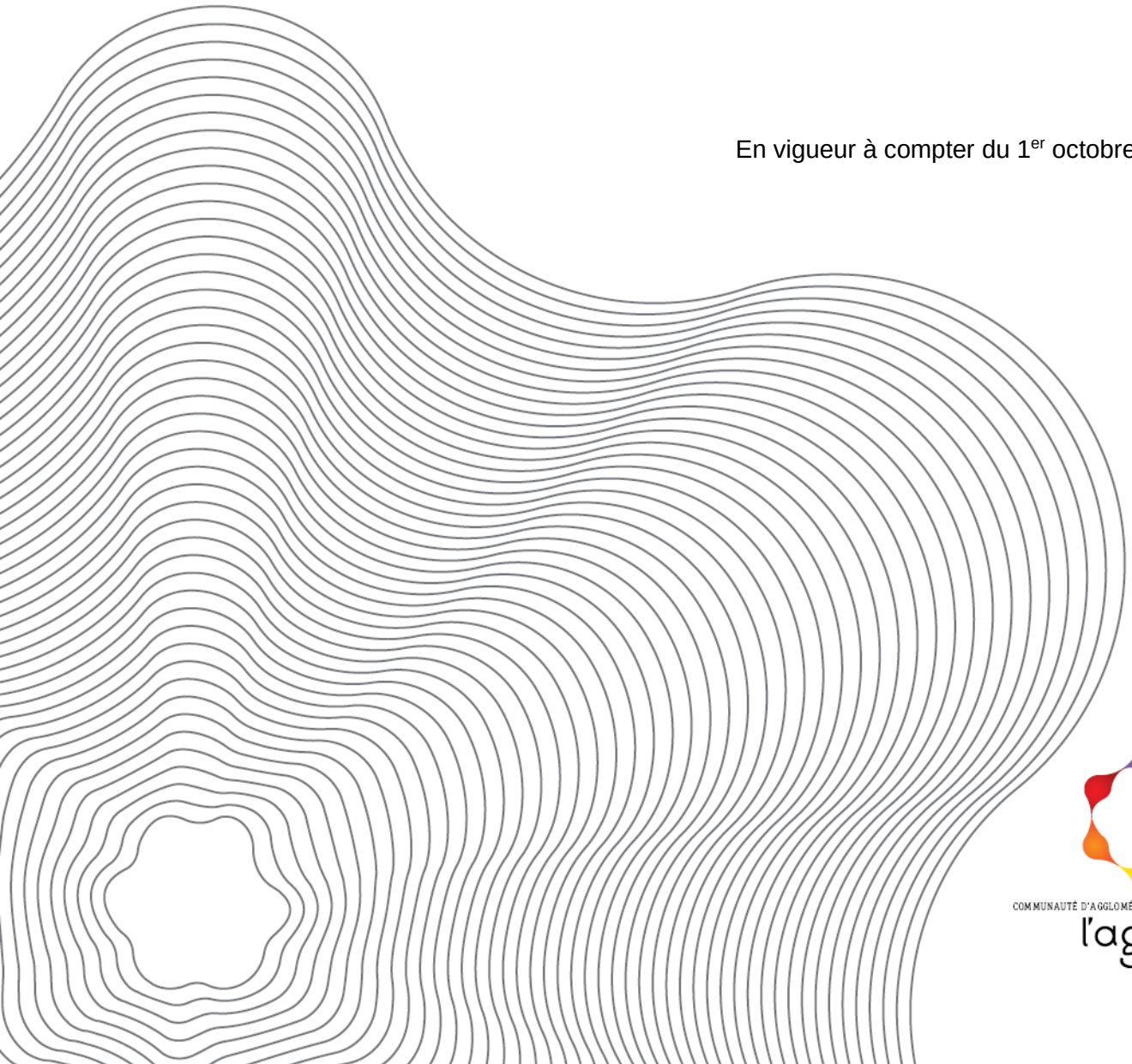
CHARTE D'UTILISATION DES SYSTEMES D'INFORMATION ET DE PROTECTION DES DONNEES PERSONNELLES

En vigueur à compter du 1er octobre 2021



COMMUNAUTÉ D'AGGLOMÉRATION DU CENTRE LITTORAL
l'agglo

Table des matières

INTRODUCTION

La CACL met en œuvre un système d'information et de communication nécessaire à l'exercice de ses missions. Elle met ainsi à disposition de ses collaborateurs des outils informatiques et de communication. La performance des services de la CACL nécessite la mise en place régulière de nouveaux outils pour mieux gérer l'information. Ce déploiement d'équipements doit s'accompagner d'une maîtrise des risques tant sur le plan de la sécurité informatique et technique, que juridique et financier. Des solutions techniques sont mises en œuvre pour diminuer ces risques, mais le comportement des utilisateurs reste prépondérant.

