DELIBERATION N° DRH/2025/175

1.4

Accusé de réception de la préfecture : 059-225900018-20250630-333910-DE-1-1
Date de réception en préfecture le 10 juillet 2025
Publié le 11 juillet 2025

Suite à la convocation en date du 16 juin 2025
LA COMMISSION PERMANENTE DU CONSEIL DEPARTEMENTAL
Réunie à Lille le 30 JUIN 2025

Sous la présidence de Christian POIRET, Président du Conseil Départemental

Nombre de membres en exercices : 82

Etaient présents : Salim ACHIBA, Charles BEAUCHAMP, Valentin BELLEVAL, Pierre-Michel BERNARD, Stéphanie BOCQUET, Anne-Sophie BOISSEAUX, Frédéric BRICOUT, François-Xavier CADART, Olivier CAREMELLE, Yannick CAREMELLE, Loïc CATHELAIN, Régis CAUCHE, Marie CHAMPAULT, Sylvie CLERC, Barbara COEVOET, Valérie CONSEIL, Frédéric DELANNOY, Sylvie DELRUE, Agnès DENYS, Béatrice DESCAMPS-MARQUILLY, Jean-Luc DETAVERNIER, Stéphane DIEUSAERT, Marie-Laurence FAUCHILLE, Isabelle FERNANDEZ, Michelle GREAUME, Maël GUIZIOU, Mickaël HIRAUX, Eric LAVALLEE, Nicolas LEBLANC, Sébastien LEPRETRE, Maryline LUCAS, Didier MANIER, Françoise MARTIN, Anne MIKOLAJCZAK, Luc MONNET, Laurent PERIN, Max-André PICK, Michel PLOUY, Christian POIRET, Eric RENAUD, Céline SCAVENNEC, Sébastien SEGUIN, Patrick VALOIS, Aude VAN CAUWENBERGE, Karima ZOUGGAGH.

Absent(e)(s) représenté(e)(s) : Martine ARLABOSSE donne pouvoir à Anne-Sophie BOISSEAUX, Grégory BARTHOLOMEUS donne pouvoir à Didier MANIER, Doriane BECUE donne pouvoir à Salim ACHIBA, Josyane BRIDOUX donne pouvoir à Françoise MARTIN, Benjamin CAILLIERET donne pouvoir à Olivier CAREMELLE, Isabelle CHOAIN donne pouvoir à Maryline LUCAS, Marie CIETERS donne pouvoir à Marie CHAMPAULT, Laurent DEGALLAIX donne pouvoir à Frédéric BRICOUT, Carole DEVOS donne pouvoir à Mickaël HIRAUX, Jean-Claude DULIEU donne pouvoir à Eric LAVALLEE, Monique EVRARD donne pouvoir à Valentin BELLEVAL, Soraya FAHEM donne pouvoir à Valérie CONSEIL, Sylvie LABADENS donne pouvoir à Jean-Luc DETAVERNIER, Vincent LEDOUX donne pouvoir à Régis CAUCHE, Michel LEFEBVRE donne pouvoir à Charles BEAUCHAMP, Valérie LETARD donne pouvoir à Karima ZOUGGAGH, Elisabeth MASSE donne pouvoir à Loïc CATHELAIN, Charlotte PARMENTIER-LECOCQ donne pouvoir à Luc MONNET, Marie-Paule ROUSSELLE donne pouvoir à Nicolas LEBLANC, Caroline SANCHEZ donne pouvoir à Christian POIRET, Marie SANDRA donne pouvoir à Stéphane DIEUSAERT, Frédérique SEELS donne pouvoir à François-Xavier CADART, Marie TONNERRE-DESMET donne pouvoir à Barbara COEVOET, Anne VANPEENE donne pouvoir à Patrick VALOIS, Jean-Noël VERFAILLIE donne pouvoir à Béatrice DESCAMPS-MARQUILLY, Philippe WAYMEL donne pouvoir à Sylvie CLERC, Isabelle ZAWIEJA-DENIZON donne pouvoir à Agnès DENYS.

Absent(e)(s) excusé(e)(s) : Paul CHRISTOPHE, Christine DECODTS, Claudine DEROEUX, Marie-Hélène QUATREBOEUFS.

Absent(e)(s) : Barbara BAILLEUL, Jean-Luc DARCOURT, Jacques HOUSSIN, Simon JAMELIN, Bertrand RINGOT, Nicolas SIEGLER.

<u>OBJET</u> : Actualisation de la convention entre l'association NORSENIORS et le Département du Nord.

Vu le rapport DRH/2025/175

DECIDE à l'unanimité:

- d'autoriser l'association NORSENIORS à mener conformément à ses statuts et dans le respect des termes de la convention ci-jointe en annexe toutes actions destinées à améliorer la qualité de vie des retraités du Département du Nord ;

- de délimiter le périmètre d'action de l'Association, dans les conditions décrites au rapport et selon les principes suivants :

  · Les actions organisées sont exclusivement à destination de l'ensemble des agents départementaux en retraite y compris les assistants familiaux ;

  · Les actions organisées par l'Association doivent être complémentaires et non similaires à celles mises en œuvre par le COS au titre de la délégation donnée par le Département du Nord pour la réalisation de prestations sociales à destination de l'ensemble des agents y compris des agents retraités.

- d'autoriser Monsieur le Président à signer la convention de fonctionnement, entre le Département du Nord et l'association NORSENIORS, dans les termes du projet ci-joint en annexe.

Le quorum a été vérifié à l'appel de l'affaire à 18 h 12.

45 Conseillers départementaux étaient présents en séance. Ils étaient porteurs de 27 pouvoirs.

Décision acquise par assentiment de l'assemblée.

Signé électroniquement

DEPARTEMENT DU NORD · CONSEIL DEPARTEMENTAL · RF

Pour le Président du Conseil Départemental
et par délégation,
La Directrice des Affaires Juridiques
et de l'Achat Public,

Claude LEMOINE

ANNEXE 1

CONVENTION DE FONCTIONNEMENT ENTRE LE DEPARTEMENT DU NORD ET L'ASSOCIATION NORSENIORS

ENTRE :

LE CONSEIL DEPARTEMENTAL DU NORD,
dont le siège est en l'Hôtel du Département, 51, rue Gustave Delory, 59047 Lille Cedex,
représenté par **Monsieur Christian POIRET, Président du Département du Nord**
d'une part,
Ci-après désigné « Le Département »

L'ASSOCIATION NORSENIORS
dont le siège est au 2 rue Jacquemars Gielee, 59000 Lille
représenté par **Madame Marie-Françoise CARRARA-COETTE**
d'autre part,
Ci-après désigné « Association NORSENIORS »

Vu la loi du 1er juillet 1901 modifiée relative au contrat d'association ;

Vu l'article 9.1 de la loi 2000-321 du 12 avril 2000 relative aux droits et citoyens dans leurs relations avec les administrations ;

Vu l'article 70 de la loi du 19 février 2007 établissant le principe de la mise en œuvre d'une action sociale par les collectivités territoriales au bénéfice de leurs agents ;

Vu l'article L1611-4 du Code Général des Collectivités Territoriales ;

Vu l'article L2125-1 du Code Général des Collectivités Territoriales ;

Vu la délibération n° DRH/2025/175 de la Commission Permanente du Conseil Départemental du 30 juin 2025.

Il a été convenu de ce qui suit :

Article 1 : Objet de la convention.

La présente convention a pour objet de définir les engagements réciproques des parties pour la réalisation des actions menées par l'Association destinées à améliorer la qualité de vie de ses adhérents, retraités du Département du Nord.

L'objet de l'Association relève de l'action sociale, les prestations fournies étant assimilables à des prestations sociales. L'Association a pour mission de proposer des prestations sociales destinées aux agents retraités du Département. Ses objectifs principaux sont les suivants :

- Améliorer la qualité de vie de ses adhérents, tant sur le plan moral que matériel ;
- Favoriser le développement personnel de ses membres dans les domaines culturel, sportif et touristique ;
- Encourager des actions et activités visant à maintenir les liens sociaux entre adhérents, afin de préserver leur dynamisme et leur intégration ;
- Collaborer avec d'autres structures poursuivant des objectifs similaires, telles que le Comité des Œuvres Sociales (COS).

Article 2 : Modalités d'octroi de la subvention du Département.

En contrepartie des obligations imposées par la présente convention et, sous la condition expresse que l'Association respecte les stipulations de la convention, le Département peut lui accorder, chaque année, une subvention à concurrence d'une somme qui fera l'objet d'une délibération du Conseil Départemental.

Le montant de la subvention sera fixé par le Conseil Départemental, après examen des comptes financiers du dernier exercice arrêté et du programme prévisionnel des activités de l'exercice, mentionnés à l'article 9, pour lequel la subvention est demandée.

L'ensemble des documents devra être établi et transmis par l'Association au Département, avant la date limite fixée chaque année n-1, par le Département, pour le dépôt des demandes de subvention pour l'année n.

Le paiement de la subvention s'effectuera par virement sur le compte de l'Association.

Article 3 : Restitution des sommes non utilisées.

S'il apparaît, y compris après l'expiration ou la dénonciation de la présente convention, qu'une partie du financement départemental n'a pas été ou ne sera pas utilisée ou bien qu'elle n'a pas été utilisée conformément aux obligations contractuelles ou règlementaires, le trop-perçu sera reversé au Département.

Article 4 : Mise à disposition et désignation des locaux.

Le Département a décidé de soutenir l'Association dans la réalisation de ses objectifs en mettant gratuitement à sa disposition les locaux désignés ci-après :

- Les locaux situés au rez-de-chaussée du Nouveau Forum, 49 rue Gustave Delory à Lille, (salles C010 et C010 bis), **tous les jeudis après-midi de 14H00 à 18H00, en dehors des périodes de vacances scolaires** ;
- L'accès à l'espace de convivialité et aux sanitaires situés à proximité
- La salle du restaurant administratif située au 5ème étage de l'Hôtel du Département, 51 rue Gustave Delory à Lille, un jeudi par mois, sur réservation préalable de l'Association.

Article 5 : État des locaux, entretien et maintenance.

Article 5.1 : Etat des locaux :

L'Association prendra les locaux dans l'état où ils se trouveront lors de son entrée en jouissance ; elle déclare bien les connaître pour les avoir vus et visités à sa convenance.

L'Association ne peut, en aucun cas, changer l'affectation des locaux, faire de nouvelles installations ou des travaux d'aménagement ou de construction.

Article 5.2 : Entretien et maintenance des locaux :

L'Association s'engage à user du matériel mis à sa disposition en « bon père de famille » et à remettre le mobilier dans l'état d'ordonnancement et de propreté tel qu'elle l'a trouvé lors de son entrée dans les lieux.

Toutes les opérations de maintenance et d'entretien des locaux sont assurées, sans refacturation, s'agissant de locaux partagés, par le Département.

Article 6 : Mise à disposition du mobilier et du matériel informatique.

Article 6.1 Mise à disposition du mobilier :

Dans les salles C010 et C010 bis :
- 16 chaises ;
- 6 tables ;
- 2 Armoires (1 en C010 et 1 en C010 bis) ;

Au sein du restaurant administratif :
- 4 tables (6 tables, une fois par an) ;
- 30 chaises (une cinquantaine, une fois par an) ;
- 1 armoire.

Article 6.2 : Mise à disposition du matériel informatique

Un ordinateur portable comprenant :
- Les logiciels de bureautique de base (Word et Excel) ;
- Un accès à la messagerie Outlook ;
- L'application Rainbow ;
- Un accès à Intranet et à Internet.

Toute demande nouvelle ou de remplacement de mobilier ou de matériel informatique devra faire l'objet d'une demande écrite et motivée auprès du Président du Département et, le cas échéant d'un procès-verbal contradictoire de mise à disposition.

Article 7 : Transmission des données à caractère personnel.

Le Département s'engage à mettre à disposition de l'Association les données dont il dispose relative aux agents départementaux partant à la retraite de manière semestrielle (Nom, Prénom, adresse, numéros de téléphone fixe et/ou portable, adresse mail personnelle).

En contrepartie, l'Association devra respecter l'ensemble des obligations fixées dans le 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 (RGPD). A ce titre, une attention particulière devra être portée pour le transfert des données à caractère personnel entre le Département du Nord et le responsable distinct de l'Association quant au respect des dispositions de l'article 32 du RGPD (cf annexe 2 jointe à la présente convention).

Article 8 : Assurances.

L'Association souscrira toutes les polices d'assurances nécessaires pour garantir sa responsabilité civile. Elle devra s'acquitter du paiement des primes et des cotisations de ces assurances et en justifier par la remise, chaque année, de l'attestation au Département.

Article 9 : Responsabilité de l'Association.

L'Association sera personnellement responsable des conséquences dommageables résultant des infractions aux clauses et conditions de la présente convention, de son fait ou de celui de ses membres.

L'Association répondra des dégradations causées aux locaux mis à disposition pendant le temps qu'elle en aura la jouissance.

Article 10 : Engagements de l'Association.

En contrepartie de la mise à disposition gratuite des locaux et du matériel qui lui est consentie et de la subvention allouée par le Conseil Départemental, l'Association s'engage expressément à :

- Mettre en œuvre tous les moyens nécessaires à la réalisation des objectifs fixés ;
- Respecter la législation fiscale et sociale propre à son activité, de telle sorte que la responsabilité du Département ne puisse être recherchée ou inquiétée en aucune façon à ce sujet ;
- Se conformer aux prescriptions législatives et règlementaires relatives à l'exercice de son objet ;
- Fournir chaque année un rapport d'activité quantitatif et qualitatif de la réalisation des objectifs prévus avant le 30 janvier ;
- Fournir chaque année le bilan et le compte de résultat de l'exercice N-1 avant le 30 juin. La présentation retenue doit permettre d'isoler le financement du Département et son affectation. Ces documents devront être certifiés par le Président de l'Association et son Trésorier ;

- Conserver les pièces justificatives des écritures passées, ainsi que le registre des procès-verbaux des délibérations du Conseil d'Administration.
- Respecter la charte départementale d'utilisation des ressources des systèmes d'information (jointe en annexe 1 de la présente convention) ;
- Respecter le Règlement Général sur la Protection des Données, mentionné à l'article 7 de la présente convention.

Article 11 : Durée de la convention.

La présente convention est conclue pour une durée d'un an, à compte de sa date de notification, après signature des deux parties. Elle sera renouvelée tous les ans par tacite reconduction, au minimum quatre fois. La durée de la convention ne pourra pas excéder cinq ans.

Article 12 : Avenant à la convention.

Toute modification des conditions ou des modalités d'exécution de la présente convention, définie d'un commun accord entre les parties, fera l'objet d'un avenant.

Article 13 : Dénonciation de la convention.

La présente convention peut être dénoncée par l'une ou l'autre des parties, par lettre recommandée avec accusé de réception en respectant un délai de préavis de deux mis à compter de la notification de ladite lettre.

