Charte des usages des Systèmes d'Information

Version janvier 2019

Table des matières

Préambule 3
ARTICLE 1 : DEFINITIONS 4
ARTICLE 2 : OBJET 6
ARTICLE 3 : CHAMP D'APPLICATION 7
ARTICLE 4 : OPPOSABILITE 7
ARTICLE 5 : CONFIDENTIALITE 8
ARTICLE 6 : CONDITIONS D'UTILISATION DES RESSOURCES 12
ARTICLE 7 : SECURITE 15
ARTICLE 8 : CONTROLE – TRACABILITE – FILTRAGE 17
ARTICLE 9 : PATRIMOINE INFORMATIONNEL 20
ARTICLE 10 : RESSOURCES UTILISEES 22
ARTICLE 11 : ACCES AUX RESSOURCES DES UTILISATEURS EN CAS D'ABSENCES ET DE DEPARTS 32
ARTICLE 12 : RESPONSABILITE DE L'UTILISATEUR 33
ARTICLE 13 : CONVENTION DE PREUVE 33
ARTICLE 14 : LOI ET REGLEMENTATION APPLICABLE 34
ARTICLE 15 : DROIT À LA DÉCONNEXION 35
ARTICLE 16 : ENTREE EN VIGUEUR 35

Préambule

Le Groupement Les Mousquetaires bénéficie d'une infrastructure informatique très élaborée par le biais de sa filiale la STIME.

Cette infrastructure informatique propose de nombreux services parmi lesquels certains sont de nature à apporter aux Utilisateurs du Groupement Les Mousquetaires (ci-après dénommé le Groupement) une aide précieuse dans le cadre de l'exercice de leurs activités professionnelles et nécessaires à l'accomplissement de leurs missions.

Ainsi, chaque société du Groupement peut mettre à la disposition de ses collaborateurs des « Ressources » appropriées telles que, notamment :

- des équipements informatiques (PC, PC portable, smartphone, tablettes, …),
- des applications bureautiques (logiciels, applications mobiles, …),
- des outils collaboratifs, une messagerie électronique permettant d'échanger courriers et Documents (E-mail, …),
- l'Intranet sur lequel sont mises à disposition de l'ensemble des Utilisateurs des Informations spécifiques sur le Groupement,
- l'Internet par lequel sont consultées, mises à disposition, téléchargées, transférées, échangées des Informations numériques.

Ces Ressources font partie du patrimoine matériel et informationnel du Groupement.

Les dispositions énoncées dans cette Charte sont capitales pour le Groupement ainsi que pour l'ensemble des sociétés qui le compose.

En vue de maintenir un environnement de travail professionnel et de protéger les Informations confidentielles ou non qui sont la propriété exclusive du Groupement, de ses Clients et de ses Partenaires commerciaux, chaque Utilisateur est tenu de respecter scrupuleusement les dispositions de la présente Charte.

Une attention toute particulière doit être portée à l'utilisation des Ressources.

Chaque Utilisateur doit avoir sans cesse à l'esprit que le bon usage de ces Ressources est gage de sécurité et d'efficacité opérationnelle pour le Groupement.

Chaque Utilisateur doit être conscient :

- d'une part, que sa négligence ou sa mauvaise utilisation des Ressources peut faire encourir des risques à l'ensemble du Groupement et à lui-même ;
- d'autre part, que l'usage de ces Ressources obéit à des règles qui s'inscrivent dans le respect de la loi et des valeurs propres au Groupement, notamment en ce qui concerne le respect de la Charte d'éthique de la relation commerciale.

Il importe de souligner les risques inhérents à l'utilisation de ces Ressources notamment à l'égard de :

- l'Intégrité et la disponibilité des systèmes d'Information et de communication du Groupement ;
- la Confidentialité des Informations véhiculées ;
- ainsi que l'image du Groupement.

Ces éléments sont à tout moment menacés par le mauvais usage, par le piratage des réseaux, des logiciels ou par l'introduction de logiciels et codes malveillants.

En l'état des techniques, et au fur et à mesure de leurs avancées, le Groupement répond sans cesse à cette menace, en mettant en œuvre tous les moyens pertinents et appropriés, afin de garantir la meilleure sécurité possible de son infrastructure informatique. Il s'agit ainsi de protéger les Ressources mises à la disposition des Utilisateurs contre tout risque de destruction ou d'altération et d'accès non autorisé.

LA SECURITE EST L'AFFAIRE DE TOUS

ARTICLE I : DEFINITIONS

Administrateur : au sein de la STIME ou des directions et services du Groupement, les administrateurs sont des Utilisateurs disposant d'accès privilégiés aux systèmes d'Information, leur permettant d'en gérer et contrôler le fonctionnement.