La présente charte définit les **conditions d'accès** et les **règles d'utilisation des moyens informatiques et des ressources extérieures** via les outils de communication de la CACL. Elle a également pour objet de **sensibiliser les utilisateurs aux risques** liés à l'utilisation de ces ressources en termes d'intégrité et de confidentialité des informations traitées. Ces risques imposent le respect de certaines règles de sécurité et de bonne conduite. L'imprudence, la négligence ou la malveillance d'un utilisateur peuvent en effet avoir des conséquences graves de nature à engager sa responsabilité civile et / ou pénale ainsi que celle de la collectivité.

Le « bon usage » des technologies de la communication est un usage responsable, qui fait appel au bon sens, à l'attention et à la prudence. Il s'appuie sur des conseils et des recommandations techniques ou d'usage, et se réfère à des règles de **déontologie professionnelle et personnelle**. En effet, si le « bon usage » avec des règles minimales de courtoisie et de respect d'autrui favorise le bon fonctionnement des outils, un comportement abusif peut avoir des conséquences négatives pour tous.

Le non-respect d'une de ces règles est susceptible d'entraîner des mesures disciplinaires internes voire, en cas de violation d'un texte législatif ou réglementaire, des poursuites judiciaires.

La présente charte est prise en application des textes réglementaires suivants :

- Convention du 28 janvier 1981 du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel.
- Directive européenne 95/46 du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données.
- Directive européenne 97/66 du 15 décembre 1997 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des télécommunications.
- Loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, modifiée par la Loi du 20 juin 2018 relative à la protection des données personnelles.
- Loi du 3 juillet 1985 et loi du 1er juillet 1992 sur la protection des logiciels.
- Loi du 5 janvier 1988 relative à la fraude informatique.
- Loi du 04 août1994 relative à l'emploi de la langue française.
- Loi du 13 juillet 1983 portant droits et obligations des fonctionnaires.
- Règlement (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.

CHAMP D'APPLICATION ET PORTEE DE LA CHARTE

La présente charte s'applique à tout utilisateur du Système d'Information et de communication de la CACL pour l'exercice de ses activités professionnelles. Elle recouvre l'ensemble des moyens informatiques, numériques et de télécommunications. La charte est diffusée à l'ensemble des utilisateurs. Elle est systématiquement remise à tout nouvel arrivant et fait l'objet d'une diffusion auprès des personnes, tierces à la CACL, amenées à utiliser notre système d'information. Des actions de communication internes sont organisées régulièrement afin d'informer les utilisateurs des pratiques recommandées.

Elle fait l'objet d'une consultation des instances représentatives du personnel avant adoption.

Quelques définitions :

On désignera sous le terme « **utilisateur »** toute personne autorisée à accéder aux outils informatiques et aux moyens de communication de la CACL et à les utiliser : employés, stagiaires, intérimaires, personnels de sociétés prestataires, visiteurs occasionnels....

Le terme « **TIC »** (Technologies de l'Information et de la Communication) désigne l'ensemble des moyens informatiques, téléphoniques et reprographiques de la CACL. Elles regroupent les matériels tels que les ordinateurs fixes ou portables, tous les autres matériels informatiques, connectiques ou bureautiques comme les serveurs, téléphones, fax, photocopieurs, câbles de réseaux. Les TIC intègrent également les logiciels et les fichiers ou bases de données…

Le terme « **système d'Information »** désigne l'ensemble des éléments qui contribuent au traitement et à la circulation de l'information dans la Collectivité (base de données, logiciels d'application, procédures, …) et du système informatique (serveur, périphériques, imprimantes, copieurs multifonction, système d'exploitation, …).

L'abréviation « **DINSI** » désigne la Direction de l'Innovation Numérique et des Systèmes d'Information.

Le terme « **donnée à caractère personnel** » désigne l'ensemble des informations relatives aux personnes physiques, directement ou indirectement identifiées. Une personne est identifiée ou identifiable dans un fichier dès lors que figurent dans ce dernier des informations permettant directement ou indirectement son identification.

Le terme « **traitement de données à caractère personnel** » désigne l'ensemble des opérations portant sur des données à caractère personnel, quel que soit le procédé utilisé (collecte, enregistrement, transfert, consultation, conservation, modification, diffusion, rapprochement…).

Le terme « **DPO (DPD)** » désigne le délégué à la protection des données, en charge de veiller au respect, par l'établissement et ses collaborateurs, de la règlementation sur la protection des données.

REGLES D'UTILISATION DU SYSTEME D'INFORMATION

Chaque utilisateur accède aux TIC nécessaires à l'exercice de son activité professionnelle dans les conditions définies par la CACL.

a) Les modalités d'intervention de la DINSI

La DINSI assure le bon fonctionnement et la sécurité des réseaux ainsi que des moyens informatiques et de communication de la CACL. Les agents/personnels de cette direction disposent d'outils techniques afin de procéder aux investigations et au contrôle de l'utilisation des systèmes informatiques mis en place.
Ils ont accès à l'ensemble des données techniques mais s'engagent à respecter les règles de confidentialité applicables aux contenus des documents.
Ils sont assujettis au devoir de réserve et sont tenus de préserver la confidentialité des données qu'ils sont amenés à connaître dans le cadre de leurs fonctions.

