'utilisateur doit faire preuve de vigilance vis-à-vis de l'identité de chacun des destinataires de ses messages, et notamment dès lors qu'il répond à des messages

collectifs ou dès lors que les adresses ne sont pas individuelles mais génériques ou des listes de diffusion ;

Seuls sont gérés les noms de domaine dont les Collectivités sont titulaires (par exemple, ceux qui se terminent par @alesagglo.fr, @ville-ales.fr, @payscevennes.fr, @ales.fr...)

Aucune pièce jointe à un mail ne doit être ouverte si l'utilisateur n'est pas absolument certain de sa provenance et de son innocuité.

Si cette pièce jointe est un document contenant des macros (tels que Word, Excel, OpenOffice Writer, Calc), il ne faut pas en permettre l'exécution (risque de macro virus).

La messagerie dispose d'un outil de filtrage qui élimine automatiquement tout message suspect, en entrée et en sortie.

La sélection est faite sur le type et le nom des pièces jointes.
Sont également éliminés tous les messages considérés comme des spams, et qui sont reconnus par la teneur du titre ou du texte du message (recherche de termes tels que viagra...).
Attention, ces filtres ne sont pas fiables à 100%.
Certains spams ne sont pas détectés, et il peut aussi arriver que des messages légitimes soient écartés.
Il est donc demandé à chaque utilisateur d'être particulièrement précautionneux face à un mail ne faisant pas parfaitement sens et invitant à accéder à un lien ou à une pièce jointe (expéditeur inconnu, contenu non professionnel, lien URL camouflé, présentation ou style rédactionnel inhabituels, etc)

Remarque importante :

Un message électronique peut constituer une preuve et peut engager fermement son expéditeur et/ou la Collectivité et son destinataire : il existe donc un risque réel qu'un agent prenne des engagements qu'il faudra ensuite respecter. Ainsi, toutes les recommandations concernant les échanges écrits avec des tiers s'appliquent également à la messagerie.
L'envoi de messages électroniques doit respecter les mêmes procédures de contrôle, de validation, d'autorisation que les courriers traditionnels ou papier.

Il est souhaitable de mettre systématiquement en copie des messages importants, son responsable et le responsable du destinataire, et il est obligatoire de transmettre pour validation à un responsable tout message qui aurait valeur contractuelle ou d'engagement.

Par ailleurs, tout message important doit être conservé (GED, dossiers partagés, etc) à des fins d'archivage.

La diffusion des messages doit être limitée aux seuls destinataires concernés, afin d'éviter l'encombrement inutile de la messagerie et une dégradation des temps de réponse.

Attention, les messages non sollicités (appels à la solidarité et autres chaînes) que leur auteur demande de diffuser à un maximum de personnes, sont généralement des canulars (hoax, etc....).

Il est rappelé que la messagerie professionnelle mise à disposition des utilisateurs est en principe réservée à un usage strictement professionnel.
Toutefois, une tolérance est admise en faveur d'un usage personnel dès lors qu'il reste dans des « proportions raisonnables ».

Envoyé en préfecture le 14/08/2024
Reçu en préfecture le 14/08/2024
Publié le 14/08/2024
ID : 030-200066918-20240814-2024_0373D-AR

Dans ce cas, les conditions fixées à l'article 6 (utilisation limitée et raisonnable, marquage des messages à caractère privé...) s'appliquent.
Cette tolérance s'applique préférentiellement aux échanges entre individus, l'utilisation de l'adresse professionnelle comme support d'échanges privés avec des entités commerciales, associatives... étant fortement déconseillée (l'adresse professionnelle n'étant plus accessible à l'utilisateur en cas de départ de la Collectivité). L'inscription, pour des besoins privés, sur des sites Internet, des réseaux sociaux, des lettres d'information doit donc privilégier les adresses électroniques privées des individus afin de réduire l'exposition de la messagerie de la Collectivité aux messages frauduleux et aux spams destinés aux particuliers.

Attention aux limites à l'utilisation de la messagerie professionnelle :
Il est expressément rappelé que les messages envoyés par un utilisateur à partir de sa messagerie professionnelle doivent de manière générale respecter les dispositions législatives et réglementaires applicables et être conformes à ses obligations déontologiques (dignité humaine, harcèlement...).

Les utilisateurs sont invités à accorder une attention particulière au contenu et à la forme des mails professionnels, d'autant plus lorsque ces derniers ont de nombreux destinataires ou groupes de diffusion.

ARTICLE 9 - ACCÈS A INTERNET

Chacun est responsable de sa navigation sur internet.

La connexion Internet mise à la disposition des utilisateurs est en principe réservée à un usage strictement professionnel mais une tolérance est néanmoins admise en faveur d'un usage privé dès lors qu'il reste raisonnable et sous certaines conditions.

Il est rappelé que, tant en matière pénale que disciplinaire, tout comportement, action ou expression via internet est appréhendé de la même manière que les autres moyens de communication et d'interaction.

9.1 Absence de confidentialité

Tout utilisateur est automatiquement émetteur et récepteur d'information.
Il faut être conscient que des traces sont laissées de la navigation sur Internet. Il s'agit, par exemple, de l'historique des consultations stocké sur le disque dur de l'utilisateur ou encore des cookies permettant la personnalisation des informations affichées sur certains sites.

9.2 Consultation des sites web

Les sites Web visités doivent par définition avoir un lien avec l'activité professionnelle.