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

BYOD (Bring your own device) : utilisation d'un équipement personnel par un Utilisateur dans le cadre de ses fonctions au sein du Groupement.

Classification : opération qui consiste à définir le niveau de criticité d'une Information selon un ou plusieurs critères de sécurité (Disponibilité, Intégrité, Confidentialité et Traçabilité). La classification s'applique à une donnée, un Document, un fichier, un programme, une application, etc.

Comportement / usage abusif : comportement ou usage contraire à la Charte et/ou illicite donc contraire à la législation et à la réglementation en vigueur.

Confidentialité : il s'agit d'un des critères de sécurité permettant de s'assurer que l'Information est accessible qu'aux personnes autorisées à y accéder.

COPE (Corporate owned personally enabled) : l'équipement de l'Utilisateur est pris en charge par le Groupement et peut être utilisé à des fins professionnelles et personnelles.

CYOD (Choose your own device) : l'Utilisateur peut choisir un équipement professionnel adapté à ses fonctions et dans cette hypothèse, cela lui est proposé par le Groupement dans un catalogue.

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

Données à caractère personnel ou données personnelles : 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. Pour déterminer si une personne est identifiable, il convient de considérer l'ensemble des moyens en vue de permettre son identification dont dispose ou auxquels peut avoir accès le responsable du Traitement ou toute autre personne.

Données personnelles Sensibles : Traitement des données à caractère personnel qui révèle l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale, ainsi que le Traitement des données génétiques, des données biométriques aux fins d'identifier une personne physique de manière unique, des données concernant la santé ou des données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique. En principe, les données sensibles ne peuvent être recueillies et exploitées qu'avec le consentement explicite des personnes.

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

Filtrage : action consistant à appliquer sur des flux d'Information un ensemble de règles autorisant ou interdisant certains Traitements informatiques.

Fonction Sécurité des Systèmes d'Information ou RSSI : au sein du Groupement, fonction chargée de définir et de contrôler la bonne application des règles permettant d'assurer la sécurité des Informations et des systèmes d'Information. La fonction est incarnée par le directeur de la Sécurité des Systèmes d'Information, son équipe, ainsi que les différents relais au sein des entités du Groupement (responsables locaux de la sécurité des systèmes d'Information, correspondants sécurité).

Habilitation : attribution à un Utilisateur de droits d'accès personnels à des Ressources par une entité autorisée.

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

Informations Classifiées : toute donnée, fichier ou document classifié aux niveaux « confidentiel » ou « secret ».

Intégrité : il s'agit d'un des critères de sécurité, qui garantit l'exactitude, la fiabilité et l'exhaustivité des Informations et des méthodes de Traitement.

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

STIME : ensemble des fonctions du Groupement en charge du développement, de la mise en œuvre et du maintien en conditions opérationnelles des systèmes d'information.

Système d'Information : ensemble organisé de Ressources (données, procédures, matériel, logiciel, personnel, etc.) permettant d'acquérir, traiter, stocker, diffuser ou détruire les Informations utilisées par les entités dans leurs métiers, et ceci quel que soit le support des Informations (numérique, papier, oral, etc.).

Tiers : personnes physiques ou morales, entités ou organismes externes en relation contractuelle avec le Groupement. Sont ainsi considérés comme des tiers : les prestataires, les fournisseurs, les intérimaires, les partenaires…

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

Traitement de données : 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.

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

ARTICLE 2 : OBJET

La présente Charte Utilisateurs énonce les règles que l'Utilisateur au sein du Groupement doit respecter. L'utilisation des Ressources mises à disposition ou utilisées dans le cadre des fonctions de l'Utilisateur, doit s'effectuer de manière sécurisée et en conformité avec la législation et la réglementation en vigueur.

La Charte à destination de l'Utilisateur a ainsi pour objet :

- de l'informer des mesures appliquées en matière de contrôle, de Traçabilité et de Filtrage des comportements et des contenus informatiques ;
- de lui faire prendre conscience de l'importance du respect de la Confidentialité et de la sécurité du Système d'Information du Groupement ;

- de l'informer de ses principaux droits, devoirs et responsabilités ainsi que des règles et recommandations en vigueur au sein du Groupement ;
- de conduire chaque Utilisateur à faire preuve de discipline en matière de sécurité afin d'assurer le bon fonctionnement des Systèmes d'Information du Groupement.

Les principes énoncés ne sont pas exclusifs de l'application des lois et de la règlementation en vigueur, de l'ensemble des règles internes au Groupement ainsi que des règles de courtoisie et de respect d'autrui.