b) Les modalités de saisine de la DINSI

La **DINSI doit impérativement être saisie** dans les cas suivants :

- En cas d'activités suspectes relatives aux moyens mis à disposition (messageries, logiciels, équipements...) ;
- En cas de souhait d'utilisation de nouveaux matériels, programmes et logiciels ;
- En cas de perte ou de vol d'équipements professionnels ;
- En cas de demande d'habilitation aux différents outils,
- Pour formuler une demande de matériels (doivent être saisies dans le formulaire sur SharePoint).

c) L'authentification

L'accès au système d'information repose sur l'utilisation d'un nom de compte ("login" ou identifiant) fourni à l'utilisateur lors de son arrivée à/chez la CACL. Cet identifiant de connexion est composé du prénom de l'utilisateur ainsi que de la première voire seconde lettre du nom (ex : martin-d). Un mot de passe est associé à cet identifiant de connexion.

Les moyens d'authentification sont **personnels et confidentiels**.

Le mot de passe doit être composé de 8 caractères minimum combinant 3 types de caractères parmi les catégories : majuscules, minuscules, chiffres, et caractères non alphabétiques (ex : !, $, #, %). Il ne peut pas contenir le nom de compte de l'utilisateur ou des parties du nom de l'utilisateur comptant plus de deux caractères successifs.
Des moyens mnémotechniques permettent de créer des mots de passe complexe, par exemple :

- En ne conservant que les premières lettres des mots d'une phrase ;
- En mettant une majuscule si le mot est un nom (ex : Chef) ;
- En gardant des signes de ponctuation (ex : ') ;
- En exprimant les nombres à l'aide des chiffres de 0 à 9 (ex : Un 1) ;
- En utilisant la phonétique (ex : acheté ht).

Exemple, la phrase « un Chef d'Entreprise averti en vaut deux » peut correspondre au mot de passe : 1Cd'Eaev2.
Le mot de passe fait l'objet d'un renouvellement tous les 6 mois. Les utilisateurs doivent procéder à cette modification dès que la nécessité de renouvellement leur est notifiée. A défaut, ils s'exposent au risque de ne pouvoir accéder à leur équipement.

d) L'habilitation

L'accès au SI et aux différents outils de communication mis en place par la CACL est soumis à une politique d'habilitation associant des droits accordés en fonction d'un profil d'utilisateur (fonction occupée). Cette politique est définie et gérée par la DINSI en lien avec les services concernés. Ces profils d'habilitation permettent de garantir que les utilisateurs ont accès aux seules données strictement nécessaires à l'accomplissement de leurs missions.

Les **comptes nominatifs** et les **autorisations** délivrés sont **strictement personnels** et ne peuvent en aucun cas être cédés, même temporairement, à un tiers. Ces droits d'accès prennent fin lors de la cessation même provisoire de l'activité professionnelle.
Pour des raisons de sécurité, la DINSI doit être informée en amont, par la hiérarchie, de tout changement (départ, arrivée, personnel temporaire ...) afin de procéder à la suppression / création / suspension des comptes utilisateurs correspondants.
Les TIC sont mises à la disposition des agents dans le cadre de leurs fonctions et des missions qu'ils exercent. Elles sont affectées à un poste et non attribuées à un agent.

e) Les règles de sécurité

Tout utilisateur s'engage à **respecter les règles de sécurité** suivantes :

- Signaler toute violation ou tentative de violation suspectée de son compte réseau et de manière générale tout dysfonctionnement.
- Signaler toute perte ou vol de support (clef USB, téléphone, ordinateur …) dès constatation de la perte ou du vol.
- Ne jamais confier son identifiant/mot de passe.
- Ne jamais demander son identifiant/mot de passe à un collègue ou à un collaborateur ou communiquer son identifiant/mot de passe à un collègue, un collaborateur ou à tiers à la CACL
- Aucun agent de la DINSI n'est amené à demander les mots de passe des utilisateurs.
- Ne jamais enregistrer le mot de passe d'un outil professionnel dans le navigateur.
- Ne pas masquer sa véritable identité.
- Ne pas usurper l'identité d'autrui.
- Ne pas modifier les paramétrages du poste de travail.
- Ne pas installer de logiciels sans autorisation.
- Ne pas copier, modifier, détruire les logiciels propriétés de la CACL.
- Verrouiller son ordinateur dès qu'il quitte son poste de travail.
- Ne pas accéder, tenter d'accéder, supprimer ou modifier des informations qui ne lui appartiennent pas.

Toute **copie de données sur un support externe** est **soumise à l'accord du supérieur hiérarchique** et doit **respecter les règles** définies par la CACL. En outre, il convient de rappeler que les visiteurs ne peuvent avoir accès au Système d'Information de la CACL sans l'accord préalable de la DINSI.

Les intervenants extérieurs doivent s'engager à faire respecter la présente charte par leurs propres salariés et éventuelles entreprises sous-traitantes. Dès lors, les contrats signés entre la CACL et tout tiers ayant accès aux données, aux programmes informatiques ou autres moyens, doivent comporter une clause rappelant cette obligation.