La copie de pages, d'images ou de documents doit respecter les droits de propriété et les contrats de licence.
L'accès Internet ne peut être utilisé comme support d'activités à but lucratif ou de nature à porter atteinte à la libre concurrence et à l'image de la Collectivité .

En particulier, la consultation d'Internet ne doit pas être un moyen pour les utilisateurs de se procurer ou de participer à des jeux, des activités commerciales ou une activité en contradiction avec la législation en vigueur.

Pourront faire l'objet d'un dépôt de plainte ou signalement au Procureur les utilisations du système d'informations, notamment le téléchargement de fichiers ou consultation de sites ou blogs à caractère pornographique, pédophile, xénophobe, antisémite, raciste..., etc. , de telles utilisations pouvant également faire, le cas échéant, l'objet d'un dépôt de plainte ou signalement au Procureur.

L'usage privé du Web pourra se faire dans la limite du raisonnable à savoir qu'il est possible de surfer, en dehors des horaires de travail, durant les pauses déjeuner ou après sa journée, et sur des sites sécurisés uniquement et qui ne sont pas de nature à compromettre la sécurité ou à nuire à l'usage des systèmes de réseaux.
Certains sites internet ne sont pas consultables pour des raisons de sécurité : webmail, réseaux sociaux, transferts de fichiers.

Pour information, les logs de connexions sont conservés de manière automatique durant une période d'un an : l'adresse du site) la date et l'heure de toute connexion à un site web depuis un ordinateur (identifié par une adresse IP) utilisant le réseau de la Collectivité.
Les utilisateurs sont informés par la présente charte que la Collectivité ne garantit aucunement la sécurité des informations personnelles envoyées ou reçues lors de l'usage privé du Web, par exemple achats en ligne, consultation de comptes bancaires en ligne, accès à des données de santé, etc. ; ceci incluant les identifiants individuels, les moyens de paiement et les documents téléchargés.
Le visionnage notamment de vidéos en streaming via des sites tels que YouTube, Dailymotion ... pourra être encadré et régulé par le département TIC (cas de régulation de la bande passante).

9.3 Téléchargements par protocole de transfert de fichier (FTP)

Les transferts sont réservés, par mesure de sécurité, au département TIC. Les demandes motivées des utilisateurs lui parviennent par logiciel de ticketing « GLPI ».

9.4 Protection par un pare-feu (firewall)

L'ouverture du réseau local à Internet est protégée par un pare-feu (firewall).
La politique d'usage d'Internet est affinée (proxy).
Il est formellement interdit aux utilisateurs d'essayer de passer outre ces deux équipements .

Le Département TIC, pour la tenue de tableaux de bord, et en tant que de besoin, a accès aux informations mémorisées par ces équipements.

9.5 Confidentialité et accès internet

Il est strictement interdit de divulguer toutes informations concernant l'activité, les missions, l'organisation ou les communications internes des collectivités ou de leurs tiers sur toute plateforme sans accord préalable de la Direction. Cette mesure implique notamment les communications faites sur les réseaux sociaux.

ARTICLE 10 – RÉSEAUX SANS FIL

Les technologies sans fil (Wifi, Bluetooth, 4G/5G) présentent de nombreuses failles de sécurité si elles sont mal configurées. De manière générale, l'usage de ces technologies est à éviter, au profit d'une connectivité filaire standard.

10.1 Réseaux wifi professionnel

L'accès aux réseaux WIFI doit être limité à une utilisation professionnelle et exceptionnelle. Les conditions d'accès sont définies dans la politique de sécurité des systèmes d'information d'Alès Agglomération.

10.2 Réseaux WIFI publics

Lors de l'utilisation de réseaux WIFI publics, il convient de veiller à se connecter sur des WIFI identifiés et fiables afin de ne pas exposer le terminal (ordinateur portable ou smartphone) à des menaces.

10.3 Partage de connexion 4G

Seuls les terminaux mobiles fournis par la Collectivité peuvent être utilisés comme point d'accès à internet pour les ordinateurs portables de la collectivité.

ARTICLE 11 –TÉLÉPHONIE ET TABLETTES

11.1 Dispositions générales

La mise à disposition de terminaux de communication, fixe et/ou mobile au sein de la Collectivité est essentiellement destinée à satisfaire les besoins professionnels.

L'utilisateur doit rester vigilant dans l'utilisation des réseaux téléphoniques publics fixes ou mobiles, la confidentialité des échanges n'étant pas garantie sur ces réseaux.

Avant tout déplacement en dehors du territoire français, il est demandé aux agents de prévenir le Département TIC afin de s'assurer que le roaming (utilisation de réseaux téléphoniques en itinérance) est actif sur les territoires concernés. A défaut, des mesures de blocages des communications pouvant entraîner des frais additionnels pourront être appliquées.
Il est demandé une vigilance particulière aux Utilisateurs quant à leurs usages en dehors du territoire français.

11.2 Dispositions spécifiques aux téléphones portables

Lorsqu'un utilisateur dispose d'un terminal mobile fourni par la Collectivité, il lui est interdit d'utiliser son terminal mobile personnel dans le cadre de son activité professionnelle.

Les ressources ou services ne doivent pas être accessibles à des tiers y compris en cas d'absence ou de dépôt momentané du téléphone portable : il convient alors de le mettre en veille dès lors qu'il n'est plus sous la surveillance de l'utilisateur, même momentanément.
Pour rappel, le titulaire du compte utilisateur est responsable de tout acte de malveillance opéré depuis le téléphone en cas de négligence.
L'usage de la mise en veille automatique avec code de déverrouillage et la personnalisation du code PIN sont également obligatoires sur les téléphones portables.
Les documents et fichiers professionnels peuvent être consultés sur le téléphone portable mais ne doivent pas être conservés au-delà de la durée nécessaire pour leur utilisation.