Article 14 : Résiliation de la convention.

Le Département se réserve le droit de mettre fin, unilatéralement et à tout moment à la présente convention, en cas de non-respect de l'une des clauses de la convention, dès lors que dans le mois suivant la réception de la mise en demeure envoyée par le Département, par lettre recommandée avec accusé de réception, l'Association n'aura pas pris les mesures appropriées.

La présente convention sera résiliée de plein droit, sans préavis, en cas de faute lourde de l'Association, de dissolution de l'Association ou en cas de destruction de locaux par cas fortuit ou de force majeure.

Article 15 : Règlements des litiges.

Tout litige né de l'exécution de la présente convention doit d'abord faire l'objet d'un règlement amiable. A défaut, le litige sera porté devant les juridictions administratives compétentes.

Fait à Lille, en deux exemplaires originaux

L'Association NORSENIORS,

Marie-Françoise CARRARA-COETTE

Le Président du Département du Nord,

Christian POIRET

Annexe 2

Charte d'Utilisation des ressources des Systèmes d'information

Version présentée lors du Comité Social Territorial du 15 juin 2023

TABLE DES MATIERES

1. PREAMBULE

1.1. Objectifs de la charte

Le présent document décrit les principes directeurs qui doivent être respectés afin de garantir l'usage correct et sécurisé des ressources des Systèmes d'Information du Département du Nord.

Cette charte a pour objectif :

- de préciser les principaux droits, devoirs et responsabilités des Utilisateurs, en accord avec la législation en vigueur, les règles de déontologie et, le cas échéant, le règlement intérieur ;
- de responsabiliser l'Utilisateur sur l'usage qu'il fait des ressources du Département mises à sa disposition, dans l'exercice de sa fonction ;
- de mettre en évidence la nécessité pour chaque Utilisateur de respecter ces règles, pour la sécurité de tous.
- d'informer les Utilisateurs sur les contrôles pouvant être réalisés pour assurer notamment la sécurité des systèmes d'information et la conformité aux lois et réglementations en vigueur.

La charte n'a pas pour objet de régir de façon exhaustive tous les cas de figure possibles, mais plutôt de fixer les principes généraux d'utilisation : c'est donc à l'esprit de ces principes que chacun devra se référer dans des situations non envisagées.

Les termes visés dans la présente charte feront l'objet de définitions à l'article « 8. Définitions ».

1.2. Champ d'application

La charte s'applique à l'ensemble du personnel tous statuts confondus, aux structures et organismes tiers (sous-traitants, prestataires, etc.) et plus globalement à l'ensemble des Utilisateurs amenés à utiliser les Systèmes d'Information du Département.

Annexée au Règlement intérieur des services, la charte est juridiquement opposable à l'ensemble des Utilisateurs et remplace l'ensemble des versions antérieures. Cette charte ne concerne toutefois pas les élus pour lesquels il existe une charte dédiée.

L'ensemble des ressources informatiques et des moyens de communication du Département du Nord sont concernés par la charte : poste de travail, serveur, messagerie, Intranet, Internet, équipement mobile, copieurs, téléphone, fax, etc.

1.3. Principes fondamentaux

1.3.1. Utilisation professionnelle des outils mis à disposition

L'utilisation des Systèmes d'Information du Département du Nord est réservée aux activités professionnelles. Toutefois, la présente charte rend possible une utilisation personnelle à condition qu'elle soit raisonnable.

En particulier, les Utilisateurs sont autorisés à faire une utilisation personnelle des ressources du Système Informatique mises à leur disposition sous réserve que cette utilisation demeure raisonnable, n'entrave pas la bonne marche des services, ne porte pas atteinte au fonctionnement normal ou la sécurité des Systèmes d'Information, ne soit pas contraire à la réglementation applicable et s'inscrive dans le respect du devoir de réserve envers le Département du Nord.

Conformément au principe de présomption d'utilisation professionnelle des Systèmes d'Information retenu par la jurisprudence, il appartient aux Utilisateurs de se conformer aux dispositions du 2.1.1.

1.3.2. Règles générales de confidentialité

Les règles d'éthique et de secret professionnel, de déontologie et d'obligation de réserve et de devoir de discrétion, imposées notamment par les articles L121-1 à L121-7 du Code général de la fonction publique, sont aussi totalement applicables.

Lors de conversations ou de communications téléphoniques dans des lieux publics, le respect des règles de discrétion est particulièrement requis.

L'attention des Utilisateurs est spécifiquement attirée sur le respect de ces règles de confidentialité sur les réseaux sociaux. Il est ainsi rappelé que chaque Utilisateur est seul responsable des propos qu'il tient sur les réseaux sociaux et plus largement sur Internet, y compris sur l'ensemble des fonctionnalités : forum, blog, wiki…. ou des applications mobiles. La responsabilité de chaque Utilisateur peut être engagée du fait de ces propos. Il est notamment demandé à l'ensemble des Utilisateurs une attention particulière concernant les informations liées à l'exercice de leur profession qui pourraient être partagées en ligne. En effet, ces informations peuvent toucher à des informations confidentielles, affecter d'autres individus qui n'ont pas consenti à leur diffusion et/ou projeter une image inexacte et incomplète de certains événements. Le Département du Nord appelle donc à la vigilance.

1.3.3. Protection des informations

L'Utilisateur veille, en tous lieux et en toutes circonstances, à ne pas porter atteinte aux intérêts du Département du Nord, de son personnel et de ses usagers.

L'Utilisateur ne devra pas permettre à des personnes non autorisées d'accéder aux informations confidentielles qu'il détient et ne devra pas diffuser sur des espaces publics comme Internet des informations à caractère confidentiel (données spécifiques au Département du Nord, informations sur des tiers, secret médical, etc.) notamment sur les réseaux sociaux ou autres applications non-professionnelles du Département.

L'Utilisateur ne doit consulter, modifier ou supprimer que les seules données dont la garde lui a été confiée. Cela concerne aussi bien les fichiers que les messages électroniques internes ou externes. Il ne doit pas usurper l'identité d'une autre personne et il ne doit pas tenter d'intercepter de communications entre tiers.

1.3.4. Respect de la législation

La mise en œuvre et l'utilisation des Systèmes d'Information sont soumises à un ensemble de textes législatifs et réglementaires. Dans le cadre de l'exercice de ses fonctions au quotidien, chaque Utilisateur peut être tenu pour responsable civilement ou pénalement en cas de manquement à ces obligations légales et réglementaires.

2. DROITS ET DEVOIRS DES UTILISATEURS DU SYSTEME INFORMATIQUE

2.1. Utilisation des ressources

2.1.1. Encadrement de l'usage personnel

Un usage personnel ponctuel et raisonnable des ressources informatiques mises à disposition par le Département du Nord, dans le cadre des nécessités de la vie courante et familiale, est toléré dès lors qu'il est mesuré, ne porte pas préjudice à l'activité professionnelle et qu'il n'est pas susceptible d'affecter la sécurité, la performance et le bon fonctionnement du Système informatique ou de mettre en cause l'intérêt et la réputation du Département du Nord.

Tout Utilisateur peut librement disposer d'un espace personnel sur son poste de travail et sur sa messagerie dans lequel il pourra introduire des fichiers protégés par le secret des correspondances. Toutefois, la sauvegarde et la restauration de cet espace personnel est sous la seule responsabilité de l'Utilisateur et la dénomination de cet espace doit faire apparaître ce caractère privé en nommant le dossier "PERSONNEL". L'usage syndical est toujours considéré comme confidentiel ([1]).

S'il fait usage de la messagerie à titre personnel, l'Utilisateur doit inscrire la mention sous cette forme «<PERSONNEL> », en début de l'objet du message et supprimer, dans le corps, toute mention relative au Département du Nord ou toute autre indication qui pourrait laisser croire que le message est rédigé par l'Utilisateur dans le cadre de l'exercice de ses fonctions.

Si l'Utilisateur reçoit, via le système de messagerie, des messages à caractère personnel, il lui est demandé, soit de les supprimer après en avoir pris connaissance, soit de les conserver dans un répertoire nommé "PERSONNEL" en prenant garde à ce que la taille de ce dossier ne puisse entraîner une saturation de sa boîte aux lettres ou de son espace de stockage.

Les correspondances électroniques détenues par l'Utilisateur dans sa boite de messagerie sont, sauf lorsqu'il les identifie comme étant personnelles, présumées avoir un caractère professionnel, de sorte que le Département du Nord peut y avoir accès hors sa présence.

Sur ce point, il est à noter que la jurisprudence[2] accorde, dans des circonstances particulières, le droit au Département du Nord d'ouvrir des fichiers identifiés comme « PERSONNEL » en présence de l'employé concerné ou après que celui-ci ait été dûment appelé.

Afin de préserver l'intégrité des Systèmes d'Information, l'Autorité Départementale pourra prendre la décision de suspendre de façon temporaire l'accès d'un Utilisateur au Système Informatique.

2.1.2. Accès aux ressources

Pour accéder aux différentes ressources comme le poste de travail, le réseau, la messagerie, l'intranet et l'internet, chaque Utilisateur dispose d'un identifiant et d'un mot de passe attribués suite à une Demande d'accès. Une authentification multifacteurs peut être exigée pour certaines ressources, notamment pour les accès et services à distance, afin de renforcer le niveau d'authentification de l'utilisateur par des moyens complémentaires aux mots de passe (Ex : code temporaire reçu par SMS, code généré depuis une application mobile, clé de sécurité, etc.).

Ces informations sont personnelles et confidentielles et ne doivent en aucun cas être communiquées à d'autres personnes. Chaque Utilisateur est seul responsable de la sécurité de ses identifiants et mot de passe. Il lui appartient de les mémoriser et de ne pas les écrire ou enregistrer sur un support non sécurisé, ni les communiquer à un tiers. L'agent doit prendre toute mesure raisonnable afin de garantir la confidentialité et la sécurité de ses identifiants et mots de passe. Il pourra notamment utiliser le gestionnaire de mots de passe mis à disposition par la DSI.

Tout accès au Système Informatique réalisé grâce à l'identifiant et au mot de passe d'un Utilisateur sera réputé réalisé par cet Utilisateur sauf en cas avéré d'usurpation d'identité.

---

[1] Voir point 6 : conditions particulières OS

[2] ; CEDH, AFFAIRE LIBERT c. FRANCE, requête n°588/13, 22 février 2018)

Le mot de passe attribué doit être changé à la première utilisation puis régulièrement. Il doit être conforme à la Politique de mots de passe du Département du Nord. Chaque Utilisateur veillera à utiliser un mot de passe différent pour chaque ressource du Système d'Information.

Les mots de passe ne sont pas conservés par la DSI. En cas de perte, l'Utilisateur demandera qu'un nouveau mot de passe soit généré.

Les droits d'accès définissent ce à quoi il est possible d'accéder avec l'identifiant et le mot de passe. Ils sont différents d'un Utilisateur à l'autre selon le poste qu'il occupe et ses fonctions. Ils sont incessibles et révocables à tout moment.

Ils sont adaptés à l'affectation des agents départementaux

Annuellement, une revue des droits des agents sera organisée entre la DSI et la hiérarchie.

2.1.3. Utilisation du poste de travail

La DSI est la seule entité habilitée à donner l'autorisation d'utiliser une application sur le poste de travail ou sur Internet.

Le contenu des supports personnalisés, de fond d'écran ou de l'écran de veille du poste de travail peut être personnalisé mais ne doit pas porter atteinte à l'image du Département du Nord, ni aux obligations de neutralité et de réserve qui s'imposent. Chaque Utilisateur doit d'ailleurs faire preuve de décence dans le choix des supports utilisés et veiller au respect de la dignité due à l'égard de sa hiérarchie comme à l'ensemble de ses collègues.

Afin de permettre un accès individuel à l'Intranet et à la messagerie le plus large possible à l'ensemble des Utilisateurs, il est rappelé aux responsables hiérarchiques dont le service dispose d'un ou plusieurs postes en libre-service que :

- les postes en libre-service, avec un téléphone à proximité, doivent être facilement identifiables et accessibles à l'ensemble des agents du service durant le temps de travail.
- les postes en libre-service permettent l'accès aux différentes ressources disponibles sur l'espace personnalisé du portail :
  - boîte aux lettres individuelle et électronique de messagerie
  - applications Bureautique et Métier du service
  - site Intranet et Internet
- les agents doivent se connecter avec leur identifiant personnel pour accéder à leur espace personnalisé sur le portail.
- les agents doivent se déconnecter de leur espace personnalisé dès la fin de l'utilisation.

2.1.4. Utilisation de la messagerie

L'utilisation de la messagerie électronique ou de la messagerie collaborative instantanée est destinée principalement aux activités professionnelles.

L'Utilisateur doit apprécier si le contenu du message qu'il diffuse n'engage pas la responsabilité de son service ou de sa direction. Dans le cas où le message engagerait la responsabilité de son service ou de sa direction, cette diffusion ne peut se faire qu'en accord avec le supérieur hiérarchique. La diffusion de messages toutes boites n'est pas autorisée sauf pour les besoins institutionnels par des personnels habilités.

Des règles spécifiques ont été établies pour l'envoi de mails par les organisations syndicales au 6.2.2 d). En dehors de ces cas d'usages, la messagerie professionnelle individuelle ne devra pas être utilisée par un agent pour une communication syndicale de masse.

Avant de diffuser un message, l'Utilisateur doit s'assurer que ce dernier :

- respecte l'obligation de neutralité, de discrétion professionnelle et de réserve, et d'une manière générale, ne porte pas atteinte aux droits et à la dignité des agents de la collectivité ;
- ne permet pas la propagation de virus ;
- respecte les sous-couverts et les visas hiérarchiques ;
- adopte le code spécifique pour les messages à grande diffusion.

Dans le cadre de l'usage de la messagerie interne, l'Utilisateur ne doit pas :

- Ouvrir des messages dont l'origine, l'expéditeur, l'objet ou le contenu est douteux, ou ouvrir les pièces jointes suspectes. Il veille notamment à respecter les consignes d'alerte en cas de suspicion d'un hameçonnage (phishing). En cas de réception d'un tel message, il avertit immédiatement le service relation utilisateur à l'aide de la fonctionnalité de signalement dans la messagerie, ou à défaut, par mail à l'adresse assistance-informatique-35858@lenord.fr ou par téléphone numéro 03.59.73.58.58.
- Mettre en œuvre une redirection automatique ou réplication de messages vers une adresse électronique externe.
- Prendre de décision importante à la seule vue d'un message électronique, si son authenticité et son intégrité ne peuvent pas être garanties (l'envoi d'un message électronique peut être confirmé par téléphone, par exemple) ;
- Echanger des informations à caractère confidentiel ou sensible (données à caractère personnel) pour les envois externes vers des destinataires tiers sans mesure de sécurité adaptée (solution de chiffrement).