LES MOYENS INFORMATIQUES

Les moyens informatiques et de télécommunication nécessaires au fonctionnement de la collectivité, qu'ils soient matériels ou logiciels, sont mis en œuvre ou approuvés par la DINSI. Pour des raisons évidentes de sécurité, d'optimisation, de compatibilité et de respect des réglementations, **aucune acquisition ou installation n'est autorisée sans l'aval de la DINSI**.

a) Configuration du poste de travail

La CACL met à disposition de chaque utilisateur un poste de travail doté des outils informatiques nécessaires à l'accomplissement de ses fonctions. L'utilisateur ne doit pas :

- Modifier ces équipements et leur fonctionnement, leur paramétrage, ainsi que leur configuration physique ou logicielle.
- Connecter ou déconnecter du réseau les outils informatiques et de communications sans y avoir été autorisé par l'équipe informatique.
- Nuire au fonctionnement des outils informatiques et de communications.

Toute installation de logiciels supplémentaires est subordonnée à l'accord de la DINSI.

b) Equipements nomades et procédures spécifiques aux matériels de prêt

Equipements nomades

On entend par « **équipements nomades** » tous les moyens techniques mobiles (ordinateur portable, tablette, téléphone mobile, clé USB etc..).

Quand cela est techniquement possible, ils doivent faire l'objet d'une sécurisation particulière, au regard de la sensibilité des documents qu'ils peuvent stocker, notamment par chiffrement.

En particulier, la copie sur support amovible de fichiers contenants des données à caractère personnel n'est autorisée que sur un support pourvu d'un dispositif de cryptage mis à disposition par La DINSI et doit être limité au strict nécessaire.

L'utilisation de smartphones pour relever automatiquement la messagerie électronique comporte des risques particuliers pour la confidentialité des messages, notamment en cas de perte ou de vol de ces équipements. Ils doivent donc être verrouillés par un moyen adapté de manière à prévenir tout accès non autorisé aux données qu'ils contiennent.

Procédures spécifiques aux matériels de prêt

L'utilisateur doit renseigner et signer un registre, tenu par la DINSI, actant la remise de l'équipement nomade ou encore la mise à disposition d'un matériel spécifique pour la tenue d'une réunion (Vidéoprojecteur). Il en assure la garde et la responsabilité et doit informer la DINSI en cas d'incident (perte, vol, dégradation) et procéder aux démarches telles que la déclaration de vol ou de plainte. Il est garant de la sécurité des équipements qui lui sont remis et ne doit pas contourner la politique de sécurité mise en place sur ces mêmes équipements.

Le retour du matériel est consigné dans le registre.

c) Internet

Les utilisateurs peuvent consulter les sites internet présentant un lien direct et nécessaire avec l'activité professionnelle, de quelque nature qu'ils soient.

Toutefois, une utilisation ponctuelle et raisonnable, pour un motif personnel, des sites internet dont le contenu n'est pas contraire à la loi et à l'ordre public, ne met pas en cause l'intérêt et la réputation de l'institution et ne porte pas atteinte au bon fonctionnement du réseau est admise.

Sont notamment proscrits et le cas échéant, sanctionnés :

- La consultation ou le téléchargement de données ayant un caractère illégal (par exemple, pédophilie, incitation à la haine raciale, trafic de stupéfiants…);

- La consultation ou le téléchargement de données ayant un caractère explicitement indécent, contraire à l'ordre public, portant atteinte à la dignité ou à la vie privée (par exemple, pornographie) ;
- Le téléchargement ou l'exploitation, de tout ou partie des données numériques soumises au droit d'auteur ou à la loi des copyrights sans autorisation et sans mention des crédits en cas de publication ;
- L'utilisation professionnelle, sauf autorisation en ce sens de la direction générale des services, des plateformes non homologuées par la collectivité (par exemple, Google Forms ou Facebook).

d) Messagerie électronique

Conditions d'utilisation
La messagerie mise à disposition des utilisateurs est destinée à un usage professionnel. L'utilisation de la messagerie à des fins personnelles est tolérée si elle n'affecte pas le travail de l'agent ni la sécurité du réseau informatique de la CACL.
Tout message qui comportera la mention expresse ou manifeste de son caractère personnel bénéficiera du droit au respect de la vie privée et du secret des correspondances. A défaut, le message est présumé professionnel.
La CACL s'interdit d'accéder aux dossiers et aux messages identifiés comme « personnel » dans l'objet de la messagerie de l'agent.
Le transfert de messages, ainsi que leurs pièces jointes, à caractère professionnel sur des messageries personnelles est soumis aux mêmes règles que les copies de données sur supports externes.
L'installation du compte de messagerie sur un client de type Outlook est interdite sur un ordinateur personnel. En revanche, les agents peuvent consulter leur messagerie à distance, depuis n'importe quel poste informatique, à l'aide d'un navigateur (Webmail). Les fichiers qui seraient copiés sur l'ordinateur utilisé par l'agent dans ce cadre doivent être effacés dès que possible de l'ordinateur utilisé.
Il est enfin rappelé que dans la mesure où une boite e-mail professionnelle est mise à disposition des collaborateurs par la CACL, l'utilisation de la messagerie électronique personnelle est à proscrire dans le cadre professionnel conformément aux obligations règlementaires notamment en matière de sécurité des données.