Les utilisateurs de smartphones professionnels ne doivent pas télécharger des applications de sources inconnues sur un site différent de celui de l'éditeur, notamment sur un site d'échange de fichiers.

Comme sur un poste de travail, l'accès à internet et les différentes capacités de communication (mail, sms) mis à disposition par la Collectivité à titre professionnel à ses

Envoyé en préfecture le 14/08/2024
Reçu en préfecture le 14/08/2024
Publié le 14/08/2024
ID : 030-200066918-20240814-2024_0373D-AR

agents, sur un smartphone mis à la disposition des utilisateurs dont les fonctions le requièrent, sont en principe réservés à un usage strictement professionnel mais une tolérance est néanmoins admise en faveur d'un usage privé dès lors qu'il reste raisonnable et ne remet pas en cause la sécurité du système d'information.

Pour des raisons de sécurité, les utilisateurs de smartphone peuvent se voir interdire l'installation et l'utilisation de certaines applications.
Une stratégie d'enrôlement par un logiciel dit MDM (mobile device management) a été mise en place afin de superviser la flotte mobile et notamment pour effectuer les mises à jour des applications métiers à distance.
Ce logiciel limite les installations d'applications par l'utilisateur à un catalogue prédéterminé afin d'empêcher toute interaction néfaste aux applications métiers installées par le département TIC lors de la configuration initiale de l'appareil.
Les utilisateurs souhaitant installer de nouvelles applications pour leur usage privé doivent en effectuer la demande au département TIC.
La demande peut recevoir une réponse négative notamment lorsque l'application en question :

- est illicite,
- comprend des problèmes de sécurité (vulnérabilités, failles de sécurité, politique de transfert de données à des tiers, etc),
- consomme les données de navigation d'une manière trop importante au regard des abonnements souscrits,
- utilise la batterie du téléphone d'une manière trop intense au regard du taux de renouvellement retenu pour la flotte mobile,
- relève d'un usage tellement privé qu'il sort du cadre de l'usage privé raisonnable et pouvant être toléré sur un téléphone professionnel mis à disposition par la Collectivité.

Par dérogation, les utilisateurs dont le niveau de responsabilité et les connaissances permettent d'éviter les utilisations dommageables du téléphone portable peuvent recevoir un profil qui conserve la capacité à installer des applications. L'accès à ce type de profil peut être révoqué par la Collectivité en cas d'utilisation problématique du téléphone.

L'accès du département TIC par le MDM ne comprend pas :

- les photos, les documents téléchargés, les données personnelles,
- les parties du téléphone relative à la captation ou à l'émission audiovisuelle ou sensitive, et notamment le micro, la caméra, le son. Pour toutes les ondes radio (son, 4G, bluetooth, etc), le détail des données transmises n'est pas accessible,
- les messages non électroniques de type SMS,
- les mails sur une messagerie autre que zimbra. Pour la messagerie zimbra, les modalités d'accès sont identiques à celles prévues à l'article 8.

Afin de protéger les données professionnelles et le système d'information de la Collectivité, le MDM permet au département TIC d'opérer à distance la suppression de toutes les données présentes sur le téléphone perdu ou volé, tant professionnelles que privées le cas échéant.

L'accès à la messagerie zimbra en contournant l'interface websso, par une installation dans un client de messagerie dit « client lourd » sur tout autre téléphone qu'un téléphone professionnel mis à disposition par la Collectivité est strictement interdit.

L'utilisation du smartphone pour la navigation sur internet relève de la responsabilité de l'utilisateur, tant au niveau de la licéité des contenus consultés que des risques associés à la consultation de sites internet n'offrant pas de garanties suffisantes de sécurité (absence de certificats notamment).

Il est interdit d'installer la carte SIM correspondant à la ligne et au forfait mis à disposition par la Collectivité dans un téléphone portable autre que celui mis à disposition. En cas de changement du téléphone porteur de la carte SIM, la ligne sera suspendue par la Collectivité.

11.3 Dispositions spécifiques aux tablettes

Outre les dispositions généralement applicables au système d'information et de communication et à tout moyen permettant l'accès aux ressources (usage à titre privé, messagerie, etc), l'utilisation des tablettes mises à disposition des utilisateurs dans le cadre de l'exercice de leur fonction ou missions est régie par les dispositions prévues à l'article 11.2 ci-dessus, notamment pour ce qui concerne :
- l'usage des données mobiles
- la stratégie d'enrôlement par le logiciel dit MDM et plus généralement les limitations et interdictions relatives à l'installation et l'utilisation des applications et programmes
- les mesures de sécurité

ARTICLE 12 - MISSIONS DU DÉPARTEMENT TIC

12.1 Droits et devoirs spécifiques des techniciens du département TIC

Les techniciens du département TIC doivent veiller à assurer le fonctionnement normal et la sécurité des réseaux et systèmes. Ils sont conduits par leurs fonctions mêmes à avoir accès à l'ensemble des informations relatives aux utilisateurs (messagerie, connexions Internet, fichiers « log » ou de journalisation, etc.) y compris celles qui sont enregistrées sur le disque dur du poste de travail, dans la mesure où cela se rattache à un objectif de sécurité du réseau.