Un système de filtrage des courriers électroniques non désirables est actif sur le Système Informatique. Lorsqu'un courrier électronique est identifié par le système comme étant non désirable car dangereux pour le système (adresse de l'expéditeur suspecte, contenu du message, etc.) il est isolé et n'est pas transmis à son destinataire.

Dans l'hypothèse où un Utilisateur ne pourrait recevoir un courrier électronique d'un tiers, il pourra faire une demande à la Direction des Systèmes d'Information pour vérifier si ce courrier électronique a été bloqué à cause de ce mécanisme de filtrage et en demander le déblocage, le cas échéant.

2.1.5. Utilisation de l'accès Internet

Afin de prévenir l'accès à certains sites non autorisés en raison de leur caractère immoral, illicite, illégal (pornographie, pédophilie, racisme, incitation à la haine raciale, révisionnisme, etc.), de leur caractère dangereux pour la sécurité du Système d'Information (phishing, sites internet malveillants ou piégés, …) ou sans utilité professionnelle, un filtrage, décrit à l'article 4.4.2, a été mis en œuvre.

Cet outil ne dispense pas les Utilisateurs d'une juste déontologie individuelle. Chaque Utilisateur est seul responsable de la décision d'accéder à un site Internet. Le fait que l'accès à un site en particulier ne soit pas interdit ne signifie pas que l'accès à ce site est autorisé et conforme à la réglementation applicable.

Si certains sites non accessibles s'avéraient présenter un intérêt professionnel, il convient de contacter le service relation utilisateur en fournissant tous les éléments d'étude nécessaire.

Le Département du Nord ne pourra être tenu responsable du contenu des sites visités par l'Utilisateur, en dehors de son activité professionnelle, ni des éventuelles compromissions ou mises en cause qui pourraient avoir lieu suite à la visite de ces sites.

En cas de situation exceptionnelle et notamment en cas de danger pour les Systèmes d'Information, l'Autorité Départementale pourra prendre la décision de suspendre momentanément l'ensemble des accès à Internet afin de préserver l'intégrité du Système Informatique.

2.1.6. Utilisation des services d'accès à distance

Dans le cadre de l'ouverture des Systèmes d'Information vers Internet (accès extranet, télétravail, synchronisation de smartphones, etc.), des services d'accès à distance à la messagerie ou à d'autres ressources du Système Informatique sont mis en place.

Les usages de matériels personnels sont soumis à une validation préalable de l'Autorité Départementale selon les procédures et prérequis en vigueur.

Dans tous les cas, les Utilisateurs veillent à ce que leurs matériels personnels respectent les bonnes pratiques en matière de cybersécurité : applications des mises à jour des systèmes et des correctifs de sécurité, présence d'un antivirus, d'un pare-feu, accès protégé par un mot de passe, … ils protègent les informations et données professionnelles qu'ils pourraient y stocker, et veillent notamment à les supprimer après leur utilisation.

Les Utilisateurs peuvent aussi connecter les matériels de l'Autorité Départementale à des réseaux Wifi privés (à leur domicile). La connexion de matériels à des réseaux Wifi publics sans mesure adaptée (VPN) est déconseillée pour des raisons de sécurité.

Les services d'accès à distance sont restreints à certains usages. L'accès est soumis à une demande particulière selon les règles en vigueur.

En particulier, pour synchroniser leur messagerie professionnelle sur un terminal mobile personnel, les agents doivent demander à la Direction des Systèmes d'Information l'activation de la synchronisation. Des règles spécifiques sont prévues pour cet usage, et font l'objet d'un contrat entre l'Autorité Départementale et l'agent, dont les règles s'appliquent en sus des règles de la présente Charte.

L'ensemble des procédures relatives à chacun des usages permis est disponible sur l'Intranet.

L'ensemble des règles décrites dans les articles précédents concernant l'utilisation des ressources restent applicables.

Dans les cas d'utilisation des services d'accès à distance, afin de limiter le risque de divulgation d'information, des précautions particulières s'imposent :

- S'assurer d'être connecté sur un réseau sécurisé (HTTPS) ;
- Être particulièrement vigilant afin de ne pas divulguer d'information confidentielle lors d'une consultation à distance. (Regard indiscret d'un tiers, etc.) ;
- Se déconnecter systématiquement et complètement du service d'accès à distance après utilisation ;
- Protéger contre le vol les équipements mobiles et accessoires ;
- Respecter les contrats de services encadrant l'usage des smartphones professionnels et personnels ;
- Dans le cas de l'utilisation éventuelle et à titre exceptionnel d'un poste de travail ou d'un smartphone non géré par l'Autorité Départementale, il convient en complément de :
    - Ne pas enregistrer de document sur le disque dur (Message, fichier en pièce jointe, etc.) ;
    - Utiliser la fonction navigation privée du navigateur ou a minima veiller à effacer l'historique de navigation au sein du navigateur utilisé ;
    - Adopter de bonnes pratiques de sécurité sur le poste de travail ou le smartphone : contrôle d'accès, présence des correctifs de sécurité, antivirus fonctionnel, pare-feu personnel, etc.

En tout état de cause, les Utilisateurs sont seuls responsables de la sécurité de leurs équipements personnels.

2.1.7. Utilisation de la téléphonie

Le Département du Nord met à disposition de certains de ses Utilisateurs des téléphones fixes, mobiles ou un logiciel de téléphonie. Ces téléphones, comme toute ressource informatique, sont destinés à un usage professionnel. Une utilisation à titre privé ponctuelle et raisonnable est tolérée. Toute utilisation à titre privé manifestement abusive peut entraîner le prononcé d'une mesure telle que définie aux 4.1 et 5 de la présente Charte.

Certains téléphones offrent des possibilités d'accès à Internet. Ces téléphones sont soumis aux mêmes règles de sécurité que les autres composants du Système Informatique et notamment (cf tutoriels):

- mises à jour régulières

- codes d'accès sécurisés

- chiffrement des données de l'appareil

- sauvegarde des données

- limitation des applications installées (magasins officiels)

2.2. Propriété intellectuelle

2.2.1. Création

Il est rappelé aux Utilisateurs des Systèmes d'Information qu'en matière de création, les droits sur les logiciels sont dévolus automatiquement au Département du Nord sauf dispositions statutaires et stipulation contraire (article L113-9 du Code de la Propriété Intellectuelle) et qu'ils ne sont donc pas autorisés pour une utilisation autre que celle du Département du Nord.

2.2.2. Duplication et utilisation de logiciels

La duplication ou l'utilisation de logiciels, gratuits ou non, sans l'autorisation des titulaires des droits est constitutive du délit de contrefaçon pouvant engager les responsabilités pénale et civile de l'Utilisateur et du Département du Nord.

Les Utilisateurs doivent donc s'abstenir de détenir de tels logiciels, de les diffuser ou d'en solliciter l'envoi en pièces jointes de la part d'un tiers. La reproduction et l'utilisation de toute application disponible via Internet sont soumises à l'autorisation préalable de l'Administrateur et à l'acceptation des titulaires des droits, qu'il s'agisse de logiciels commerciaux, de Sharewares ou de logiciels gratuits. Il convient également de ne pas transférer de données à caractère personnel ou sensibles à des tiers pour l'usage d'applications ou de services en ligne sur Internet sans accord préalable de l'Administrateur, du DPD et du RSSI.

2.2.3. Duplication et utilisation d'Œuvres

Il est rappelé aux Utilisateurs des Systèmes d'Information que l'utilisation d'Internet permet d'accéder à des informations ou à des œuvres diffusées en infraction avec la législation ainsi qu'à des données ou des œuvres protégées dont le téléchargement ou la duplication peuvent être subordonnés à l'accord du titulaire des droits.

Les Utilisateurs doivent donc prendre toutes dispositions pour consulter ou reproduire de manière licite les données ou œuvres protégées par des droits d'auteur, sous quelque forme que ce soit, notamment les œuvres musicales, audiovisuelles et littéraires.

2.3. Traitement de données à caractère personnel

La loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés et le 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, précisent strictement les conditions légales de la collecte, de l'enregistrement, et de la conservation des données à caractère personnel, ainsi que les conditions de leur traitement automatisé,

Le Département du Nord est considéré comme responsable des traitements qu'il met en œuvre sur des données à caractère personnel. Un Délégué à la Protection de Données (DPD) du Département du Nord a été désigné conformément à la législation en vigueur. Il peut être contacté à l'adresse dpd@lenord.fr

Les Utilisateurs des Systèmes d'Information s'engagent à respecter, dans le cadre de leur exercice professionnel, les règles issues de la loi « Informatique et libertés » et du RGPD, notamment en ce qui concerne les obligations du responsable de traitement (notamment information des personnes, confidentialité et sécurité des données) et les droits des personnes visées par les traitements (notamment accès et rectification).

Certaines informations (ethnies, convictions philosophiques, politiques, religieuses, données de santé etc.) sont considérées comme étant des données sensibles. Les Utilisateurs ne peuvent traiter cette catégorie de données sans y avoir été expressément autorisés préalablement par le responsable des traitements et/ou par ses missions.

En l'absence de formalités déclaratives, il est rappelé que la messagerie départementale ne doit pas être utilisée pour communiquer des données à caractère personnel à un tiers n'ayant pas qualité pour les recevoir.

En tant qu'autorité de contrôle, la Commission nationale de l'informatique et des libertés (CNIL) peut prendre des sanctions à l'encontre des personnes qui ne respectent pas les obligations relatives à la protection des données à caractère personnel.

Conformément aux articles 48 à 56 de la loi n°78-17 « Informatique et libertés » du 6 janvier 1978, chaque Utilisateur bénéficie de droits spécifiques sur les traitements de données à caractère personnel dont il fait l'objet, dans les limites des textes applicables :

- Le droit à l'information sur les traitements de données le concernant ;
- Le droit d'accès à ses propres données personnelles ;
- Le droit de rectification ou de suppression de ses données ;
- La possibilité de s'opposer ou de limitation pour des motifs légitimes, à figurer dans un fichier ;

L'Utilisateur pourra faire valoir ses droits en s'adressant au DPD à l'adresse dpd@lenord.fr.

2.4. Départs et absences

Avant son départ du Département ou une absence prolongée, il appartient à l'Utilisateur de sauvegarder et de supprimer ses fichiers et messages à objet personnel. Il ne doit pas dupliquer ou conserver des données professionnelles (fichiers, éléments de messagerie, ...) quel que soit le support ou le matériel personnel (smartphone, clé USB, ...). En outre, tous les équipements fournis doivent être restitués au Département du Nord avant le départ de l'Utilisateur.

Préalablement à son départ ou à une absence prolongée, l'Utilisateur s'assure que tous les documents professionnels nécessaires en sa possession sont accessibles pour les besoins du service et active les notifications d'absence sur la messagerie. Il peut désigner un mandataire (agent du service) de son choix en vue de consulter les messages à caractère professionnel. Cette consultation doit être exclusivement orientée pour les besoins du bon fonctionnement du service. Toute consultation de messages dénués de rapport avec les dossiers professionnels est interdite.

Pour les besoins de la continuité du service et dans l'impossibilité de joindre l'Utilisateur, un accès peut être réalisé en son absence sur demande justifiée et validée par le supérieur hiérarchique. Le supérieur hiérarchique, ou toute personne déléguée par ce dernier, sera ainsi habilité à consulter uniquement les fichiers à caractère professionnel.

En cas de décès d'un agent, seul le répertoire nommé "PERSONNEL" pourra être transmis aux familles qui en formuleront expressément la demande auprès de l'Autorité Départementale. Aucun accès libre aux matériels professionnels ne pourra être donné.

Les messages à objet personnel et syndicaux ne seront jamais consultés.

Enfin, il est rappelé qu'en cas de départ d'un Utilisateur du Département du Nord, une suppression de l'ensemble de sa boîte aux lettres de messagerie sera effectuée un mois après son départ effectif.

2.5. Sécurité

L'Utilisateur est responsable de l'usage des ressources auxquelles il a accès.

Afin de contribuer à la sécurité des Systèmes d'Information du Département du Nord, l'Utilisateur doit adopter un comportement responsable qui se traduit notamment par :

- Le verrouillage de son poste de travail en cas d'absence même temporaire ;
- Le respect de la configuration matérielle et logicielle des équipements qui sont mis à sa disposition ;
- L'utilisation limitée des supports amovibles (clé USB, disque dur externe, etc) en privilégiant les autres solutions d'échanges. Lorsque son utilisation est indispensable, l'Utilisateur devra s'assurer que le support ne contient pas de virus et il devra chiffrer les documents contenant des données confidentielles ou sensibles ;
- La récupération immédiate des documents sensibles qu'il envoie, imprime ou photocopie sur les fax, les imprimantes ou les photocopieurs ;
- La sauvegarde régulière des données stockées localement sur le poste de travail vers le lecteur réseau du Département du Nord, espaces collaboratifs ou autres espaces sécurisés mis à disposition ;
- L'application immédiate des mises à jour de sécurité ou du système d'exploitation demandées par l'Administrateur, et le redémarrage du poste de travail si nécessaire ;
- L'interdiction d'utiliser des solutions de stockage ou de sauvegarde externe pour les données professionnelles hors celles proposées par le Département ;
- Un redémarrage régulier de son poste de travail.

L'ensemble des préconisations précédentes restent valables dans le cadre du télétravail, en respect des dispositions de la charte applicable au télétravail, l'agent en télétravail doit veiller en outre à :

- Utiliser systématiquement le matériel informatique professionnel mis à disposition (sauf à titre exceptionnel);
- Privilégier un lieu de télétravail sécurisé (absence de tiers, va-et-vient limité, accès aux documents de travail confidentiels difficile pour un tiers, etc.) ;

L'Utilisateur devra porter également une attention particulière aux éléments de sécurité lié à la signature électronique.

2.6. Opinions personnelles

La liberté d'expression se trouve limitée dans l'exercice de certaines fonctions et en particulier par le devoir de réserve des agents publics. L'utilisateur n'émettra pas d'opinions personnelles susceptibles de porter préjudice au Département du Nord.

L'Utilisateur désirant participer en tant que contributeur à une communauté virtuelle externe (réseaux sociaux) ayant un rapport avec son activité professionnelle doit obtenir l'autorisation formelle de sa hiérarchie. L'Utilisateur reste responsable du contenu qu'il diffuse.