Consultation de la messagerie
En cas d'absence d'un agent et afin de ne pas interrompre le fonctionnement du service, la DINSI peut, ponctuellement transmettre au supérieur hiérarchique un message électronique à caractère exclusivement professionnel et identifié comme tel par son objet et/ou son expéditeur (cf. conditions d'utilisation).
Le supérieur hiérarchique n'a pas accès aux autres messages de l'agent. L'agent concerné est informé dès que possible de la liste des messages qui ont été transférés.
En cas d'absence prolongée d'un agent (longue maladie), le chef de service peut demander à la DINSI, après accord de son directeur, le transfert des messages reçus.

Modération de la messagerie
La CACL met en place un mécanisme de modération par lequel les courriels envoyés par les collaborateurs aux listes de diffusion générale ("Agents", "Elus"…) font l'objet d'une approbation avant d'être envoyés aux destinataires concernés. Ce mécanisme peut le cas échéant être étendu à d'autres listes de diffusion en fonction des contraintes règlementaires.

Cette modération poursuit plusieurs objectifs :

- Prévenir l'envoi de données personnelles en nombre à des destinataires autorisés et ainsi, le risque de violation de données personnelles conformément aux exigences légales ;
- Veiller à ce que les destinataires soient bien le public adéquat pour le message à transmettre ;
- S'assurer que le message est cohérent, approprié et complet dans un souci de clarté et de pertinence de l'information.

Cette modération est assurée par la direction générale des services, après relecture de la déléguée à la protection des données. En cas d'interrogations sur le contenu du courriel, le collaborateur à l'origine est recontacté afin d'apporter un complément d'information, de rectifier une erreur avant envoi définitif ou d'être réorienté vers l'interlocuteur adéquat.

Ces **mesures de modération** sont **strictement réservées à cette hypothèse** et ne sauraient entraver les communications entre les collaborateurs et élus.

Courriel non sollicité
La CACL dispose d'un outil permettant de lutter contre la propagation des messages non désirés (spam). Aussi, afin de ne pas accentuer davantage l'encombrement du réseau lié à ce phénomène, les utilisateurs sont invités à limiter leur consentement explicite préalable à recevoir un message de type commercial, newsletter, abonnements ou autres, et de ne s'abonner qu'à un nombre limité de listes de diffusion notamment si elles ne relèvent pas du cadre strictement professionnel.

e) Messageries instantanées

La CACL met à disposition des utilisateurs, *via* **Microsoft Teams**, une messagerie instantanée. Cette messagerie est particulièrement appropriée aux échanges de messages simples et courts dont la teneur et le formalisme ne justifient pas l'utilisation de la messagerie classique. Les mêmes règles d'usage que pour la messagerie électronique s'appliquent notamment s'agissant de l'utilisation à des fins exclusivement professionnelles sauf exceptions mesurées.
Cette messagerie permet de connaitre la disponibilité d'une personne que l'on souhaite contacter, d'initier une conversation instantanée par vidéo, audio ou texte entre deux ou plusieurs utilisateurs et de partager en temps réel des ressources informatiques. Cette application est également disponible sur les téléphones professionnels.

Par ailleurs, les collaborateurs dotés d'un portable professionnel peuvent éventuellement disposer de l'application **WhatsApp**, service de messagerie instantanée. L'usage de cet outil est strictement limité à des échanges professionnels instantanés et informels afin de partager des **informations non confidentielles**. En aucun cas, les collaborateurs ne sont autorisés à échanger des données à caractère personnel, à gérer des dossiers personnels de collaborateurs ou d'usagers, par le biais de cette application ou à échanger des données professionnelles de la collectivité (par exemple, notes internes, documents de travail, données financières…).

Chaque agent et élu de la CACL dispose d'un accès à la messagerie instantanée Microsoft Teams, ce qui n'est pas le cas de WhatsApp. Par conséquent, **Microsoft Teams** constitue le **moyen officiel de messagerie instantanée de la CACL** et doit être **privilégié** par l'ensemble des collaborateurs. Si l'utilisation de WhatsApp est tolérée, cette application n'est pas considérée comme une composante du Système d'Information de la CACL.

f) Outil de visioconférence

La CACL met à disposition des utilisateurs, pour l'exercice de leur activité professionnelle, un outil de visioconférence permettant d'organiser et de participer à des réunions avec un ou plusieurs utilisateurs – internes ou externes à la CACL – de manière dématérialisée.