ARTICLE 3 : CHAMP D'APPLICATION

La Charte s'applique aux Ressources et Utilisateurs concernés.

Sont considérés comme :

- **Ressource (d'un système d'Information) :** tout élément intervenant dans la mise en œuvre et le fonctionnement d'un système d'Information (Informations sous toutes leurs formes, Équipements individuels, imprimante, smartphone, tablette, logiciel, serveur de fichiers, base de données, applications métiers, équipement réseau, service réseau interne / souscrit sur Internet, espace disque, messagerie électronique, etc.).

- **Utilisateur (d'un Système d'Information) :** toute personne, qu'elle soit interne ou externe au Groupement (salarié, apprenti, stagiaire, travailleur temporaire et plus généralement l'ensemble du personnel externe ayant accès à tout ou partie des systèmes d'information du Groupement) qui est autorisée à utiliser les Ressources du Systèmes d'Information et les Informations du Groupement. L'Utilisateur désigne toute personne appelée à créer, utiliser, consulter, et mettre en œuvre ces Ressources de manière permanente ou occasionnelle. Il désigne également les Administrateurs, les exploitants et les prestataires externes intervenant sur le SI.

ARTICLE 4 : OPPOSABILITE

La présente Charte constitue une annexe au règlement intérieur et produit, à ce titre, les mêmes effets. Par conséquent, elle revêt un caractère disciplinaire selon l'article L. 1321 du Code du Travail.

En conséquence, l'Utilisateur est supposé en avoir pris connaissance.

Le Groupement utilise à cet effet les moyens qu'il juge adéquats pour la diffuser auprès des utilisateurs. Un moyen adéquat et suffisant est l'un des moyens suivants : remise en main propre aux Utilisateurs, diffusion sur l'intranet, annexe signée aux conventions de stage pour les stagiaires externes (universités, écoles…), transmission individuelle via la Messagerie électronique du Groupement.

La Charte s'applique à l'ensemble des sociétés du Groupement Les Mousquetaires.

Elle s'applique dans l'ensemble des pays où le Groupement exerce une activité et peut dans certains pays être complétée par un additif précisant les règles d'usage ainsi que les dispositifs pouvant être mis en place localement pour assurer la sécurité et le bon fonctionnement des Systèmes d'Information et rappelant les dispositions législatives et règlementaires en vigueur.

Les contrats entre les sociétés du Groupement Les Mousquetaires et tout Tiers donnant accès aux données, aux programmes informatiques ou Ressources liées à l'infrastructure informatique du Groupement, devront stipuler que les Utilisateurs s'engagent à respecter la présente Charte.

Les responsables des Utilisateurs externes s'engagent à faire respecter la présente Charte par leurs propres salariés et éventuelles entreprises sous-traitantes.

ARTICLE 5 : CONFIDENTIALITE

Le respect de la Confidentialité, inhérente aux activités du Groupement, est inscrit dans le Règlement intérieur. Il s'applique aux Ressources.

La sauvegarde des intérêts du Groupement nécessite le respect par l'Utilisateur d'une obligation générale et permanente de Confidentialité, de discrétion et de secret professionnel à l'égard des Ressources et Informations dont il a connaissance dans l'exercice de ses fonctions.

Le respect de cette obligation implique notamment que l'Utilisateur veille à ce que les Informations qu'il exploite ne puissent pas être consultées, modifiées ou reproduites par un tiers non autorisé.

L'attention de l'Utilisateur est attirée sur les risques liés à la diffusion de contenus d'Information sur internet, en particulier au sein des réseaux sociaux et sur les blogs. Il est donc interdit de diffuser à l'extérieur du Groupement et, plus particulièrement, sur Internet, la moindre Information Classifiée, qu'elle soit ou non protégée par une obligation légale de secret ou une obligation contractuelle de Confidentialité.

L'Utilisateur doit donc respecter son obligation de Confidentialité à l'égard des tiers qui, à l'intérieur comme à l'extérieur du Groupement, n'ont pas à connaitre des Informations concernant le Groupement et ses clients.

a) Données à caractère personnel

L'Utilisateur devra veiller tout particulièrement à préserver la sécurité, la Confidentialité et l'Intégrité des Données à caractère personnel recueillies ou transmises dans le cadre de son activité professionnelle.

Il veillera également à préserver les Traitements et extractions des bases de données afin de respecter les dispositions de la loi « Informatique et Libertés » dans sa dernière version et du Règlement général sur la protection des données du 27 avril 2016 (RGPD). Ces dispositions obligent à prendre toutes précautions utiles afin de préserver la sécurité des Informations et d'empêcher en particulier que celles-ci ne soient déformées ou endommagées ou que des tiers non autorisés y aient accès.