Les techniciens du département TIC sont tenus au secret professionnel et à une obligation de discrétion professionnelle.
Ils ne doivent pas divulguer des informations qu'ils auraient été amenés à connaître dans le cadre de leurs fonctions, et en particulier lorsque celles-ci sont couvertes par le secret des correspondances ou relèvent de la vie privée des utilisateurs et ne mettent en cause ni le bon fonctionnement technique des applications, ni leur sécurité, ni l'intérêt de la Collectivité.

12.2 Rôle en matière de sécurité

En matière de sécurité, le département TIC a pour mission de :
- veiller à la sécurité, l'intégrité et la disponibilité du réseau informatique,
- identifier le plus rapidement les attaques (virus, vers, trojan, rançongiciels, DOS, exfiltration de données, ...),
- mettre en place les actions de communication et techniques visant à stopper le plus rapidement la diffusion des virus et les tentatives d'intrusion ou de détournement portant sur le réseau.

12.3 Audits/tests

Des audits ayant pour objectif de vérifier la conformité des mesures en place par rapport à la politique de sécurité des systèmes d'information en vigueur sont organisés régulièrement.
L'ensemble des utilisateurs doit, lors de ces audits, se soumettre aux contrôles de son matériel et de ses bonnes pratiques.

12.4 Enregistrement des activités pour contrôle

Les utilisateurs sont informés et donc parfaitement conscients que leurs activités sur les systèmes de la Collectivité sont tracées et enregistrées conformément à la politique de traitement de l'information en vigueur. Ces enregistrements peuvent être exploités en cas d'incident de cybersécurité ou de suspicion de malveillance ou de fuite de données.
Ces données peuvent être transmises aux autorités compétentes si nécessaire.

Pour les informations relatives à l'utilisation des **postes de travail**, sont enregistrés pendant trois mois les détails :

- des connexions sur les postes de travail : identifiant des connexions réussies et refusées,
- des « erreurs système » recensées sur les postes de travail,
- des incidents recensés par le logiciel antivirus et l'EDR (end point detection and response, service de détection et de réponse des terminaux) sur les postes de travail,
- des incidents recensés par le pare-feu individuel, pour les postes de travail qui en sont munis : flux bloqués, non-conformités détectées, etc...

Les logs de **connexion à internet** sont conservés de manière automatique durant une période de un an :
- l'adresse du site,
- la date et l'heure de toute connexion à un site web depuis un ordinateur (identifié par une adresse IP) utilisant le réseau de la Collectivité,
L'attribution de l'adresse IP au nom d'une machine est conservée pendant un an.
Les informations enregistrées, pour chaque accès aux ressources partagées (ressources «réseau »), sont :

- date et heure de la connexion,
- identifiant utilisé pour la connexion,
- profil associé à la connexion (privilèges accordés, capacité de lecture et/ou écriture).

La durée de conservation des journaux est de trois mois.

Les informations enregistrées, pour chaque **connexion aux Systèmes d'Information de la Collectivité depuis l'extérieur**, sont :

- Date et heure de début et de fin de connexion,
- Applications consultées,
- Identifiant utilisé pour la connexion,
- Volumes de données transmis.

La durée de conservation des journaux est d'un an.

Pour les **appels téléphoniques**, sont enregistrées les métadonnées associées à la communication suivantes : le numéro appelé, la date, l'heure, la durée et le coût de tous les appels téléphoniques externes passés par les postes téléphoniques (fixes, mobiles et cellulaires) et les fax reliés aux réseaux téléphoniques de la Collectivité sont archivées ou peuvent être requises.
Les quatre derniers chiffres sont masqués pour toute édition, conformément au RGPD.

Pour la **messagerie électronique**, une copie de tout message électronique entrant ou sortant est conservée 30 jours.

Il est nécessaire d'obtenir l'autorisation du Département TIC avant de volontairement tenter de crypter ou masquer ses activités sur les systèmes.

Envoyé en préfecture le 14/08/2024
Reçu en préfecture le 14/08/2024
Publié le 14/08/2024
ID : 030-200066918-20240814-2024_0373D-AR

12.5 Communication, sensibilisation et information

Toute demande d'assistance informatique et pour tout élément du système d'information et de communication est à effectuer en priorité sur le logiciel de ticketing GLPI afin que le Département TIC puisse en assurer l'assignation et le suivi de l'intervention.

Lors de son intégration, tout utilisateur d'un système d'information de la Collectivité reçoit une initiation au bon usage du SI, conçue voire directement effectuée par un agent du département TIC.
Le Département TIC est à la disposition des agents pour leur fournir toute information concernant l'utilisation des ressources informatiques et de communication électronique. Il informe les utilisateurs régulièrement sur l'évolution du système d'information et sur les menaces susceptibles de peser sur sa sécurité.

Des opérations de communication internes sont organisées, de manière régulière, afin d'informer les agents sur les pratiques d'utilisation recommandées du système d'information et de communication.
Tout utilisateur d'un système d'information de la Collectivité peut être invité à participer à des séances de sensibilisation aux risques liés à la sécurité informatique.

12.6 Prise de main à distance

Le département TIC dispose d'outils de prise de main à distance qui sont principalement employés pour assurer le bon fonctionnement des SI ou pour permettre le bon fonctionnement du SI pour chaque utilisateur.
Ces prises de main et observations à distance se feront toujours avec l'accord de l'intéressé : il est averti par un message à l'écran qu'il doit valider pour que la prise de main ou l'observation puisse démarrer. En cas de prise de main suspecte, l'agent se doit d'en référer directement au département TIC.