Tout **enregistrement** des réunions, de l'image ou du contenu des conversations doit être **soumis à l'accord préalable des utilisateurs concernés**. Il appartient à l'organisateur de la réunion de solliciter cet accord, d'informer les personnes sur le traitement, de procéder à cet enregistrement et de gérer l'accès à cet enregistrement par les personnes qui ont à en connaitre le contenu.

g) Téléphone/ Tablette

La CACL met à disposition des utilisateurs, pour l'exercice de leur activité professionnelle, des téléphones fixes et mobiles et des tablettes le cas échéant.
L'utilisation du téléphone à titre privé est admise à condition qu'elle demeure raisonnable.
Des restrictions d'utilisation par les agents des téléphones fixes sont mises en place en tenant compte de leurs missions. A titre d'exemple, certains postes sont limités aux appels nationaux, d'autres peuvent passer des appels internationaux.

La DINSI s'interdit d'accéder au suivi individuel de l'utilisation des services de télécommunications et d'accéder à l'intégralité des numéros appelés via l'autocommutateur mis en place et via les téléphones mobiles. Toutefois, en cas d'utilisation manifestement anormale, la DINSI sur demande de la Direction Générale, se réserve le droit d'accéder au suivi individuel et aux numéros complets des relevés individuels.

Management des Devices Mobiles (MDM)
Le MDM constitue un outil de gestion de la flotte mobile. Il permet de maintenir les téléphones mobiles et tablettes en état de marche et d'assurer à distance leurs mises à jour ainsi que l'installation de nouvelles applications.
Il permet d'assurer la sécurité de ces équipements et des données qui y transitent comme nous l'impose la règlementation. Notamment, le MDM permet de localiser à un instant précis le support de stockage et d'accès aux données, de le verrouiller et de supprimer les données qui y figurent. Les fonctionnalités de verrouillage et d'effacement des données ne sont utilisées par la DINSI, dans le cadre de la conformité au RGPD, qu'en cas de vol et/ou de perte des équipements. La fonctionnalité de géolocalisation n'est mise en œuvre par la DINSI qu'en cas de vol et/ou de perte des équipements et uniquement sur demande de l'utilisateur ou de l'autorité territoriale.

Par ailleurs, l'accès à cet outil est réservé aux seules personnes strictement habilitées au sein de la DINSI à accéder à ces données. Il ne peut, en aucun cas, être un outil à la disposition des managers pour gérer leurs équipes.

h) Utilisation des outils informatiques par les organisations syndicales

La CACL peut autoriser l'accès et l'utilisation de ses systèmes d'information aux organisations syndicales. Un protocole d'accord entre la CACL et les organisations syndicales détermine les conditions et modalités précises de cet accès.

i) Accès depuis l'extérieur – Service VPN

La DINSI a mis en place un service VPN permettant l'accès au réseau et aux outils de travail numériques de la CACL depuis l'extérieur.
L'accès au VPN est réservé exclusivement aux ordinateurs portables gérés par la DINSI et n'est accordé que sur une demande justifiée, validée le cas échant par le chef de service et le directeur dont dépend le demandeur, et dont la DINSI évaluera la pertinence.
L'accès au VPN est personnel. Il est accordé à un utilisateur qui s'engage à en faire un usage strictement professionnel et à ne pas partager son accès avec d'autres personnes.
Les utilisateurs du VPN acceptent que leur activité sur le VPN soit journalisée, conformément à la réglementation en vigueur.

j) Utilisation de dispositifs personnels

Sur le site de la CACL, l'utilisation de dispositifs personnels n'est pas autorisée. Ainsi, les ordinateurs personnels, les clés USB ou disques durs ne peuvent être utilisés à des fins professionnelles.

En cas de besoin de récupérer sur un autre support des données professionnelles (par exemple, clé USB remise par un prestataire, disque dur remis par un partenaire), il convient de se rapprocher de la DINSI afin de procéder au transfert de données de manière sécurisée.

k) Utilisation de nouveaux matériels, programmes et logiciels

L'utilisateur n'est en aucun cas habilité à installer des logiciels, programmes ou nouveaux équipements au sein du système d'information de la CACL. En cas de souhait d'un nouveau logiciel, programme ou équipement, l'utilisateur est invité à saisir la DINSI par l'intermédiaire du formulaire de demande disponible sur l'intranet.

l) Partage de données en interne et en externe

SHAREPOINT
Un intranet, géré sous SharePoint, est mis à disposition des agents de la CACL. Il permet le stockage et le partage des données exploitées dans le cadre de leurs missions. Ces données peuvent être accessibles par des tiers externes à la collectivité.

Chaque agent a un espace dédié, et des espaces en partage selon les groupes de travail auxquels il appartient. L'agent doit **favoriser l'utilisation du SharePoint** pour les documents et dossiers qui appellent un **travail collaboratif** ou qui doivent être accessibles à plusieurs personnes ou à l'ensemble d'un service.

ONEDRIVE
L'attribution d'une licence Office attribue aux agents concernés un accès à un cloud personnalisé, OneDrive. C'est un espace de stockage en ligne d'une capacité d'un tera octets (1 To), accessible *via* internet.

Il permet également le partage d'informations, aussi bien en interne qu'en externe. L'agent doit réserver l'utilisation du OneDrive aux documents ou dossiers qui n'ont pas vocation à être rendus accessibles à un ensemble de collaborateurs.