2.7. Signalement des incidents

En cas de suspicion d'infection virale ou tous autres actes de malveillance (perte ou chiffrement de fichier, demande de rançon, activité anormale, ...) sur le poste de travail, l'Utilisateur doit :

- déconnecter le poste de travail du réseau en débranchant le câble réseau ou en activant le mode avion pour les ordinateurs portables

- laisser l'ordinateur allumé et ne pas le redémarrer

- avertir immédiatement le service relation utilisateur au 03 59 73 58 58

En cas de perte ou de vol, quelles qu'en soient les circonstances, après avoir pris les dispositions auprès de l'Opérateur de Téléphonie et auprès de l'Autorité de Police, l'Utilisateur doit :

- contacter le service relation utilisateur dans les délais les plus brefs, au 03 59 73 58 58 aux heures ouvrables ou en envoyant un mail à l'assistance-informatique-35858@lenord.fr

- modifier immédiatement son mot de passe d'accès au Système d'Information.

Le Département est déchargé de toute responsabilité en cas d'usage frauduleux par toute personne autre que le bénéficiaire du matériel.

En cas de vol, l'Utilisateur devra fournir une copie du récépissé de dépôt de plainte faite au commissariat de police ou à la gendarmerie.

Une procédure de violation de données sera ouverte auprès du DPD si le matériel concerné contenait des données à caractère personnel.

Comportements et actes illicites

Le Code pénal interdit à tout Utilisateur de stocker ou de diffuser tout document proscrit par la loi. Sont concernés notamment, mais non exclusivement, par cette interdiction :

- les images et/ou textes à caractère pédophiles ;
- les images et/ou textes à caractère racistes ;
- le trafic de stupéfiants ;
- les atteintes à la Sécurité Nationale ;
- les propos injurieux et/ou à caractère diffamatoire.

Dans le cas où un agent recevrait à son insu de tels documents, il doit les détruire. Les mêmes sanctions pénales que celles prévues pour les cas listés précédemment sont applicables aux Utilisateurs qui accèdent à ces sites Web et participent à des forums traitant de ces sujets.

Les Utilisateurs doivent en outre être conscients que ces mêmes sites sont susceptibles de récupérer leurs adresses e-mails et de les utiliser.

En cas de procédure judiciaire pour une infraction présumée aux dispositions du code pénal, le Département du Nord pourrait être tenu de communiquer sur demande de l'autorité judiciaire, l'ensemble des éléments litigieux présents dans les systèmes d'information ainsi que toute autre information demandée.

3. DROITS ET DEVOIRS DE L'ADMINISTRATEUR

Au travers des habilitations dont ils disposent, les Administrateurs du Système d'Information, titulaires de comptes à privilèges sur tout ou partie du Système d'Information (équipements réseaux et de sécurité, environnements techniques, postes de travail, applicatifs métier), ont des capacités très importantes :

- Accès à l'ensemble des données ;
- Accès à l'ensemble des traces ;
- Capacité à engendrer, par maladresse ou malveillance, des incidents graves.

3.1. Rappel des missions des Administrateurs du Système d'Information

Les Administrateurs ont pour mission de participer à la mise en œuvre, à la surveillance, au maintien en condition opérationnelle et à l'administration des éléments du Système d'Information sur leurs périmètres d'intervention (équipements réseaux, serveurs, postes de travail, bases de données, applications…).

Ils participent activement, en collaboration avec le RSSI, au maintien du niveau de sécurité du Système d'Information en mettant en œuvre les mesures de sécurité techniques, en appliquant les correctifs de sécurité et en prenant part, en toute transparence, aux audits de sécurité.

L'Administrateur est autorisé à prendre toutes les dispositions nécessaires au maintien de la sécurité et du fonctionnement des ressources dans son périmètre de responsabilité.

Il a notamment le droit de :

- veiller à la bonne utilisation des ressources dans son domaine de responsabilité, notamment en ce qui concerne les volumes d'informations transmis et reçus, la gestion des espaces de stockage et la capacité des équipements ;
- traiter (détection, analyse, éradication, filtrage, etc.) tout flux informatique présentant des risques de sécurité (virus, intrusion, utilisation d'un logiciel interdit, etc.) ;
- isoler ou arrêter des comptes Utilisateurs, équipements, ressources ou systèmes informatiques, en cas de menace importante pouvant compromettre la sécurité de l'ensemble du Système Informatique.

3.2. Protection des données et respect de la vie privée

Les Administrateurs du Système d'Information se doivent de protéger les données auxquelles ils peuvent avoir accès dans le cadre de leur mission, en particulier :

- Les données sensibles ou classifiées du Département ;
- Les données personnelles des Utilisateurs ;
- Les données relevant d'une règlementation particulière, notamment données de santé, données à caractère personnel, …

La présente charte informatique établit un contrat de confiance entre les Utilisateurs et les Administrateurs sur la protection de ces données personnelles. La discrétion des administrateurs est non seulement un devoir mais également un élément primordial de ce contrat de confiance.

Cet engagement ne se limite pas aux données personnelles, les administrateurs pouvant être amenés, pour des raisons de continuité d'activité, à accéder ou à fournir l'accès aux données professionnelles de l'utilisateur (fichiers, messagerie…) à d'autres utilisateurs dûment habilités, après demande de service validée par le RSSI (Responsable de la Sécurité des Systèmes d'Information) ou le DSI.

L'Administrateur est soumis à plusieurs obligations relatives au secret professionnel et à la préservation des informations confidentielles auxquelles il a accès :

- il n'accède ou ne donne accès aux informations du Système Informatique qu'après autorisation explicite de la part de leur(s) Propriétaire(s) et dans le strict respect des procédures formalisées ou dans le cas particulier prévu pour les incidents de sécurité ou par la loi ;
- il respecte ses engagements de confidentialité. Ainsi, il ne divulgue aucune information dont il a pris connaissance dans le cadre de ses fonctions, en particulier lorsque celle-ci est couverte par le secret des correspondances ou relève de la vie privée des Utilisateurs, et ne remet en cause ni le bon fonctionnement des ressources du Système Informatique, ni leur sécurité ;
- il a un devoir d'information, de conseil et de mise en garde vis-à-vis des Utilisateurs ;
- il a un devoir d'alerte auprès du Responsable de la Sécurité des Systèmes d'Information (RSSI) s'il a connaissance d'un événement pouvant impacter la sécurité du SI.

Les Administrateurs engagent leur responsabilité en cas d'utilisation abusive des privilèges qui leur sont conférés, notamment pour exercer un contrôle des activités des utilisateurs.

Les activités des Administrateurs sont tracées dans le cadre du contrôle du SI. L'Autorité Départementale s'engage, conformément aux recommandations de la CNIL, à ne conserver ces logs que pour une durée de 6 mois au-delà de laquelle ils seront systématiquement effacés.

3.3. Utilisation des comptes à privilèges

Au titre de leurs missions, les Administrateurs ont pour mission d'assurer le fonctionnement normal et la sécurité des réseaux, systèmes et/ou applicatifs selon leurs périmètres d'intervention. Ils sont conduits par leurs fonctions même à avoir accès à des informations personnelles relatives aux agents (messagerie, historique des sites visités, fichiers « logs » ou de journalisation, etc.) y compris celles qui sont enregistrées sur le disque dur du poste de travail (fichiers temporaires, cookies…).

L'accès aux données enregistrées par les agents départementaux dans leur environnement informatique (qu'elles soient personnelles ou non) ne peut être justifié que dans les cas où le bon fonctionnement des systèmes informatiques ne pourrait être assuré par d'autres moyens moins intrusifs.

En tant qu'acteur clé de la sécurité des systèmes d'information et des données qui lui sont rendues accessibles, il pèse une responsabilité accrue sur les Administrateurs. A ce titre, l'Administrateur est tenu à des obligations de :

- **Loyauté** : l'Administrateur étant investi de larges pouvoirs de surveillance sur les données qui circulent sur les systèmes d'information du Département du Nord, le respect de règles d'éthique est attendu de sa part. Peuvent être notamment reconnus comme un défaut de loyauté :
  - Le fait d'accéder ou de se maintenir, frauduleusement dans tout ou partie d'un système de traitement automatisé de données,
  - Le fait d'entraver ou de fausser le fonctionnement d'un système de traitement automatisé de données
  - Le fait d'introduire frauduleusement des données dans un système de traitement automatisé, d'extraire, de détenir, de reproduire, de transmettre, de supprimer ou de modifier frauduleusement les données qu'il contient
  - Le fait, sans motif légitime, notamment de recherche ou de sécurité informatique, d'importer, de détenir, d'offrir, de céder ou de mettre à disposition un équipement, un instrument, un programme informatique ou toute donnée conçus ou spécialement adaptés pour commettre une ou plusieurs des infractions
  - La participation à un groupement formé ou à une entente établie en vue de la préparation, caractérisée par un ou plusieurs faits matériels, d'une ou de plusieurs des infractions
- **Transparence** : l'Administrateur doit exercer ses missions dans le cadre du règlement intérieur et de la présente charte informatique. Il est à noter que le non-respect des principes de cette charte pourra être analysé comme une violation du contrat de travail pouvant donner lieu à des sanctions disciplinaires, y compris un licenciement.
- **Confidentialité** : l'Administrateur est tenu à une obligation particulière de confidentialité tenant notamment au secret professionnel. Il ne doit pas divulguer les informations auxquelles il aurait pu avoir accès lors de l'exercice de ses fonctions, a fortiori lorsqu'elles sont couvertes par le droit à la vie privée ou le secret des correspondances, à moins qu'une disposition législative ne l'impose (ex. en cas de découverte de contenus illicites).

Compte tenu de la « dépendance » départementale à l'égard de ce type de fonctions, le non-respect de ces obligations peut donner lieu à la fois à une responsabilité de la collectivité, mais également en cas d'agissement imputable à l'agent à une responsabilité pénale personnelle de l'Administrateur (au titre des articles 226-15 ou 323-1 et suivants du code pénal) ou faire l'objet d'une faute grave dans le cadre d'une procédure de licenciement.

Les Administrateurs disposent à la fois de compte(s) utilisateur et de compte(s) d'administration. Les comptes d'administration doivent être réservés aux tâches nécessitant des privilèges élevés, les tâches courantes devant être effectuées à l'aide des comptes d'utilisation.

En particulier, les activités quotidiennes de bureautique, messagerie et navigation internet doivent être réalisées au travers du compte d'utilisation et non au travers du compte d'administration. De même, les comptes utilisateur ne doivent pas être Administrateur de leur poste de travail.

Que les dispositifs techniques l'imposent ou non, les Administrateurs se doivent d'être exemplaires sur le respect de la politique de mots de passe spécifique aux Administrateurs et leur stockage.

3.4. Propriété intellectuelle

Les Administrateurs doivent être irréprochables en matière de protection de la propriété intellectuelle et donc s'interdire :

- L'installation, la diffusion ou l'utilisation de logiciels en dehors des conditions définies par le contrat de licence (notamment sans disposer des licences adéquates pour les logiciels commerciaux) ;
- Le stockage ou la diffusion de contenus multimédias protégés (musiques, films…).

3.5. Conduite en cas d'incident de sécurité

En cas de soupçon ou d'incident touchant la sécurité des Systèmes d'Information (c'est-à-dire touchant la disponibilité, la confidentialité, l'intégrité ou la traçabilité des services ou des données), les Administrateurs sont tenus d'en référer dans les meilleurs délais au Responsable de la Sécurité des Systèmes d'Information (RSSI) et de respecter les mêmes consignes décrites pour les Utilisateurs (déconnexion du poste du réseau, …)

Dans le cas d'absolue nécessité ou d'un incident de sécurité avéré, lié à la sécurité des systèmes d'information et afin de déterminer la cause ou les origines, le Responsable de la Sécurité des Systèmes d'Information (RSSI) et l'Administrateur habilité pourront avoir accès à l'ensemble des données ou matériels (postes de travail, serveurs, équipements réseaux, …) du Système d'Information.

Il conviendra d'associer le DPD si l'incident impacte des données à caractère personnel.

3.6. Conduite en cas d'utilisation abusive du SI

Les Administrateurs peuvent être amenés à constater, dans le cadre de leur activité, des utilisations abusives du Système d'Information ou des manquements à la charte informatique ou à la Politique de Sécurité du Système d'Information : téléchargement ou stockage de contenus ou de logiciels protégés…

Dans ce cas, les Administrateurs transmettent ces informations au Responsable de la Sécurité des Systèmes d'Information (RSSI).

Les usages répréhensibles doivent être signalés sans délai au RSSI.

3.7. Accueil des prestataires

De nombreux prestataires sont amenés à intervenir sur le Système d'Information du Département du Nord, de manière ponctuelle ou plus régulière. Dans le cadre de ces interventions, ils sont souvent amenés à utiliser des comptes à privilège. Ces comptes doivent être nominatifs et disposer d'une date d'expiration, et suivre le dispositif de gestion des identités en vigueur.

Lorsque les dispositifs concernés ne permettent pas de définir un compte nominatif, les Administrateurs doivent changer le mot de passe du compte privilégié préalablement à l'intervention du prestataire, pour le changer à nouveau à la fin de son intervention.

Il est de la responsabilité de l'Administrateur accueillant le prestataire de veiller aux actions techniques menées sur le Système d'Information.

4. CONTROLES

La responsabilité du Département peut être engagée en raison des agissements de ses agents. Pour cette raison, il met en place un contrôle de l'utilisation des différents moyens de communication et d'information mis à la disposition des Utilisateurs.

Conformément aux exigences du droit français dans ce domaine, les restrictions et les surveillances mises en place sont définies ci-après.

La réalisation de ces contrôles est sous la responsabilité de la Direction des Systèmes d'Information.

4.1. Cadre général

En cas de non-respect des règles de la présente charte, d'agissements frauduleux, fautifs ou dommageables, l'agent à l'origine des fautes pourra être tenu pour personnellement responsable et faire, le cas échéant, l'objet de sanctions disciplinaires et éventuellement de poursuites judiciaires.

Un retrait ou une suspension temporaire de l'accès aux ressources évoquées au 2.1 pourra être prononcé.

4.2. Supervision de la messagerie

Afin d'assurer la sécurité des systèmes d'information, la supervision des systèmes de messagerie porte de manière globale ou par utilisateur sur de la collecte d'informations techniques. La supervision est réalisée dans le strict respect du secret des correspondances privées et n'a pas pour but de contrôler le contenu des messages.

Chaque message fait l'objet

- D'un contrôle de l'adresse émettrice afin de vérifier la non-usurpation des adresses utilisées en interne ;
- D'une analyse automatique visant à bloquer tout message non-conforme (type de pièce-jointe, taille, ...) ;
- D'un traitement automatique visant à détecter la présence de liens malveillants, de virus et à l'éradiquer si possible. En cas de détection, les adresses de l'émetteur et du destinataire, l'objet du message et le type de virus détecté sont automatiquement envoyés sur une console d'administration, à des fins statistiques.

4.3. Poste de travail, bureautique et Smartphones

Un logiciel de gestion de parc informatique est utilisé et délivre un inventaire technique automatique des équipements professionnels.