ARTICLE 13 - MISSIONS DU DPO (DÉLÉGUÉ A LA PROTECTION DES DONNÉES)

Le Délégué à la protection des données est l'interlocuteur privilégié de la CNIL. Il veille à la bonne application de la loi Informatique et Libertés. Il s'assure du respect du droit à la protection des données personnelles des administrés et des utilisateurs, les cas de saisine étant indiqués à l'article 6.3.2.

Il peut être joint par courriel : dpo@alesagglo.fr ou par voie postale à l'adresse suivante : Alès Agglomération, À l'attention du délégué à la protection des données (DPO) Bâtiment ATOME, 2 rue Michelet, 30105 Alès Cedex

ARTICLE 14 – DROIT À L'IMAGE ET DROITS D'AUTEUR

L'image d'une personne ne peut être utilisée ou diffusée sans son consentement écrit (celui de son responsable légal pour un mineur).

Les photos prises dans le cadre des activités de la Collectivité ne peuvent pas être utilisées à des fins personnelles, et leur réutilisation est interdite sans le consentement écrit de la personne dont l'image a été capturée.
Cette obligation s'applique aux enregistrements vidéo et sonores.

Envoyé en préfecture le 14/08/2024
Reçu en préfecture le 14/08/2024
Publié le 14/08/2024
ID : 030-200066918-20240814-2024_0373D-AR

Par application des dispositions relatives aux droits d'auteur, il est rappelé qu'il est interdit à l'utilisateur de télécharger des contenus multimédias (écrit, MP3, films, ...) non libres de droits, de les mettre à disposition sur le réseau ou de les réutiliser de quelque manière que ce soit, sans le consentement de l'auteur ou l'autorisation de la personne compétente.

Le streaming (lecture directe) d'œuvres non libres de droits est également interdit.

ARTICLE 15 – INFORMATIONS ET SANCTIONS DES UTILISATEURS

15.1 Information des utilisateurs

Chaque utilisateur a le devoir de se former aux techniques de sécurité physiques et logicielles, notamment via les formations internes dispensées par le Département TIC ou les publications Léo.

15.2 Sanctions

Tout utilisateur ne suivant pas les règles et obligations le concernant rappelées dans cette charte pourra se voir, par mesure conservatoire, suspendre l'accès aux ressources informatiques, téléphoniques, et/ou à certains services (internet, messagerie...).

L'utilisation de tous moyens techniques permettant de contourner une ou plusieurs règles de la présente charte (free proxy, client VPN, SSH...) pourra être considéré comme un facteur aggravant de l'action répréhensible ou dommageable.

D'une manière générale tout utilisateur n'ayant pas respecté les textes en vigueur pourra être poursuivi civilement et/ou pénalement.

Il est par ailleurs indiqué que, indépendamment de l'interdiction expresse par la présente charte de certaines actions, celles-ci peuvent recevoir la qualification d'infraction par le Code pénal, principalement aux articles abordant les atteintes aux systèmes de traitement automatisé de données (323-1 et suivants).
Sont ainsi notamment répréhensibles :
- l'accès ou le maintien dans un tel système, avec ou sans modification de données, par exemple pour un prestataire conservant un accès spécifique au-delà de ce qui lui est nécessaire, ou un agent public conservant ses accès
- le fait d'extraire, de détenir, de reproduire, de transmettre, de supprimer ou de modifier frauduleusement les données.

ARTICLE 16 : DISPOSITIONS SPÉCIFIQUEMENT APPLICABLES AUX UTILISATEURS AGENTS PUBLICS

Pour cet article, « utilisateurs » s'entend au sens d'« utilisateurs agents publics ».

16.1 Rappel général

Les utilisateurs s'engagent à ce que leur activité sur le réseau ne soit pas de nature à remettre en cause la neutralité du service public (non-discrimination, neutralité religieuse et neutralité politique) ainsi que l'ensemble des obligations qui s'imposent aux agents publics conformément aux dispositions statutaires et réglementaires (obligation de réserve, obligation de discrétion professionnelle, secret professionnel, etc....).

Envoyé en préfecture le 14/08/2024
Reçu en préfecture le 14/08/2024
Publié le 14/08/2024
ID : 030-200066918-20240814-2024_0373D-AR

De plus, la communication ou le partage de documents de nature politique ou religieuse envers les autres utilisateurs par les outils couverts par la présente charte sont interdits.

Outre le caractère disciplinaire, l'utilisateur est informé que sa propre responsabilité, celle de son chef de service, et celle de la Collectivité 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.

16.2 : Usage de la messagerie professionnelle

En complément de la mention dans l'article 8, il est précisé que le contenu des messages des utilisateurs visés par le présent article ne doit pas être susceptible de contrevenir aux obligations des agents publics ou de constituer un manquement à leurs devoirs.

Les manquements sont entre autres :

- les manquements à l'obligation de discrétion professionnelle (ne pas divulguer d'éléments internes à l'administration vers l'extérieur, ou d'éléments propres au service voire à l'emploi à des collègues n'ayant pas à en connaître), au devoir de réserve (position envers son administration et en tant qu'agent public), au respect du secret professionnel (ne pas révéler d'informations confidentielles, tant vers l'extérieur qu'envers des services ou collègues n'ayant pas à en connaître), à l'obligation de dignité, ou tout ce qui peut être relatif au harcèlement moral par courrier électronique,
- tous messages antisémites, racistes ou xénophobes, constitutifs de toute désobéissance hiérarchique, relatifs aux pétitions électroniques, susceptibles de porter atteinte à l'obligation de neutralité du service public...,
- un usage privé inapproprié de la messagerie, du fait notamment de la fréquence trop importante des messages reçus ou envoyés, du volume de données échangées (messages et pièces jointes), du transfert de messages professionnels confidentiels, etc., ainsi qu'en cas d'utilisation abusive ou malveillante de la mention « privé ».