ADMINISTRATION DU SYSTEME D'INFORMATION

Afin de surveiller le fonctionnement et de garantir la sécurité du système d'information de la CACL, différents dispositifs sont mis en place. Ils visent en priorité à maintenir une qualité de service en contrôlant le bon fonctionnement des équipements, la disponibilité du Système d'Information mais également le respect des règles de « bon usage » et ceci dans le cadre de la législation applicable et notamment de la loi sur l'informatique et les libertés.

Les agents de la DINSI sont responsables de la supervision technique des systèmes. Les responsables hiérarchiques seront informés en cas de manquements graves résultant du non-respect de cette charte et il est de leur devoir d'intervenir.

a) Les systèmes automatiques de filtrage

A titre préventif, des systèmes automatiques de filtrage permettant de diminuer les flux d'information pour la CACL et d'assurer la sécurité et la confidentialité des données sont mis en œuvre. Il s'agit notamment du filtrage des sites Internet, de l'élimination des courriels non sollicités, du blocage de certains protocoles.

Le filtrage des sites internet mis en place prévoit le blocage des catégories de sites suivantes : Substances illicites, piratage informatique, activités illégales, discrimination, violence explicite, groupes extrémistes, pornographie et pédo pornographie, vente d'armes, d'alcool, tabagisme, site de téléchargements illégaux, sites de phishing.

b) Les systèmes automatiques de traçabilité

La DINSI opère sans avertissement les investigations pour donner suite à la constatation d'une anomalie (alerte de sécurité, ralentissements, sollicitation anormale de la bande passante …) ou nécessaires à la résolution de dysfonctionnements du système d'information ou de l'une de ses composantes, qui mettent en péril son fonctionnement ou son intégrité.

Elle s'appuie pour ce faire, sur des fichiers de journalisation qui recensent toutes les connexions et tentatives de connexions au et depuis le système d'information. Ainsi, L'ensemble des connexions entrantes et sortantes sont journalisées, conformément à la législation en vigueur.

Ces fichiers peuvent comporter les données suivantes : dates, postes de travail, objet de l'évènement, durée de connexion, volume de données échangés, sites web consultés, fichier partagé ouvert ou modifié.

La DINSI est le seul utilisateur de ces informations qui sont effacées à l'expiration d'un délai d'un an conformément à la réglementation.

c) Gestion du poste de travail

A des fins de maintenance informatique, la DINSI peut accéder à distance à l'ensemble des postes de travail. Cette intervention s'effectue avec l'autorisation expresse de l'utilisateur, sauf circonstances exceptionnelles empêchant de solliciter cette autorisation.

Dans le cadre de mises à jour et évolutions du système d'information, et lorsqu'aucun utilisateur n'est connecté sur son poste de travail, la DINSI peut être amenée à intervenir sur l'environnement technique des postes de travail. Il s'interdit d'accéder aux contenus identifiés comme personnels.

PROCEDURE APPLICABLE LORS DU DEPART DE L'UTILISATEUR

Lors de son départ, l'utilisateur doit restituer à la DINSI les matériels mis à sa disposition.
Il doit préalablement effacer ses fichiers et données privées. Toute copie de documents professionnels doit être autorisée par le supérieur hiérarchique.

A l'exception des contenus privés produits et reçus par les utilisateurs, les documents et messages électroniques, reçus ou produits dans le cadre de l'activité professionnelle des utilisateurs au sein de la collectivité, constituent des archives publiques au sens du code du patrimoine (article L.211-1 du code du patrimoine). Par conséquent, ces données professionnelles doivent être conservées.

Les documents identifiés comme "personnel" par l'utilisateur sont, en tout état de cause, supprimés à son départ, et son compte désactivé.

PROTECTION DES DONNEES A CARACTERE PERSONNEL

a) Mise en œuvre ou modification d'un traitement de données à caractère personnel

Toute constitution ou modification de traitement de données à caractère personnel doit faire l'objet, préalablement à sa mise en œuvre, d'une consultation du délégué à la protection des données (DPO) et d'une saisine de la DINSI lorsqu'il s'agit d'acquérir un nouvel outil ou de faire un usage différent d'un outil déjà existant. Aucun traitement ne saurait être mis en œuvre sans consultation préalable du DPO quant à sa conformité à la réglementation. Une fiche d'instruction à compléter par le service en charge de la mise en œuvre du traitement est disponible sur l'intranet. Elle doit être envoyée au DPO en vue de l'analyse du traitement à mettre en œuvre. Les agents tiennent à disposition du DPO les informations nécessaires à cette analyse.