Afin d'assurer la sécurité des systèmes d'information, chaque fichier fait l'objet d'un traitement automatique visant à détecter la présence de virus et à l'éradiquer si possible. En cas de détection, la localisation du fichier, son nom et le type de virus détecté sont automatiquement envoyés sur une console d'administration, à des fins statistiques et de contrôles. En cas de contamination par un virus, le poste de travail pourra être également isolé de tout réseau à distance.

En cas de perte ou de vol du matériel, des mesures particulières pourront être mises en place pour l'effacement des données.

En cas de constatation d'incidents liés au non-respect de la charte, la procédure suivante sera appliquée :

- Au premier constat, l'agent sera informé via la messagerie.
- En cas de récidive, le supérieur hiérarchique direct sera prévenu.

4.4. Supervision des accès internet

Afin d'assurer la sécurité des systèmes d'information, la supervision des systèmes d'accès Internet porte de manière globale ou individuelle sur de la collecte d'informations techniques.

4.4.1. Contrôle global.

- La liste des sites les plus visités et les temps passés sont collectés à des fins statistiques, et aussi pour optimiser le cas échéant l'accès à certains de ces sites ou catégorie de sites.
- L'accès à certains sites non autorisés en raison de leur caractère immoral, illicite ou illégal (pornographie, pédophilie, racisme, incitation à la haine raciale, révisionnisme, etc.) est filtré.

4.4.2. Filtrage Internet – Droits d'accès

Suivant le profil Utilisateur paramétré par la Direction des Systèmes d'Information, un filtrage de la navigation Internet est activé suivant l'un des deux modes suivants :

- Paramétrage standard : une liste de catégories de sites internet est accessible par l'Utilisateur pour un usage professionnel et un usage personnel raisonnable.
- Paramétrage étendu : sur demande du responsable hiérarchique, certains agents, pour assurer leur mission, pourront avoir accès à une liste étendue de sites internet.

Dans tous les cas, la consultation de sites Internet doit se faire en conformité avec les règles détaillées dans la présente Charte Informatique. Les Utilisateurs sont responsables des choix opérés dans la consultation de pages internet, et seront responsables en cas de réalisation d'activités non autorisées.

Les autorisations données pour accéder à des paramétrages plus tolérants sont révocables à tout moment en cas de non-respect des règles posées par la présente Charte.

En cas de problème mettant en péril la sécurité des Systèmes d'Information, la navigation de l'ensemble des agents sera verrouillée sur un paramétrage restreint, permettant d'assurer la continuité des services rendus par le Département.

4.4.3. Déchiffrement des flux HTTPS

Afin d'assurer la sécurité des systèmes d'information (détection des flux entrants/sortants anormaux, identification de logiciels malveillants ou protection du patrimoine informationnel), un déchiffrement automatisé des flux HTTPS est mis en œuvre.

Le déchiffrement s'applique à l'ensemble des agents du Département du Nord. Une liste de catégories de sites web non concernés par la mesure a été définie sur la base de la sensibilité des informations échangées (données bancaires, de santé, etc.).

L'analyse des traces générées ne se fait que sur la base de la détection d'un incident. Ces données seront minimisées aux champs strictement nécessaires à l'analyse d'un incident. Elles seront conservées hors environnement de production et pour une durée maximum de 6 mois.

Les données collectées lors des opérations de déchiffrement ne sont accessibles qu'au Responsable de la Sécurité des Systèmes d'Information (RSSI) et aux administrateurs habilités. En cas de nécessité d'accès à un document à caractère personnel ou privé, l'ouverture ne pourra être effectuée qu'en présence de l'intéressé ou à défaut après information de ce dernier en conformité avec les préconisations de l'ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information).

Par ailleurs, la procédure de déchiffrement des flux fait l'objet d'une déclaration librement accessible au registre du DPD.

4.5. Autres traces

Les solutions de sécurité, les outils d'authentification et les applications mises en œuvre génèrent des enregistrements ou traces utilisés pour le suivi, l'administration et le support des solutions. Ces traces peuvent être

remises aux autorités compétentes pour effectuer des recherches en cas de suspicion d'une activité malveillante pouvant porter atteinte au Département du Nord.

Une exploitation statistique des enregistrements peut être réalisée sous forme anonyme pour des motifs opérationnels. Elle consiste à établir des statistiques relatives aux connexions réalisées.

Conformément aux recommandations de la CNIL, le Département conserve les traces pendant une durée de six mois et de les archiver pendant un an sur un support indépendant.

4.6. Utilisation des traces

Un contrôle de l'utilisation des différents moyens de communication et d'information mis à la disposition des Utilisateurs est mis en place pour les différents motifs évoqués ci-dessus. Si les traces générées sont systématiques, leur utilisation est encadrée par les exigences du droit européen[3].

A ce titre, l'utilisation des traces des Utilisateurs ne peut être effectuée qu'en préservant un équilibre entre loyauté des procédés utilisés pour établir les faits reprochés tout en évitant de mettre en place une surveillance électronique automatique des agents départementaux.

Les garanties suivantes devront être mises en place par le Département pour préserver cet équilibre :

- L'agent est informé, préalablement à leur mise en place, de la possibilité du Département de prendre des mesures de surveillance de ses moyens de communication ainsi que de la mise en place préalables de telles mesures,
- L'agent doit être en mesure d'apprécier l'étendue de la surveillance opérée par le Département et le degré d'intrusion dans sa vie privée (motif de la surveillance, période de surveillance, personnes ayant accès aux données),
- Le Département avance des motifs légitimes pour justifier la surveillance des moyens de communication et l'accès à leur contenu,
- Le Département préserve des moyens proportionnés pour prouver l'atteinte à la charte,
- Le Département doit permettre à l'agent de vérifier l'exercice de ces garanties adéquates,
- Le Département conserve les traces selon les durées définies par les dispositions légales.

Par la prise de connaissance de la présente charte, les agents départementaux sont informés de la possibilité de prendre des mesures de surveillance et de leur mise en œuvre.

[3] AFFAIRE BĂRBULESCU c/ ROUMANIE, Requête n°61496/08, 5 septembre 2017), grande chambre ; CEDH, AFFAIRE LIBERT c. FRANCE, requête n°588/13, 22 février 2018)

5. NON-RESPECT ET SANCTIONS

Les cas de non-respect de la charte seront traités proportionnellement à la gravité, la récurrence et/ou au caractère intentionnel.

Un rappel au respect des dispositions de la charte informatique par l'autorité territoriale pourra être effectué dans un premier temps.

Outre les sanctions civiles et pénales auxquelles il pourrait être condamné, l'Utilisateur ne respectant pas les règles définies par la présente charte s'expose également aux sanctions disciplinaires prévues par les dispositions statutaires, à l'exception des organisations syndicales (cf point 6) et des Utilisateurs extérieurs au Département (prestataires externes). Ces derniers, outre les sanctions civiles et pénales auxquelles ils pourraient être condamnés, s'exposent également à la résiliation de leur contrat et à la fermeture des droits d'accès s'il est constaté une répétition de comportements contraires à la présente charte, ainsi qu'à l'application de toute pénalité qui pourrait être due du fait de leur faute contractuelle.

6. DISPOSITIONS PARTICULIERES D'ACCES ET D'UTILISATION DES RESSOURCES INFORMATIQUES PAR LES ORGANISATIONS SYNDICALES.

La mise en œuvre des droits syndicaux au sein du Département du Nord s'effectue dans un souci constant de garantir et d'améliorer ces droits afin de permettre un dialogue social de qualité. En raison de l'évolution des technologies de l'information et de la communication (TIC) et du droit applicable en la matière, il est nécessaire d'actualiser la partie de la charte informatique réservée aux organisations syndicales du Département du Nord

Il est rappelé que :

- L'article L113-1 du Code général de la fonction publique reconnaît aux agents départementaux le libre exercice du droit syndical ;
- les organisations syndicales assurent la représentation du personnel et ont exclusivement pour objet l'étude et la défense des droits ainsi que des intérêts matériels et moraux, tant collectifs qu'individuels, des agents ;
- nul ne peut être inquiété en raison de son affiliation ou de sa non appartenance à un syndicat ;
- les représentants des organisations syndicales ne peuvent faire l'objet d'aucune discrimination sur quelque plan que ce soit, en particulier sur celui du déroulement de leur carrière ;
- la reconnaissance du droit syndical demeurerait inefficace s'il ne s'accompagnait du droit de disposer des moyens nécessaires à son plein exercice ;
- l'exercice du droit syndical de la fonction publique territoriale rejoint celui de la fonction publique d'Etat pour certaines dispositions.

Textes spécifiques de référence

- décret n°85-397 du 3 avril 1985 relatif à l'exercice du droit syndical dans la fonction publique territoriale, notamment son article 4-1 ;
- circulaire du 20 janvier 2016 relative à l'exercice du droit syndical dans la fonction publique territoriale, notamment la section II B. Accès aux technologies de l'information et de la communication
- décret n° 2014-1319 du 4 novembre 2014 relatif aux conditions d'accès aux techniques de l'information et de la communication et à l'utilisation de certaines données par les organisations syndicales dans la fonction publique de l'Etat ;
- arrêté du 4 novembre 2014 relatif aux conditions générales d'utilisation par les organisations syndicales des technologies de l'information et de la communication dans la fonction publique de l'Etat ;
- la déclaration au registre du délégué à la protection des données

Les technologies de l'information et de la communication (TIC) sont utilisées par les organisations syndicales dans l'exercice de leurs activités. Ces TIC sont mises à leur disposition et sont constituées d'au moins, en application de l'article 2 de l'arrêté du 4 novembre 2014 susvisé :

- une adresse de messagerie électronique aux coordonnées de l'organisation syndicale,
- une page d'information syndicale spécifiquement réservée et accessible sur le site intranet du Département du Nord.

Le présent document décline pour le Département du Nord les dispositions définies par l'arrêté du 4 novembre 2014 relatif aux conditions générales d'utilisation par les organisations syndicales des TIC dans la fonction publique de l'État, applicable aux collectivités territoriales.

6.1. Cadre général

Les conditions générales d'utilisation des TIC par les organisations syndicales, définies dans la charte informatique, visent à simplifier l'action quotidienne des acteurs du dialogue social pour qu'il soit plus efficace, tout en préservant le bon fonctionnement de l'outil de travail, propriété du département du Nord.

La présente charte s'applique pour l'ensemble des organisations syndicales et pourra faire l'objet de révisions, sur l'initiative de l'autorité territoriale, le cas échéant sur proposition des organisations syndicales représentatives.

Les différents outils TIC disponibles sont les suivants :

- Matériel informatique, connexion au réseau, et accès à la messagerie électronique et aux outils de communication (messagerie instantanée, visio, téléphone fixe, téléphone portable);
- Boîtes aux lettres électroniques (BAL) institutionnelles avec adresse de messagerie pour chaque syndicat ;
- Outil de gestion des listes de diffusion pour les envois en masse de messages électroniques vers les agents ;
- Mise à disposition d'une page dédiée à chaque syndicat sur l'intranet avec la possibilité de faire des liens vers l'externe ;

Chaque organisation syndicale devra, dans la limite de l'offre technique du Département du Nord, remplir une demande sur les moyens dont elle souhaite pouvoir disposer (en s'appuyant sur l'espace Intranet réservé à cet effet).

Les organisations syndicales, ainsi que leurs membres, engagent leur responsabilité sur les informations ou prises de position qu'ils décident de rendre publiques par l'intermédiaire d'un des outils TIC.

C'est en particulier le cas dans l'hypothèse du non-respect de dispositions de nature pénale (par exemple, injure et diffamation publiques, contrefaçon, obligations imposées par la loi informatique et libertés) ou statutaires (par exemple, violation du devoir de discrétion professionnelle).

Cet espace étant mis à la disposition des organisations syndicales par le Département du Nord, l'autorité territoriale se réserve le droit de revenir vers le ou les référents des organisations syndicales ne respectant pas ce point en application de l'article 4 de l'arrêté du 14 novembre 2014 susvisé.

A défaut, l'autorité territoriale appliquera les dispositions du 6.5 de la présente charte.

6.2. Gestion des outils mis à disposition des organisations syndicales - Cadre d'utilisation

L'accès aux technologies de l'information et de la communication (TIC) au sein du Département du Nord est autorisé pour l'ensemble des organisations syndicales, dans les conditions définies ci-après par l'autorité territoriale conformément à l'article 4-1 du décret n°85-397 du 3 avril 1985 susvisé.

Chaque organisation syndicale qui sollicite une utilisation de la messagerie électronique ou du site intranet dans les conditions prévues à l'arrêté du 4 novembre 2014 et par la présente charte, désigne lors de sa demande, un ou plusieurs interlocuteurs référents, affectés à l'organisation syndicale pour lequel la messagerie électronique ou le site intranet a été créé. En cas de vacances de référent, l'organisation syndicale transmet dans un délai de 30 jours à compter du départ effectif, le nom d'au moins un nouveau référent.

A défaut, l'autorité territoriale appliquera les dispositions du 6.5 de la présente charte.

6.2.1. Le matériel informatique

L'équipement des locaux syndicaux en matériel et logiciels informatiques s'effectuera selon le même rythme et selon les mêmes modalités, notamment en termes de sécurité, que l'équipement professionnel de l'ensemble des agents.

Ces dispositions concernent les locaux mis à la disposition des organisations syndicales par l'administration en application des dispositions des articles 3 et 4 du décret n°85-397 du 3 avril 1985.

Le matériel et les logiciels fournis permettront :

- la connexion gratuite au réseau interne du Département du Nord (messagerie et intranet) et l'accès à Internet ;
- la possibilité de mise en ligne d'informations destinées aux sites syndicaux.

6.2.2. La messagerie

La messagerie permet d'émettre ou de recevoir des messages internes et externes provenant soit des services du Département du Nord, soit d'organismes ou de personnes extérieures.

Les dispositions ci-dessous déclinent celles de l'article 7 de l'arrêté du 4 novembre 2014 susvisé.

a) Création des boîtes aux lettres syndicales

Chaque organisation syndicale peut demander, via le formulaire à disposition sur intranet, la création d'une adresse électronique syndicale, en désignant nominativement un référent chargé d'assurer le suivi de la boite aux lettres. C'est cette adresse électronique qui devra être exclusivement utilisée par l'organisation syndicale pour l'envoi des messages à contenu syndical. Elle ne se substitue pas aux boîtes aux lettres professionnelles des responsables syndicaux. Les boites aux lettres syndicales seront ainsi créées par la DSI et leur suivi sera assuré par le référent désigné par l'organisation syndicale.

La boîte aux lettres syndicale est un moyen d'échanges d'informations entre un délégué syndical et :

- les autres délégués syndicaux ;
- la représentation nationale ou locale du syndicat ;
- les agents départementaux.