16.3 : Communications publiques dans le cadre de la sphère privée

Il est rappelé que, même dans le cadre de ses activités privées, l'agent public reste soumis aux droits et obligations qui s'appliquent dans ses communications et prises de parole. Ainsi, et quand bien même sa liberté d'expression en tant que citoyen est protégée, le devoir de réserve, la discrétion professionnelle, et le respect du secret professionnel trouvent particulièrement à s'appliquer dans les publications sur des sites permettant de s'exprimer auprès d'un public (réseaux sociaux) ou dans des publications sur un site personnel.

Toute atteinte à l'image de la Collectivité à travers des forums, réseaux sociaux ou autre publication à caractère public de la part d'un agent sera considérée comme une faute professionnelle et passible des sanctions prévues par la loi.

16.4 Précautions spécifiques quant à l'utilisation des ressources

Lors de l'utilisation de ressources concernées par le droit à l'image, plus généralement au droit au respect de la vie privée, ou concernées par les droits d'auteurs et droits voisins, les précautions à respecter mentionnées à l'article 14.2 pèsent plus particulièrement sur les utilisateurs agents publics.
En effet, des agissements irrespectueux des droits des tiers sont susceptibles d'amener à ce que la responsabilité de la Collectivité soit recherchée lorsque ses moyens sont utilisés, en plus de la responsabilité civile et/ou pénale de l'auteur de ces agissements.

Envoyé en préfecture le 14/08/2024
Reçu en préfecture le 14/08/2024
Publié le 14/08/2024
ID : 030-200066918-20240814-2024_0373D-AR

Les utilisateurs sont informés que ces conséquences de leurs actes peuvent le cas échéant être prises en compte lors d'une procédure disciplinaire.

16.5 Accès aux données pour continuité du service

L'absence de l'agent ne doit pas se traduire par une perte d'accès aux données et fichiers nécessaires au fonctionnement du service.

L'agent doit veiller à ce que le service puisse accéder aux documents, logiciels et dossiers indispensables à l'activité, que ce soit par transmission des documents et dossiers aux collègues, mise à disposition dans un dossier partagé, ou création de comptes pour accéder aux applications, mais à l'exclusion de toute communication de mots de passe personnels.
En cas de nécessité de service (absence de l'agent due à la maladie, accident, décès, ou urgences quelle qu'en soit la nature...), le supérieur hiérarchique pourra demander par écrit au département TIC l'accès aux données de travail de l'agent absent ou la création d'un autre compte pour remplacer l'agent.

Le responsable du département TIC ou son supérieur hiérarchique sont les seuls habilités à désigner les agents TIC pouvant communiquer ces informations.

En cas de départ définitif ou d'absence prolongée d'un agent public et si la continuité du service le nécessite, le successeur récupère les documents de travail ainsi que les messages d'ordre professionnel, à l'exception des documents et messages privés (voir article 6.1 Documents privés et professionnels).

16.6 Comportement contraire à la charte

L'utilisation de tous moyens techniques permettant de contourner une ou plusieurs règles de la présente charte (free proxy, client VPN, SSH...) pourra être considérée comme une faute professionnelle.

En cas de manquement et/ou d'intention manifeste de nuire au bon fonctionnement des ressources ou à l'activité des services, l'agent public sera passible de sanctions disciplinaires proportionnelles à la gravité des manquements constatés.

ARTICLE 17 – INFORMATION DES UTILISATEURS

Cette charte est évolutive et susceptible d'être modifiée et complétée régulièrement en fonction des évolutions technologiques et réglementaires en la matière.

Elle fera l'objet d'une large diffusion, tant collective qu'individuelle, par tout moyen utile (intranet, messagerie, note de service, affichage...) afin que nul ne puisse ignorer son existence et son contenu.

Le fait que la présente charte aborde certains sujets n'empêche pas que des notes de service viennent fixer des modalités techniques spécifiques à certains éléments du système d'information et de communication.

Toutes les personnes responsables d'un accès, usage ou utilisateur doivent veiller à communiquer et à faire accepter les termes de la présente charte à toute personne à laquelle elles permettraient, sous leur propre responsabilité, d'accéder au système d'information et de communication de la Collectivité.

Envoyé en préfecture le 14/08/2024
Reçu en préfecture le 14/08/2024
Publié le 14/08/2024
ID : 030-200066918-20240814-2024_0373D-AR

La présente charte a fait l'objet d'une consultation du Comité Social Territorial le 11 juin 2024 et est applicable à compter du 1er juillet 2024.

ANNEXE 1 – LÉGISLATION ET BASES LÉGALES

Le législateur et la jurisprudence offrent un corpus de règles permettant de préciser les modalités d'utilisation de l'outil informatique, des réseaux et de la téléphonie, en essayant d'offrir une solution médiane, conciliant le souci légitime des employeurs, et notamment les personnes publiques, d'assurer l'exécution de leurs missions et la protection des droits des agents, tout statut confondu et plus généralement de l'ensemble des utilisateurs de ces outils.

La présente annexe a donc pour objectif d'informer les utilisateurs des principaux textes législatifs et réglementaires définissant notamment les droits et obligations des personnes utilisant les moyens informatiques.