Le DPO formule un avis quant à la conformité du traitement envisagé ainsi que des recommandations à destination des services. Le registre des activités de traitement est mis à jour par le DPO en cas de mise en place ou de modification d'un traitement de données à caractère personnel.

b) Notification des violations de données à caractère personnel

Conformément à la règlementation en vigueur, la CACL doit notifier à la Commission nationale de l'informatique et des libertés (CNIL) – et aux personnes concernées le cas échéant -, toute violation de données personnelles survenue pour un traitement dont elle est responsable. Ainsi, à cet effet, l'agent qui a connaissance d'une violation de données doit en informer, sans tarder, le délégué à la protection des données et la DINSI lorsque le système d'information de la CACL est concerné par la violation. Il tient à leur disposition les informations nécessaires à l'analyse de la violation. Une procédure et une fiche sont disponibles à cet effet sur l'intranet.

Une violation de données est constituée par tout incident de sécurité, d'origine malveillante ou non et se produisant de manière intentionnelle ou non, ayant comme conséquence de compromettre l'intégrité, la confidentialité ou la disponibilité de données personnelles (par exemple, suppression accidentelle de données, perte d'une clé USB non sécurisée contenant des données, erreur de destinataire d'un courriel contenant des données personnelles, vol d'un téléphone portable professionnel…).

Le délégué à la protection des données est chargé, en lien avec la DINSI, de mener les investigations nécessaires et d'effectuer les recommandations qui s'imposent eu égard aux conséquences avérées et/ou prévisibles de cette violation.

RESPONSABILITES- SANCTIONS

Le manquement aux règles et mesures définies par la présente charte est susceptible d'engager la responsabilité de l'utilisateur et d'entraîner des sanctions à son encontre.

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

ENTREE EN VIGUEUR DE LA CHARTE

La présente charte a été adoptée après information et consultation du Comité Technique.
Elle est applicable à compter du **1er octobre 2021.**

ANNEXE 1 – ENGAGEMENT DE CONFIDENTIALITE

Je soussigné/e Monsieur/Madame ……..,exerçant les fonctions

de : ……..

au sein de la Communauté d'Agglomération du Centre Littoral étant à ce titre amené/e à accéder à des données à caractère personnel, déclare reconnaître la confidentialité desdites données.

Je m'engage par conséquent, conformément aux articles 121 et 122 de la loi du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés ainsi qu'aux articles 32 à 35 du règlement général sur la protection des données du 27 avril 2016, à prendre toutes précautions conformes aux usages et à l'état de l'art dans le cadre de mes attributions afin de protéger la confidentialité des informations aux- quelles j'ai accès, et en particulier d'empêcher qu'elles ne soient communiquées à des personnes non expressément autorisées à recevoir ces informations.

Je m'engage en particulier à :

- ne pas utiliser les données auxquelles je peux accéder à des fins autres que celles prévues par mes attributions ;
- ne divulguer ces données qu'aux personnes dûment autorisées, en raison de leurs fonctions, à en recevoir communication, qu'il s'agisse de personnes privées, publiques, physiques ou morales ;
- ne faire aucune copie de ces données sauf à ce que cela soit nécessaire à l'exécution de mes fonctions ;
- prendre toutes les mesures conformes aux usages et à l'état de l'art dans le cadre de mes attributions afin d'éviter l'utilisation détournée ou frauduleuse de ces données ;
- prendre toutes précautions conformes aux usages et à l'état de l'art pour préserver la sécurité physique et logique de ces données ;
- m'assurer, dans la limite de mes attributions, que seuls des moyens de communication sécurisés seront utilisés pour transférer ces données ;
- en cas de cessation de mes fonctions, restituer intégralement les données, fichiers informatiques et tout support d'information relatif à ces données.

Cet engagement de confidentialité, en vigueur pendant toute la durée de mes fonctions, demeurera effectif, sans limitation de durée après la cessation de mes fonctions, quelle qu'en soit la cause, dès lors que cet engagement concerne l'utilisation et la communication de données à caractère personnel.

J'ai été informé que toute violation du présent engagement m'expose à des sanctions disciplinaires et pénales conformément à la réglementation en vigueur, notamment au regard des articles 226-16 à 226-24 du code pénal.

Fait à Matoury, le……., en 2 exemplaires

Nom : ……Signature :

ANNEXE 2 – LISTE DES OUTILS ET APPLICATIONS MIS A DISPOSITION

Logiciels Métiers :

- Sedit RH : Gestion des ressources humaines
- Sedit GF : Gestion financière
- Bodet – Kelio : Gestion du temps de travail
- Légimarchés : Rédaction des marchés publics
- Marchés sécurisés : Gestion de la dématérialisation des marchés publics
- Ubitransport (2Place) : Gestion des lignes de transport urbain et interurbain
- OFA : appli web pour la fiscalité
- SOLEA : appli web pour la fiscalité
- Optinet : plateforme de gestion des bacs de collectes
-

Logiciels de productivité :

- Suite Microsoft Office 365 (Word, Excel, Outlook, PowerPoint, Publisher, Planner, Forms, FindTime…)
- ADOBE CC
- Gespage
- Post-Office : Gestion du courrier
- BL Scan : Enregistrement du courrier
- Chorus pro : plateforme de dématérialisation des factures
- Suite Docapost (I-parapheur, signature OTP, fast élus)

Applications de communication :

- Teams : Messagerie instantanée, visioconférence