En raison de motifs liés à la sécurité du système d'information, l'usage d'autres messageries à des fins syndicales que celle(s) mise(s) à disposition par la collectivité est interdite. Il est également rappelé que la boîte mail professionnelle ne doit pas être utilisée pour l'envoi en nombre aux agents départementaux de communication/de messages à caractère syndical.

b) Les règles de dénomination des boîtes à lettres

Les dénominations des boites aux lettres existantes et utilisées seront conservées.

Les nouvelles demandes se conforment aux règles ci-dessous.

Les boites aux lettres syndicales sont intitulées : « *nom du syndicat* @lenord.fr »

c) Création des listes de diffusion

Chaque organisation syndicale, en application des dispositions combinées de l'article 2 du décret n° 2014-1319 du 4 novembre 2014 et 3-2 du décret n°82-447 du 28 mai 1982, sera destinataire des seules données nécessaires pour la constitution de listes d'adresses électroniques nominatives professionnelle à des fins syndicales.

Elle devra définir son besoin en termes de listes de diffusion et en fera la demande en s'adressant au service relation utilisateur de la DSI.

Le nom de chaque liste de diffusion permet d'identifier l'organisation syndicale utilisatrice et le périmètre concerné par la liste en application de l'article 8 de l'arrêté du 4 novembre susvisé. Les règles de dénomination seront les suivantes :

- toutes les listes de diffusion commenceront par le préfixe : Syndicat-dénomination du syndicat
- le suffixe portera l'information : @liste.lenord.fr

L'adresse de la liste de diffusion sera libellée de la manière suivante : « syndicat-dénomination du syndicat@liste.lenord.fr ».

Les adresses des listes de diffusion ne sont pas visibles pour les agents car les listes sont utilisées en destinataire copie cachée

(1) Mise à disposition des données

Lorsque l'organisation syndicale en aura fait la demande, elle sera destinataire des seules données nécessaires, conformément à la déclaration au registre du délégué à la protection des données (nom, prénom, service d'affectation, adresse postale professionnelle, mail professionnel, catégorie, corps, grade d'appartenance).

(2) Mise à disposition d'un outil de gestion des listes

Un outil de gestion des listes de diffusion sera mis à disposition des organisations syndicales qui en font la demande. Il s'agit de l'outil Sympa. Les interlocuteurs référents-désignés, auront par le biais de cet outil accès à la création du contenu de la liste et à la gestion de son contenu (adresse mail professionnelle).

Il est à noter que pour éviter toute possibilité d'utilisation détournée, le Département du Nord ne doit pas pouvoir exercer de contrôle sur les listes de diffusion ainsi constituées. Cette précaution est prise afin d'éviter que l'autorité territoriale puisse connaître l'opinion favorable d'un agent à une organisation syndicale voire son appartenance à celle-ci sur la base du choix opéré par cet agent quant à son acceptation ou son refus de recevoir des messages à caractère syndical.

(3) Mise à jour des listes

Cette mise à disposition des données sera effectuée une fois par an. Chaque organisation syndicale pourra alors mettre à jour ses listes de diffusion. Les nouveaux arrivants sont invités à contacter directement les OS pour s'inscrire sur les listes dans l'attente de l'actualisation annuelle.

d) Règles d'usage de la messagerie

L'usage de cette boîte aux lettres se fait sous la responsabilité du, ou des, interlocuteurs référents, de la boite aux lettres. En particulier, les règles d'accès doivent être respectées :

- mot de passe personnalisé,
- confidentialité des mots de passe,
- non-divulgation de ces mots de passe.

La messagerie ne doit pas être utilisée de façon abusive ou anormale notamment pour certaines fonctions telles que l'envoi répété de messages.

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

Il est rappelé que les impératifs techniques et de sécurité du système d'information peuvent nécessiter de contingenter les envois en nombre en application des dispositions de l'article 7 de l'arrêté du 4 novembre susvisé.

L'origine syndicale de l'envoi est mentionnée dans l'objet de chaque message électronique.

L'usage des accusés de réception et accusés de lecture est interdit.

La liberté d'accepter ou de refuser un message électronique syndical doit pouvoir s'exercer à tout moment par les agents. Elle est rappelée de manière claire et lisible dans chaque message électronique adressé par l'organisation syndicale.

Lorsque les organisations syndicales utilisent des listes de diffusion, elles devront indiquer aux destinataires des messages syndicaux qu'ils peuvent demander à tout moment à en être radiés.

Un lien de désabonnement doit être inclus dans tous les messages. Il est à noter sur ce point que la liberté des agents d'accepter ou de refuser un message électronique syndical doit pouvoir s'exercer à tout moment auprès du ou des référents de chaque organisation syndicale en application du II B. de la circulaire du 20 janvier 2016 susvisée.

Les organisations syndicales sont tenues de faire droit à ces demandes dans les plus brefs délais.

Les listes de diffusion ne peuvent pas être utilisées à d'autres fins que la diffusion d'information d'origine syndicale.

Les messages adressés à une liste de diffusion doivent être concis et adressés si possible en fin de journée afin de ne pas impacter les performances du réseau pour l'ensemble des utilisateurs.

Dans l'objectif de limiter les coûts et l'engorgement du réseau, les obligations ci-dessous devront être respectées :

- La taille totale des messages avec utilisation de liste de diffusion ne devra pas dépasser 4 Mo. Les pièces jointes ne sont pas autorisées. Au-delà, le message sera rejeté.
    - Remarque : il s'agit de la taille totale du message.
    - Pour connaître la taille d'un message, il est possible d'enregistrer le message avant de l'envoyer. Le message est alors transféré dans le dossier " brouillon " où sa taille apparaît.

6.2.3. Publication sur le site intranet du Département (article 9 de l'arrêté du 4 novembre 2014 susvisé)

Chaque organisation syndicale peut demander la mise à disposition d'une ou plusieurs pages d'information syndicale sur le site intranet du département du Nord.

L'insertion sur ces pages de liens hypertexte vers des sites syndicaux extérieurs peut être autorisée par l'autorité territoriale sur demande expresse de l'organisation. Pour rappel, tout lien hypertexte fait l'objet d'une analyse de sécurité au moment de sa consultation.

Afin de ne pas aller à l'encontre de l'expression syndicale, les propos tenus sur les pages mises à disposition des OS ne feront pas l'objet d'un contrôle a priori ; leur contenu ne fera pas l'objet d'une fixation préalable à leur communication aux agent départementaux.

Les organisations syndicales, ainsi que leurs membres, engagent leur responsabilité sur les informations ou prises de position qu'ils décident de rendre publiques par l'intermédiaire d'un des outils TIC.

C'est en particulier le cas dans l'hypothèse du non-respect de dispositions de nature pénale (par exemple, injure et diffamation publiques, contrefaçon, obligations imposées par la loi informatique et libertés) ou statutaires (par exemple, violation du devoir de discrétion professionnelle).

En cas de non-respect de ces dispositions, l'autorité territoriale reviendra vers le ou les référents des organisations territoriales concernées et le cas échéant appliquera les dispositions de l'article 6.5 de la présente charte.

6.3. Période des élections professionnelles – cas particulier

Pendant la période de six semaines précédant le jour du scrutin organisé pour le renouvellement ou la mise en place d'une ou plusieurs instances de concertation, en application de l'article 3-1 modifié du décret n°82-447 du 28 mai 1982 modifié, toute organisation syndicale dont la candidature a été reconnue recevable a accès, au sein des services dont les personnels sont concernés par le scrutin, aux mêmes technologies de l'information et de la communication et dans les mêmes conditions.

L'outil de gestion des listes sera mis à leur disposition avec les adresses de listes souhaitées dont elles devront elles-mêmes définir les critères.

Ces organisations syndicales doivent respecter l'ensemble des règles de gestion définies ci-dessus pour l'utilisation et la gestion des TIC.

Un protocole spécifique pourra être mis en place afin de prévoir les modalités de communication, dérogatoires aux dispositions de la présente charte, des organisations syndicales pendant la période électorale.

6.4. Les engagements de chaque acteur

6.4.1. Engagements des syndicats

Chaque responsable syndical qui sollicite l'utilisation de la messagerie électronique ou du site intranet s'engage à :

- désigner un ou plusieurs interlocuteurs référents pour la messagerie électronique ou le site intranet ;
- respecter les règles d'utilisation précisées précédemment ;
- respecter les dispositions de nature pénale (notamment relative aux injures et diffamation), les obligations imposées par la loi informatique et libertés ainsi que statutaires (notamment le principe de neutralité, le devoir de réserve et de discrétion professionnelle).
- signaler à l'administration les changements éventuels des interlocuteurs référents et les demandes de suppression de boîtes à lettre ; à défaut de référent, c'est le responsable du syndicat qui en fera office

- ne pas interpeller des responsables hiérarchiques par le biais de messages électroniques identiques envoyés en nombre (pétition électronique) ;
- ne pas adopter un comportement visant à engorger le réseau départemental ;
- respecter le principe de finalité des données mises à disposition pour la constitution des listes afin d'établir des listes de diffusion pour la communication syndicale ;
- informer ses membres au regard des obligations CNIL et s'assurer de la bonne déclaration des données individuelles éventuellement traitées au sein de son registre des traitements de données.

Pour rappel, les données à caractère personnel ne peuvent être recueillies et traitées que pour un usage déterminé, explicite et légitime. Un fichier constitué à des fins de communication syndicale ne peut pas être utilisé dans un autre but que celui qui a été initialement défini.

Tout détournement de finalité est passible de 5 ans d'emprisonnement, de 300 000 € d'amende (article 226-21 du Code pénal) et de sanctions administratives prononcées par la CNIL.

6.4.2. Engagements du Département du Nord

Le Département du Nord s'engage à :

- accorder, au maximum dans le mois suivant la demande écrite, l'ouverture des boîtes aux lettres syndicales si la demande est recevable ;
- intégrer les boîtes aux lettres des organisations syndicales dans l'annuaire électronique ;
- respecter la confidentialité des messages électroniques en provenance ou à destination des boîtes aux lettres syndicales (contenu, auteurs et destinataires) en application de l'article 5 de l'arrêté du 4 novembre 2014 sus-visé, dans le cadre des textes en vigueur et de la jurisprudence relative au secret de la correspondance ;
- concernant l'outil de gestion des listes de diffusion, la formation et l'accompagnement seront pris en charge directement par la mise en place de tutoriels.
- fournir une assistance technique

6.5. Mesures applicables en cas de non-respect de la charte

Tout usage qui irait en contradiction avec les dispositions de la présente charte informatique pourra faire l'objet de mesure(s) temporaire(s) ou définitive(s) telles que la suspension ou la suppression de tout ou partie des TIC mises à disposition de l'organisation syndicale et précisées à l'article 6.1.

Un rappel au respect des dispositions de la charte informatique par l'autorité territoriale sera effectué dans un premier temps. Si ce rappel n'est pas suivi d'effet (persistance de l'usage non conforme au terme du délai indiqué dans le courrier de rappel ou répétition de cet usage), l'autorité territoriale pourra suspendre les accès et/ou les fonctionnalités des TIC concernées.

La mesure de suspension aura pour objectif de mettre fin au non-respect de la/des règle(s) enfreinte(s). Le rétablissement des accès aux TIC sera opéré dès la mise en conformité avec les dispositions de la charte informatique.

En cas de non-respect successifs et/ou multiples et /ou récurrents des règles de la présente charte par une OS, il pourra être décidé la suppression de la mise à disposition de l'organisation syndicale de la/des TIC ayant été utilisée(s) de manière irrégulière.

En cas de publication, via l'intranet, contenant des propos considérés comme étant à caractère diffamant ou injurieux et/ou ne respectant pas le principe de neutralité religieuse et politique du service public et/ou le devoir de réserve restreint des organisations syndicales, il sera demandé à l'organisation syndicale le retrait de la publication litigieuse dans un délai indiqué et déterminé en fonction du contenu de la publication. Dans l'hypothèse où cette demande ne serait pas suivie d'effet, l'accès à cette publication sera supprimé.

Ces mesures pourront être contestées devant le tribunal administratif de Lille.

7. STATUT DE LA CHARTE

La charte est juridiquement opposable à l'ensemble des utilisateurs et remplace l'ensemble des versions antérieures

Les règles et obligations ci-dessus énoncées s'appliquent à tout Utilisateur autorisé, à l'exception des élus qui sont régis par une charte dédiée, à utiliser les ressources du Système Informatique et les Systèmes d'Information du Département du Nord.

Ces derniers comprennent toutes les ressources informatiques et les moyens de communication du Département du Nord et notamment les serveurs, stations de travail, périphériques, et équipements mobiles et téléphonie propriétés du Département du Nord, qu'ils soient connectés ou non aux réseaux du Département du Nord.

Le respect des règles définies par la présente Charte s'étend également à l'utilisation des systèmes informatiques d'organismes extérieurs au Département du Nord, accessibles par l'intermédiaire des réseaux du Département du Nord, par exemple le réseau Internet.

La présente Charte pourra faire l'objet d'amendements de la part du Département du Nord.

8. DEFINITIONS

- **Activités autorisées :** Lors de l'attribution des Droits d'accès, l'Utilisateur a accès à des activités autorisées définies dans le cadre de son activité.

- **Activités non autorisées :** Elles regroupent les activités légales non nécessaires à l'activité de l'agent et les activités illégales punies par le droit français (pédophilie, pornographie, racisme, discrimination…).

- **Administrateur :** Un administrateur désigne toute personne qui a pour rôle d'assurer le bon fonctionnement du Système d'Information de la collectivité. Pour mener à bien sa mission, il dispose de pouvoirs et de droits d'accès étendus sur le Système Informatique. Cela peut concerner les membres de la Direction des Services Informatiques ou les Services support métiers. Les administrateurs du système d'information opèrent sous la responsabilité de l'Autorité Départementale

- **ANSSI** : L'Agence Nationale de la Sécurité des Systèmes d'Information est un service français rattaché au secrétariat général de la Défense et de la Sécurité nationale (SGDSN). Elle assure la mission d'autorité nationale en matière de sécurité des systèmes d'information. À ce titre, elle est chargée de proposer les règles à appliquer pour la protection des systèmes d'information de l'État et de vérifier l'application des mesures adoptées. Elle apporte son expertise et son assistance technique aux administrations et aux entreprises. Dans le domaine de la défense des systèmes d'information, elle assure un service de veille, de détection, d'alerte et de réaction aux attaques informatiques, notamment sur les réseaux de l'État.

- **Autorité Départementale :** selon le contexte, ce terme peut désigner :

  - le Département du Nord, personne morale de droit public propriétaire du système d'information pris globalement (par exemple dans les articles 3.1.4 et 3.1.6)
  - ou, le plus souvent, la personne juridiquement responsable des systèmes d'information du Département et habilitée à prendre des décisions concernant leur utilisation (par exemple dans les articles 3.1.1, 3.1.5, 4.2 ou 8).

    Dans ce cas, il s'agit soit de l'autorité territoriale elle-même, chef des services départementaux, soit d'une personne délégataire de fonction ou délégataire de signature.