Sources internationales et communautaires :

- La Déclaration universelle des droits de l'homme du 10 décembre 1948
- Convention européenne de sauvegarde des droits de l'homme du 4 novembre 1950
- Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel. Strasbourg, 28.I.1981
- Convention de Budapest sur la cybercriminalité du 23 novembre 2001
- Charte des droits fondamentaux de l'Union Européenne du 7 décembre 2000
- Directive du 12 juillet 2002 modifiée par la Directive 2009/136/CE (la « Directive ePrivacy)
- Règlement général sur la protection des données (RGPD) : règlement 2016/679/UE du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement et de la libre circulation des données à caractère personnel

Lois :

- Loi n° 78-17 du 6 janvier 1978. Loi relative à l'informatique, aux fichiers et aux libertés
- Loi n° 94-665 du 4 août 1994 modifiée, relative à l'emploi de la langue française.
- Loi n°2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique
- Ordonnance n° 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives.
- Loi n° 2021-1382 du 25 octobre 2021 relative à la régulation et à la protection de l'accès aux œuvres culturelles à l'ère numérique

Codes :

- Code des relations entre le public et l'administration
- Code général de la fonction publique
- Code civil et notamment ses articles 9 (droit à la vie privée) et 1240 et suivants (responsabilité civile délictuelle)
- Code du patrimoine et notamment ses articles L.211-1 à L211-6 (archives)
- Code pénal et notamment ses articles 222-17 (menace par écrit ou image), 226-1 à 226-8, 226-15 à 226-24 (atteinte à la vie privée) , 227-23, 227-24, 323-1 à 323-7 (atteintes aux systèmes de traitement automatisé de données), 432-9 (atteintes au secret des correspondances), 434-23, articles R. 625-10 à R. 625-13 (atteintes aux droits de la personne résultant des fichiers ou des traitements informatique)
- Code de la propriété intellectuelle et notamment son article L.122-6 et suivants (exploitation d'un logiciel)
- Code du travail
- Code des postes et communications électroniques et notamment ses articles L. 34-1 (Protection de la vie privée des utilisateurs de réseaux) et R.10-13 (conservation des données de connexion)
- Code de procédure civile et notamment son article 145 (référé probatoire)

Décrets :

- Décret n°88-145 du 15 février 1988 relatif aux agents contractuels de la fonction publique territoriale 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 non titulaires de la fonction publique territoriale
- Décret n°2005-1124 du 6 septembre 2005 pris pour l'application de l'article 17-1 de la loi n° 95-73 du 21 janvier 1995 et fixant la liste des enquêtes administratives donnant lieu à la consultation des traitements automatisés de données personnelles mentionnés à l'article 21 de la loi n° 2003-239 du 18 mars 2003
- Décret n° 2019-536 du 29 mai 2019 pris pour l'application de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés

Autres (Dispositions mentionnées et recommandations dispensées par la CNIL...) et jurisprudence abondante en la matière, par exemple :

- Arrêt de la cour de cassation n°4164 du 02/10/2001, 99-42.942 (courriers électronique et la vie privée du salarié)
- CAA de Rennes, 14.01.2010 (l'usage de la messagerie professionnelle est en principe réservé à une finalité professionnelle)

ANNEXE 2 - GLOSSAIRE

Les définitions utilisées n'ont vocation à s'appliquer qu'à la présente charte, sauf mention contraire dans d'autres actes.

Activité professionnelle : l'activité nécessaire, utile, dépendante ou complémentaire à l'activité des services, quelle qu'en soit la nature.

Administrateur : au sein du département TIC, les administrateurs sont des techniciens disposant d'accès privilégiés au niveau des systèmes d'information, leur permettant d'en gérer et contrôler le fonctionnement.

Authentifiant / moyen d'authentification : élément ou ensemble d'éléments permettant à un Utilisateur ou à une ressource d'un système d'information de prouver son identité afin, par exemple, de se voir attribuer des droits d'accès à un système d'information ou à des informations (mot de passe, carte à puce et code d'activation correspondant, bi-clé cryptographique et certificat électronique associé, etc.).

Blog : « journal sur Internet ». Défini souvent comme un site personnel, il s'agit d'un espace individuel d'expression, créé pour donner la parole à tous les internautes.

CNIL : Commission Nationale de l'Informatique et des Libertés, autorité administrative indépendante ayant un rôle d'alerte, de conseil et d'information ainsi qu'un pouvoir de sanction

Cookie : fichier stocké sur le poste qui permet de retracer le parcours d'un utilisateur sur un site web.

Confidentialité : un des critères de sécurité permettant de s'assurer que l'information ne soit accessible qu'aux personnes autorisées à y accéder.

Délégué à la Protection des Données : personne au sein de la Collectivité en charge du contrôle du respect par tous les responsables de traitements et les utilisateurs de la réglementation en matière de protection des données personnelles. Outre le contrôle, il accompagne les responsables de traitement, s'assure de la conformité permanente, fait le lien avec les autorités nationales de contrôle dont la CNIL, et peut être confidentiellement sollicité par les utilisateurs.

Document : lorsqu'il est numérique, un document est une forme de représentation de l'information consultable à l'écran d'un équipement. Cela comprend notamment les courriels, fichiers, vidéos, photographies, etc.

Donnée personnelle ou Donnée à caractère personnel : toute information se rapportant à une personne physique identifiée ou identifiable ; est réputée être une « personne physique identifiable » une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale.

EDR (end point detection and response) : logiciel et service permettant la détection de comportements anormaux des postes informatiques et serveurs, type exfiltration de données, chiffrement de données et permettant d'apporter une réponse, type fin du processus, isolation du poste.