- **Bande passante :** Elle est coûteuse et limitée. Elle définit la quantité d'informations qui peut circuler en même temps sur le réseau. Plus il y a d'Utilisateurs qui utilisent le réseau en même temps, plus les performances du réseau décroissent. Certains sites Web proposant des animations graphiques lourdes à charger peuvent provoquer des blocages ou des temps d'accès réduits auprès des autres Utilisateurs.

- **Chiffrement :** Fait de chiffrer, de coder un texte pour qu'il ne soit lisible que par une personne connaissant le code de chiffrage (Crypter est souvent employé, mais il s'agit d'un anglicisme).

- **Base de Registre** : désigne la base de données utilisée par le système d'exploitation et contenant les données de configuration du système d'exploitation et des autres logiciels installés devant s'y connecter. La Base de Registre assure la cohésion et la stabilité du système d'exploitation.

- **Code malveillant, virus, malware (troyens,…) :** Un code malveillant est un logiciel qui a pour effet, recherché ou non, de nuire en perturbant plus ou moins gravement le fonctionnement de l'ordinateur infecté. Il peut se répandre à travers tout moyen d'échange de données numériques comme l'Internet, mais aussi les clés USB, les smartphones, les tablettes, etc.,

- **Confidentialité :** Fait d'assurer que l'information n'est accessible qu'aux personnes autorisées. La confidentialité est une obligation légale pour les données personnelles,

- **Demande d'accès :** Dans le cas où un agent ne disposerait pas de ses informations, Nom d'utilisateur et Mot de passe, il doit en faire la demande à son responsable hiérarchique ou à son référent informatique.

- **Déchiffrement de flux HTTPS :** Opération qui consiste à déchiffrer des communications chiffrées à l'aide du protocole HTTPS.

- **Délégué à la Protection des Données (DPD) :** Le Délégué à la Protection des Données est la personne chargée de la protection des données personnelles au sein d'une organisation.

- **Direction des Systèmes d'Information :** La Direction des Systèmes d'Information est la division de l'Autorité Départementale responsable du fonctionnement et de la sécurité des Systèmes d'Information. Elle dispose des droits les plus étendus pour contrôler l'utilisation faite du Système Informatique par les Utilisateurs. La Direction des Systèmes d'Information opère sous la responsabilité de l'Autorité Départementale.

- **Disponibilité :** Fait d'assurer que les ressources nécessaires à la fourniture d'un service du Système Informatique sont accessibles lorsqu'elles sont sollicitées,

- **Donnée personnelle :** Toute information relative à une personne physique identifiée ou qui peut être identifiée, directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres.

- **Droits d'accès :** Les droits d'accès définissent ce à quoi il est possible d'accéder avec l'identifiant et le mot de passe. Ils sont différents d'un Utilisateur à l'autre selon le poste qu'il occupe et ses fonctions.

- **Habilitation :** Lors de l'attribution des Droits d'accès, l'Utilisateur a accès à des Activités autorisées définies dans le cadre de ses missions.

- **Hacking :** désigne un ensemble de techniques permettant d'exploiter les possibilités, failles et vulnérabilités d'un élément ou d'un groupe d'éléments matériels ou humains.

- **HyperText Transfer Protocol (HTTP) :** HTTP est un protocole de communication développé pour le web.

- **HyperText Transfer Protocol Secure (HTTPS) :** HTTPS est une version chiffrée du protocole HTTP.

- **Intégrité :** Fait d'assurer que l'information est fiable et ne peut subir aucune altération volontaire ou involontaire,

- **Incident :** « Tout évènement qui ne fait pas partie du fonctionnement standard d'un service et qui cause, ou peut causer, une interruption ou une diminution de la qualité de ce service.[4] » Un incident peut être l'infection virale d'un poste de travail comme le vol d'un smartphone.

- **Log de connexion, trace, journal de connexion :** Données informatiques créées à chaque utilisation des ressources d'un réseau interne ou externe (Internet par exemple). Ces données contiennent toutes les informations utiles sur les différentes étapes de la manipulation. En cas de problème il devient plus facile d'en repérer l'origine,

- **Mail, Message électronique, Courriel :** Désigne la notion de courrier stocké et véhiculé de manière électronique,

- **Identifiant et Mot de passe :** Chaque Utilisateur dispose d'un identifiant et d'un mot de passe lui permettant de s'authentifier sur le réseau. Ces informations sont personnelles et confidentielles. Pour se connecter au service à distance de la messagerie, le compte de l'Utilisateur est identique à son adresse de messagerie (ex. jean.durant@lenord.fr). Le mot de passe est donné par la Direction des Systèmes d'Information et doit être modifié par l'Utilisateur à la première connexion (se rapprocher du service relation utilisateur via le numéro 03.59.73.58.58 ou par mail assistance-informatique-35858@lenord.fr).

- **Phishing ou Hameçonnage** : Technique de fraude par courriel, basée sur l'usurpation d'identité de banques ou d'entreprises commerciales, afin d'obtenir de l'Utilisateur des renseignements confidentiels (mot de passe, numéros de cartes de crédit, par exemple).

---

[4] Définition d'un incident selon le référentiel de bonnes pratiques de management des Systèmes d'Information ITIL (Information Technology Infrastructure Library).

- **Poste de travail** : Un poste de travail désigne l'ordinateur de bureau, l'ordinateur portable, la tablette, le smartphone, le téléphone utilisé par un agent dans le cadre de son activité ainsi que leurs périphériques.

- **Protocole** : Un protocole de communication est un système de règles permettant à deux ou plusieurs entités d'un système de communication de se transmettre des données sur un réseau. Les protocoles définissent ainsi la syntaxe, la sémantique et les modalités opératoires (émission, réception, synchronisation, gestion des erreurs, etc.) d'une communication.

- **Référents informatiques :** Les référents informatiques sont les relais entre les services et la Direction des systèmes d'informations. Ils s'assurent notamment que chaque agent dispose des moyens techniques pour accéder au réseau. Chaque agent peut connaître les coordonnées de son référent en se rapprochant de sa hiérarchie.

- **Registre du DPD** : liste des traitements de données à caractère personnel mis en œuvre au sein du département du Nord.

- **Réseau :** Le réseau représente les moyens mis en place par le Département du Nord pour relier les Utilisateurs entre eux, au système informatique et éventuellement à Internet. Ses performances décroissent avec l'augmentation du trafic (voir « Bande passante »).

- **Ressource :** composant matériel (ordinateur, imprimante, serveur,…) ou immatériel (application, base de données, procédures,…) contribuant au traitement de l'Information,

- **Responsable de la Sécurité des Systèmes d'Information (RSSI) :** Le RSSI est chargé de la définition et de la mise en œuvre de la politique de sécurité des systèmes d'information qui consiste à garantir la disponibilité, la sécurité, et l'intégrité du système d'information et des données. Il opère sous la responsabilité de l'Autorité Départementale.

- **Responsable des traitements :** Le responsable du traitement de données à caractère personnel est la personne, l'autorité publique, le service ou l'organisme qui détermine ses finalités (à quoi il va servir) et ses moyens (selon quelles modalités)

- **Service d'Accès à Distance de la Messagerie :** Ce service fourni aux agents dûment habilités, permet l'accès à la messagerie internet du Département du Nord depuis un poste de travail situé en dehors des locaux du Département du Nord en utilisant une connexion par l'Internet.

- **Services Internet :** Ils désignent la mise à disposition par les serveurs locaux ou distants de moyens d'échanges et d'informations diverses : Web (http ://…), Messagerie, FTP (transfert de fichiers), SMTP (e-mail/Courrier électronique), Discussion en temps réel, forums de discussion, groupe de news…

- **Shareware :** Un shareware est un logiciel d'éditeur, normalement payant, mais qui peut être offert au téléchargement par ce dernier dans une version temporairement gratuite ou avec des fonctionnalités limitées. Après cette période d'essai, l'utilisateur doit rétribuer l'éditeur s'il veut continuer à utiliser le logiciel ou avoir accès à la version complète de ce logiciel.

- **Smartphone :** Un smartphone est un téléphone mobile disposant aussi des fonctions d'un assistant numérique personnel. Il peut aussi fournir les fonctionnalités d'agenda, de calendrier, de navigation Web, de consultation de courrier électronique, de messagerie instantanée, etc.

- **Spam, pourriel :** Le spam est l'envoi massif, et parfois répété, de courriers électroniques non sollicités, à des personnes avec lesquelles l'expéditeur n'a jamais eu de contact et dont il a capté l'adresse électronique de façon irrégulière,

- **Système d'authentification :** L'authentification consiste, pour un système informatique, à effectuer la vérification de l'identité d'une personne, qui s'y connecte. Un système d'authentification consiste en l'ensemble des outils et procédures visant à valider les authentifications,

- **Système de messagerie, Messagerie électronique :** Ensemble de solutions permettant à un message électronique d'être véhiculé, stocké et consulté par l'Utilisateur,

- **Système d'Information :** Un système d'information est un ensemble organisé de ressources (matériels, logiciels, personnel, données et procédures) qui permet de collecter, regrouper, classifier, traiter et diffuser de l'information sur un environnement donné.

- **Système Informatique et ressources informatiques :** Ces termes regroupent l'ensemble des ressources techniques (matériel, logiciel,...), mises à la disposition des agents par la Direction des Systèmes d'Information du Département du Nord, permettant d'acquérir, de stocker, de transformer et de communiquer des informations. Il regroupe notamment : les serveurs départementaux, les postes de travail, les postes en libre-service, les connexions Internet, les périphériques (disques durs, imprimantes, etc.) ainsi que les ordinateurs portables, organiseurs électroniques, périphériques amovible (clé USB), smartphone,...

- **Télétravail** : Le télétravail désigne toute forme d'organisation du travail dans laquelle les fonctions qui auraient pu être exercées par un agent dans les locaux de son employeur sont réalisées hors de ces locaux de façon régulière et volontaire en utilisant les technologies de l'information et de la communication.

- **Traçabilité :** Fait d'assurer que les modifications apportées à l'Information sont enregistrées et peuvent être analysées dans le futur.

- **Traitement de données à caractère personnel :** Toute opération ou tout ensemble d'opérations portant sur des données à caractère personnel et notamment, la collecte, l'enregistrement, la transmission, la consultation ou la communication.

- **Utilisateur :** Agent de la collectivité, stagiaire, organisations syndicales, prestataire ou toute personne à laquelle un quelconque droit d'accès à tout ou partie des Systèmes d'Information du Département du Nord est accordé.

- **Virus et Antivirus :** Le virus est un programme informatique créé en général pour être diffusé automatiquement sur Internet (ou sur une clé USB...) et destiné à détruire tout ou partie des informations présentes sur un ordinateur, un smartphone ou un réseau informatique. Les antivirus sont des programmes destinés à empêcher les virus de se propager mais il est possible que de nouveaux virus ne soient pas reconnus par cette protection. On peut éviter la propagation des virus en évitant d'ouvrir des pièces jointes estimées suspectes provenant de personnes d'origine inconnue.

ANNEXE 3 :

Clauses pour les contrats avec les sous-traitants du Département

Préambule

Une Donnée à Caractère Personnel désigne toute information se rapportant à une personne physique identifiée ou identifiable, directement ou indirectement.

Un traitement est « toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données ou des ensembles de données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction ».

Le responsable de traitement est la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui, seul ou conjointement avec d'autres (les responsables conjoints de traitement), détermine les finalités et les moyens du traitement.

Le sous-traitant est un organisme traitant des Données à Caractère Personnel pour le compte, sur instruction et sous l'autorité d'un responsable de traitement.

Le cycle de vie des données se définit sur deux périodes consécutives :

- A la fin de leur durée d'utilité courante (DUC), lorsque les données ne sont plus d'utilisation quotidienne par le service, elles peuvent faire l'objet d'un préarchivage.
- A la fin de leur durée d'utilité administrative (DUA), lorsque les données n'ont plus d'utilité administrative et juridique, elles font l'objet d'un archivage ou d'une suppression

Ces durées de conservation sont définies dans les référentiels d'archivage ou en lien avec le service des archives.

A. Objet

Les présentes clauses ont pour objet de définir les conditions dans lesquelles le sous-traitant s'engage à effectuer pour le compte du responsable de traitement les opérations de traitement de données à caractère personnel définies ci-après.
Dans le cadre de leurs relations contractuelles, les parties s'engagent à respecter la réglementation en vigueur applicable au traitement de données à caractère personnel et, en particulier, le règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 (ci-après, « ***le règlement européen sur la protection des données*** ») ainsi que la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés (ci-après la « ***loi informatique et libertés*** »).

B. Description du traitement faisant l'objet de la sous-traitance

Le sous-traitant est autorisé à traiter pour le compte du responsable de traitement les données à caractère personnel nécessaires pour fournir le ou les service(s) suivant(s) : réalisation des actions menées par l'association Norsenior destinées à améliorer la qualité de vie de ses adhérents, retraités du Département du Nord.

La nature des opérations réalisées sur les données est la collecte, l'enregistrement, l'organisation, la conservation, l'extraction, la consultation, l'utilisation et la destruction.

La ou les finalité(s) du traitement sont :

- Améliorer la qualité de vie de ses adhérents, tant sur le plan moral que matériel ;
- Favoriser le développement personnel de ses membres dans les domaines culturel, sportif et touristique ;
- Encourager des actions et activités visant à maintenir les liens sociaux entre adhérents, afin de préserver leur dynamisme et leur intégration ;
- Collaborer avec d'autres structures poursuivant des objectifs similaires, telles que le Comité des Œuvres Sociales (COS).

Les données à caractère personnel traitées sont les données des agents retraités du Département du Nord.

Les catégories de personnes concernées sont : nom, prénom, adresse postale, numéros de téléphone fixe et/ou portable, adresse mail personnelle.

Pour l'exécution du service objet du présent marché, le responsable de traitement met à la disposition du sous-traitant les données identifiés plus haut.

Les durées de conservation des données (DUC, DUA) et le sort des données définis en accord avec le Département du Nord sont : conservation le temps d'adhésion à l'association Norsenior.

Dans le cas où le sous-traitant héberge des données de santé, l'hébergement qui sera proposé au Département du Nord devra être en conformité avec les dispositions de **l'article L1111-8 du code de la santé publique**. Sont entendues comme données de santé, l'ensemble des données se rapportant à l'état de santé d'une personne concernée qui révèlent des informations sur l'état de santé physique ou mentale passé, présent ou futur de la personne concernée.