Équipement individuel : tout équipement, mis à disposition par la Collectivité à titre professionnel, fixe ou mobile, permettant à un Utilisateur d'accéder à des systèmes d'information de la Collectivité et/ou de traiter localement sur l'équipement des informations de la Collectivité (ordinateurs fixes, ordinateurs portables, téléphones mobiles, téléphones mobiles intelligents (dits « smartphones »), tablettes tactiles, etc.).

Firewall : aussi appelé « pare-feu ». Serveur qui permet d'assurer la sécurité des informations internes au réseau local en filtrant les entrées et en contrôlant les sorties selon une procédure automatique.

FTP : *File Transfer Protocol* ou Protocole de transfert de fichiers, système permettant l'échange de fichiers sur le réseau Internet.

Habilitation : attribution à un utilisateur de droits d'accès à des ressources par une entité autorisée.

Information : élément de connaissance (donnée, son, image fixe ou animée...) susceptible d'être conservé, traité ou transmis suivant un mode de codification défini et à l'aide d'un support matériel (papier) ou électronique (information dématérialisée).

Intégrité : un des critères de sécurité, garantie de l'exactitude, de la fiabilité et de l'exhaustivité des informations et des méthodes de traitement.

IP : *Internet Protocol* . Une adresse IP est un code numérique qui identifie un ordinateur individuel sur Internet, et par extension son utilisateur.

Log : fichier qui conserve la trace de toutes les requêtes qui ont été adressées à un serveur.

Macro : un terme générique pour désigner un moyen de mémoriser un enchaînement de tâches au sein d'un logiciel.

Mail : aussi appelé « courriel », est un message électronique.

Marquage : opération consistant à apposer de manière visuelle ou non le niveau de classification d'une information sur un support.

Moyens téléphoniques : ensemble composé de tous les téléphones fixes ou portables, les radiotéléphones, les assistants personnels, les fax, modems... mis à disposition par la Collectivité pour l'exercice de l'activité professionnelle.

Moyens informatiques : ensemble composé par les réseaux (filaires, sans fil, ...), les serveurs, les postes de travail (pc fixes et mobiles, macintosh, clients légers ...), les écrans, les logiciels (systèmes d'exploitation (Windows, linux...) bureautiques, métiers...), les moyens d'impression, les supports de stockage externes (disques durs externes, clés USB ...).

Système d'archivage électronique (SAE) : logiciel permettant un archivage électronique des actes originaux, respectant les normes nationales

Services Internet/Intranet : ensemble des moyens d'échanges et d'informations diverses : site web, intranet Léo, messagerie, forum...

Proxy : serveur qui permet de contrôler et d'améliorer l'accès à certaines pages Web en les stockant en cache (ou copie).

Ressource (d'un système d'information) : tout élément intervenant dans la mise en œuvre et le fonctionnement d'un système d'information (informations sous toutes leurs formes, équipements individuels, imprimante, logiciel, serveur de fichiers, base de données, applicatif, équipement réseau, service réseau interne / externe, espace disque, messagerie électronique, etc.).

Spam : aussi appelé « pourriel » ou « courrier indésirable », est un mail non sollicité, en général effectué à des fins publicitaires.

Système d'Information (SI) : ensemble des moyens techniques et Ressources destinés au traitement de l'information.

Système d'information et de communication : ensemble composé des **moyens informatiques**, des **moyens téléphoniques** , plus **généralement**, de tout matériel communiquant mis à disposition par la Collectivité, même utilisé à l'extérieur de la Collectivité (lieux publics, domicile...)et de l'ensemble des informations (appartenant, détenues ou placées sous la responsabilité de la Collectivité), des fichiers, données et bases de données, du système de messagerie électronique, du réseau interne de la collectivité collaboratif ou non (par exemple l'intranet Léo), des abonnements à des services interactifs, des machines virtuelles, des applications Saas ou hébergées, du cloud public/privé, ainsi que de l'ensemble du parc de logiciels.
Pour des raisons de sécurité du réseau, est également considéré comme faisant partie du système d'information et de communication, **le matériel personnel des agents connecté au réseau de la Collectivité, ou contenant des informations à caractère professionnel.**

Département TIC : officiellement dénommé Département Systèmes d'informations, il est composé d'un ensemble de services en charge du développement, de la mise en œuvre technique et du maintien en conditions opérationnelles du Système d'information et de communication. L'usage de l'appellation Département TIC est historique mais reconnu par la majorité des utilisateurs.

TIC : technologies de l'information et de la communication, regroupe les techniques utilisées dans le traitement et la transmission des informations, principalement de l'informatique, de l'internet et des télécommunications.

Tiers : entités ou organismes externes en relation contractuelle avec la Collectivité. Sont ainsi considérés comme des tiers : les prestataires, les intérimaires, les partenaires...

Traçabilité : un des critères de sécurité, traduisant la garantie que les événements et les accès aux Ressources sont enregistrés à travers des traces accessibles et, en cas de besoin, opposables.

Traitement de l'information, traitement de données : élaboration, modification, stockage, échange, diffusion, présentation ou destruction de l'information, quelle que soit la forme sous laquelle est exploitée cette information (électronique, imprimée, manuscrite, vocale, image...).

Utilisateur (d'un système d'information) : toute personne, quel que soit son statut, qui accède à, ou utilise, des systèmes d'information et des informations de la Collectivité, de manière permanente ou occasionnelle. Désigne également les administrateurs, les exploitants et les prestataires externes intervenant sur les SI de la Collectivité.