C. Obligations du sous-traitant vis-à-vis du responsable de traitement

Le sous-traitant s'engage à :

1. Traiter les données uniquement pour la ou les seule(s) finalité(s) qui fait/font l'objet de la sous-traitance

2. Traiter les données conformément aux instructions documentées du responsable de traitement figurant dans le présent contrat

Si le sous-traitant considère qu'une instruction constitue une violation du règlement européen sur la protection des données ou de toute autre disposition du droit de l'Union ou du droit des Etats membres relative à la protection des données, il en **informe immédiatement** le responsable de traitement. En outre, si le sous-traitant est tenu de procéder à un transfert de données vers un pays tiers ou à une organisation internationale, en vertu du droit de l'Union ou du droit de l'Etat membre auquel il est soumis, il doit informer le responsable du traitement de cette obligation juridique avant le traitement, sauf si le droit concerné interdit une telle information pour des motifs importants d'intérêt public.

3. Garantir la confidentialité des données à caractère personnel traitées dans le cadre du présent contrat

4. Veiller à ce que les personnes autorisées à traiter les données à caractère personnel en vertu du présent contrat :

- s'engagent à respecter la **confidentialité** ou soient soumises à une obligation légale appropriée de confidentialité
- reçoivent la **formation** nécessaire en matière de protection des données à caractère personnel.

5. Prendre en compte, s'agissant de ses outils, produits, applications ou services, les principes de protection des données dès la conception et de protection des données par défaut

6. Renseigner le Département sur la sous-traitance envers des tiers

Le sous-traitant peut faire appel à un autre sous-traitant (ci-après, « ***le sous-traitant ultérieur*** ») pour mener des activités de traitement spécifiques. Dans ce cas, il informe préalablement et par écrit (avec accusé réception) le responsable de traitement de tout changement envisagé concernant l'ajout ou le remplacement d'autres sous-traitants. Cette information doit indiquer clairement les activités de traitement sous-traitées, l'identité et les coordonnées du sous-traitant et les dates du contrat de sous-traitance.
Le responsable de traitement dispose d'un délai maximum de 21 jours à compter de la date de réception de cette information pour présenter ses objections. Cette sous-traitance ne peut être effectuée que si le responsable de traitement n'a pas émis d'objection pendant le délai convenu.

Le sous-traitant ultérieur est tenu de respecter les obligations du présent contrat pour le compte et selon les instructions du responsable de traitement. Il appartient au sous-traitant initial de s'assurer que le sous-traitant ultérieur présente les mêmes garanties suffisantes quant à la mise en œuvre de mesures techniques et organisationnelles appropriées de manière à ce que le traitement réponde aux exigences du règlement européen sur la protection des données. Si le sous-traitant ultérieur ne remplit pas ses obligations en matière de protection des données, le sous-traitant initial demeure pleinement responsable devant le responsable de traitement de l'exécution par l'autre sous-traitant de ses obligations.

7. Prendre en compte le droit d'information des personnes concernées

Il appartient au responsable de traitement de fournir l'information aux personnes concernées par les opérations de traitement au moment de la collecte des données.

8. Veiller à l'exercice des droits des personnes

Dans la mesure du possible, le sous-traitant doit aider le responsable de traitement à s'acquitter de son obligation de donner suite aux demandes d'exercice des droits des personnes concernées : droit d'accès, de rectification, d'effacement et d'opposition, droit à la limitation du traitement, droit à la portabilité des données, droit de ne pas faire l'objet d'une décision individuelle automatisée (y compris le profilage).

Le sous-traitant doit répondre, au nom et pour le compte du responsable de traitement et dans les délais prévus par le règlement européen sur la protection des données aux demandes des personnes.
Le sous-traitant informera le délégué à la protection des données de toute demande de droit d'accès, à l'adresse suivante : dpd@lenord.fr.

9. Notifier les violations de données à caractère personnel

Le sous-traitant notifie au responsable de traitement toute violation de données à caractère personnel dans les meilleurs délais après en avoir pris connaissance, à l'adresse mail suivante : dpd@lenord.fr. Une justification de ces délais de notification devra être apportée par le sous-traitant afin que le responsable de traitement puisse satisfaire à ses obligations au titre de l'article 33 du Règlement (UE) 2016/679 du Parlement Européen et du Conseil du 27 avril 2016.

10. Aider le Département à respecter ses obligations relatives à la protection des données

Le sous-traitant aide le responsable de traitement pour la réalisation d'analyses d'impact relatives à la protection des données.
Le sous-traitant aide le responsable de traitement pour la réalisation de la consultation préalable de l'autorité de contrôle.

11. Mettre en œuvre des mesures de sécurité

Le sous-traitant s'engage à mettre en œuvre les mesures de sécurité visant apporter une protection suffisante des données à caractère personnel.

Les mesures mises en œuvre par le sous-traitant doivent être adaptées à la sécurité des données confiées. Le sous-traitant détaillera les mesures de protection des données à caractère personnel mises en œuvre au sein de son organisation, le cas échéant parmi les mesures suivantes :

- **l'anonymisation des données** : description des mécanismes d'anonymisation, des garanties qu'ils apportent contre une ré identification éventuelle et à quelle fin ils sont mis en œuvre.

- **le cloisonnement de données** : description des méthodes utilisées pour cloisonner le traitement chez le sous-traitant.

- **le contrôle des accès logiques** : description de la manière dont les profils utilisateurs sont définis et attribués. Il conviendra de détailler les moyens d'authentification mis en œuvre en précisant, le cas échéant les règles applicables aux mots de passe (longueur minimale, structure obligatoire, durée de validité, nombre de tentatives infructueuses avant blocage du compte, etc.).

- **la politique de journalisation** : description de la politique de journalisation des événements et de conservation des traces qui en résultent.

- **la politique d'archivage** : description de la politique de conservation et gestion d'archives électroniques contenant des données à caractère personnel mise en œuvre pour garantir leur intégrité, leur authenticité, leur accessibilité et leur lisibilité, pendant toute la durée nécessaire.

- **la politique de sécurisation des documents papiers** : description de la sécurisation de la gestion des documents papiers (de l'impression au stockage jusqu'à la destruction et aux échanges de documents).

- **la politique de minimalisation des données collectées** : la sensibilité des données peut être réduite à l'aide des méthodes suivantes : filtrage et retrait, réduction de la sensibilité par transformation, réduction du caractère identifiant des données, réduction de l'accumulation de données, restriction de l'accès aux données.

12. Veiller au sort des données

a) Les fonctionnalités

L'application doit disposer de fonctionnalités suffisantes pour mettre en place le cycle de vie des données et limiter la durée de conservation dans l'application.
A minima, les fonctionnalités attendues sont :

- La réalisation d'export de données dans un format structuré exploitable et ouvert (XML, csv…)
- La suppression de données/documents.

Le sous-traitant précisera également si l'application est en capacité de mettre en œuvre les opérations suivantes :

- Paramétrer la durée de conservation et le sort final des différentes catégories de données/documents, dans le respect des règles applicables
- Mettre en œuvre des traitements de restriction d'accès à la fin de leur durée d'utilité courante (DUC)
- Générer un export au format SEDA (Standard d'Echange de Données pour l'Archivage)
- Définir un périmètre de mise en œuvre des opérations grâce à des fonctionnalités de requêtes multicritères et de « marquage » des données/documents (à titre d'exemple : effectuer plusieurs traitements successifs sur les données/documents d'une personne, d'un ensemble de personnes ou l'ensemble de la base, pour un intervalle de dates et un périmètre géographique donnés)
- Opérer des contrôles sur les traitements avant leur mise en œuvre et, le cas échéant, de permettre des modifications sur le périmètre du traitement et la saisie de métadonnées complémentaires
- Tracer les traitements dans le journal des événements
- Produire un rapport sur les traitements d'export et de purge effectués dans l'application (a minima : date du traitement, périmètre, volume concerné).

b) Les traitements

Le sous-traitant précisera également s'il est en capacité de mettre en œuvre les traitements suivants, selon les instructions du responsable de traitement :

<u>Au terme de la durée de conservation des données définie</u> :

- Restreindre l'accès aux données à l'issue de la durée d'utilité courante (DUC)
- Extraire et transférer tout ou partie des données en vue de leur archivage intermédiaire et/ou définitif
- Supprimer tout ou partie des données après accord des Archives départementales.

<u>Lorsqu'il est mis fin au traitement des données</u> :

- Transférer les données au nouveau responsable de traitement désigné par le responsable de traitement
- Extraire et transférer tout ou partie des données en vue de leur archivage intermédiaire définitif

- Supprimer tout ou partie des données après accord des Archives Départementales.

Le transfert doit s'accompagner de la suppression de toutes les copies existantes dans les systèmes d'information du sous-traitant du traitement. Une fois supprimées, il doit justifier par écrit de la destruction des données.

13. Communiquer les coordonnées de son délégué à la protection des données

Le sous-traitant communique au responsable de traitement **le nom et les coordonnées de son Délégué à la Protection des Données**, s'il en a désigné un conformément à l'article 37 du règlement européen sur la protection des données.

14. Tenir un registre d'activités de traitement de données

Le sous-traitant déclare **tenir par écrit un registre** de toutes les catégories d'activités de traitement effectuées pour le compte du responsable de traitement comprenant :

- Le nom et les coordonnées du responsable de traitement pour le compte duquel il agit, des éventuels sous-traitants et, le cas échéant, du délégué à la protection des données ;
- Les catégories de traitements effectués pour le compte du responsable du traitement ;
- Le cas échéant, les transferts de données à caractère personnel vers un pays tiers ou à une organisation internationale, y compris l'identification de ce pays tiers ou de cette organisation internationale et, dans le cas des transferts visés à l'article 49, paragraphe 1, deuxième alinéa du règlement européen sur la protection des données, les documents attestant de l'existence de garanties appropriées ;
- Dans la mesure du possible, une description générale des mesures de sécurité techniques et organisationnelles, y compris entre autres, selon les besoins :
    - La pseudonymisation et le chiffrement des données à caractère personnel ;
    - Des moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et des services de traitement ;
    - Des moyens permettant de rétablir la disponibilité des données à caractère personnel et l'accès à celles-ci dans des délais appropriés en cas d'incident physique ou technique ;
    - Une procédure visant à tester, à analyser et à évaluer régulièrement l'efficacité des mesures techniques et organisationnelles pour assurer la sécurité du traitement.

15. Mettre à disposition la documentation démontrant le respect des obligations

Le sous-traitant met à la disposition du responsable de traitement la **documentation nécessaire pour démontrer le respect de toutes ses obligations** et pour permettre la réalisation d'audits, y compris des inspections, par le responsable du traitement ou un autre auditeur qu'il a mandaté, et contribuer à ces audits. Ces audits ne pourront être réalisés qu'une (1) fois par année civile maximum, sauf pour les contrôles d'audit liés à l'audit initial. Le responsable de traitement devra conserver à sa charge tous les frais et coûts engendrés par la réalisation de ces audits à l'exception de la contribution du sous-traitant à l'audit prévue à l'article 28 3. h) du RGPD.

Les audits seront réalisés exclusivement par la société retenue par le responsable de traitement dans le cadre de son marché d'audit. Si cet auditeur venait à être en concurrence avec le sous-traitant, une concertation serait mise en œuvre avant de débuter les opérations d'audit.
Enfin, le responsable de traitement devra avertir par écrit le sous-traitant du déclenchement de l'audit au minimum dix (10) jours ouvrés à l'avance et devra décrire précisément le périmètre de l'audit.

D. Obligations du responsable de traitement vis-à-vis du sous-traitant

Le responsable de traitement s'engage à :

1. **Fournir au sous-traitant les données visées au B des présentes clauses**

2. **Documenter par écrit toute instruction concernant le traitement des données par le sous-traitant**

3. **Veiller, au préalable et pendant toute la durée du traitement, au respect des obligations prévues par le règlement européen sur la protection des données de la part du sous-traitant**

4. **Superviser le traitement, y compris réaliser les audits et les inspections, auprès du sous-traitant**

5. **Respecter ses obligations règlementaires relatives à la gestion du cycle de vie et à l'archivage des données.**

RAPPORT N° DRH/2025/175

COMMISSION PERMANENTE
Réunion du 30 juin 2025

OBJET : Actualisation de la convention entre l'association NORSENIORS et le Département du Nord.

Dans le cadre de sa politique sociale en faveur de ses agents, le Département du Nord a signé en 2012 une convention avec l'association NORSENIORS, structure à but non lucratif régie par la loi de 1901. Cette association a pour mission de proposer des prestations sociales destinées aux agents retraités du Département. Ses objectifs principaux sont les suivants :

- améliorer la qualité de vie de ses adhérents, tant sur le plan moral que matériel ;
- favoriser le développement personnel de ses membres dans les domaines culturel, sportif et touristique ;
- encourager des actions et activités visant à maintenir les liens sociaux entre adhérents, afin de préserver leur dynamisme et leur intégration ;
- collaborer avec d'autres structures poursuivant des objectifs similaires, telles que le Comité des Œuvres Sociales (COS).

À ce titre, l'association bénéficie de divers avantages en nature, notamment la mise à disposition de locaux, de matériel informatique et de services bureautiques. Elle perçoit également une subvention annuelle d'un montant de 2 000 €.

L'article 70 de la loi du 19 février 2007 établit le principe de la mise en œuvre d'une action sociale par les collectivités territoriales au bénéfice de leurs agents. Dans le respect du principe de libre administration, la loi confie à chaque collectivité le soin de déterminer le type de prestations, leur montant et leurs modalités de mise en œuvre. L'assemblée délibérante décide ainsi librement des modalités de mise en œuvre de l'action sociale, soit en la gérant directement, soit en la confiant à un ou plusieurs prestataires.

Elle confie ainsi à l'assemblée délibérante le soin de fixer le périmètre des actions, c'est-à-dire la nature des prestations définies par l'article L.731-3 du CGFP, que la collectivité entend engager à ce titre ainsi que le montant des dépenses consacrées à l'action sociale, qui relèvent des dépenses obligatoires des collectivités locales (art. 71 - Loi 19/02/2007 et art. L2321-2 CGCT).

Le Département du Nord mène historiquement une politique d'action sociale plutôt volontariste dépassant largement le cadre de l'action sociale réglementée.

Il est proposé à la Commission permanente :

- d'autoriser l'association NORSENIORS à mener conformément à ses statuts et dans le respect des termes de la convention ci-jointe en annexe toutes actions destinées à améliorer la qualité de vie des retraités du Département du Nord ;

- de délimiter le périmètre d'action de l'Association, dans les conditions décrites au rapport et selon les principes suivants :

  o Les actions organisées sont exclusivement à destination de l'ensemble des agents départementaux en retraite y compris les assistants familiaux ;

  o Les actions organisées par l'Association doivent être complémentaires et non similaires à celles mises en œuvre par le COS au titre de la délégation donnée par le Département du Nord pour la réalisation de prestations sociales à destination de l'ensemble des agents y compris des agents retraités

- d'autoriser Monsieur le Président à signer la convention de fonctionnement, entre le Département du Nord et l'association NORSENIORS, dans les termes du projet joint en annexe.

Jean-Luc DETAVERNIER
Vice-Président