Les Informations portant sur les consommateurs ne doivent être stockées que sur les supports et matériels prévus à cet effet. Il est interdit de transmettre ces données, par quelque moyen que ce soit, à un tiers non autorisé.

L'Utilisateur s'engage, à prendre toutes précautions conformes aux usages et à l'état de l'art dans le cadre de ses attributions afin de protéger la confidentialité des données personnelles auxquelles il a accès, et en particulier d'empêcher qu'elles ne soient communiquées à des personnes non expressément autorisées à recevoir ces informations.

L'Utilisateur s'engage en particulier à :

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

L'utilisateur est informé que toute violation de la présente obligation l'expose à des sanctions disciplinaires, administratives et pénales conformément à la réglementation en vigueur. Ces obligations pèsent sur l'Utilisateur pendant toute la durée du contrat le liant au Groupement ainsi qu'après sa rupture pour quelque raison que ce soit.

Conformément aux exigences sur la Protection des Données à caractère personnel, l'Utilisateur est informé que le Groupement a la qualité de responsable de Traitement pour la collecte et le Traitement des Données à caractère personnel communiquées par l'Utilisateur pour les besoins de son activité professionnelle (nom, prénom, numéros de téléphone fixe et mobile, adresse postale et électronique, titre et fonctions professionnelles, …). Le détail de ces traitements est décrit dans la Politique Données personnelles du collaborateur de son entité.

Dans le cadre de son activité professionnelle, les données seront conservées à l'issue de la fin du contrat liant l'Utilisateur au Groupement conformément aux délais de prescription définis par le code civil.

Dans le cadre de la défense des droits du Groupement et l'intérêt légitime qui s'exerce dans le respect des libertés et droits fondamentaux des Utilisateurs, ces données sont susceptibles d'être traitées à des fins de gestion du contentieux. Elles seront conservées jusqu'à l'épuisement des voies de recours.

Les Données à caractère personnel communiquées par l'Utilisateur ne sont transmises à aucun tiers à des fins commerciales ou de prospection. La sous-traitance de la gestion technique et comptable des bases de données du Groupement est encadrée par contrat écrit entre le Groupement et ses sous-traitants. Le Groupement veille à ce que les sous-traitants respectent strictement les dispositions relatives à la sécurité et la Confidentialité des Données à caractère personnel objet du Traitement.

Chaque personne concernée par le(s) Traitement(s) mis en œuvre par le Groupement dispose des droits suivants :

- droit d'accès, de rectification et d'effacement des données la concernant ;
- droit d'opposition au Traitement ;
- droit à la limitation du Traitement de ses données ;
- droit à la portabilité des données ;
- droit d'introduire une réclamation auprès de la CNIL.

Les demandes accompagnées d'un justificatif d'identité peuvent être adressées à :
dpolesmousquetaires@mousquetaires.com
Pour toute question sur les règles de protection des Données à caractère personnel mises en œuvre par le Groupement, les demandes peuvent être adressé au Délégué à la Protection des Données (DPO) à l'adresse suivante : dpolesmousquetaires@mousquetaires.com

b) Gestion des accès

L'accès aux Ressources est encadré par les directions désignées par le Groupement à cet effet ou les collaborateurs qui ont été spécialement habilités à délivrer les Moyens d'authentification à chaque Utilisateur (code confidentiel, carte à puce, etc.).

Pour tous les Moyens d'authentification, l'Utilisateur doit respecter les règles de délivrance et de mise à jour en vigueur au sein du Groupement. Toute Habilitation peut être modifiée ou supprimée sans préavis, notamment en fonction des nécessités de service.

De manière générale, les Moyens d'authentification sont personnels, confidentiels et non transmissibles d'un Utilisateur à toute autre personne.

Les accès réalisés à l'aide d'un Moyen d'authentification propre à chaque Utilisateur ou à partir d'un Outil de nomadisme attribué individuellement sont réputés être le fait du détenteur de ce Moyen d'authentification ou de cet Outil de nomadisme.

L'Utilisateur ne doit pas tenter de contourner les dispositifs de sécurité d'accès en place, de s'introduire de façon illicite dans un système ou d'accéder aux Ressources auxquelles il n'est pas habilité.

i) Accès au réseau interne du Groupement

Aucun outil informatique de nomadisme non mis à la disposition ou agréé par le Groupement ne doit être connecté au réseau interne du Groupement qu'ils soient issus du BYOD, du CYOD ou du COPE.

Toute Ressource pourra être soumise à tout contrôle de sécurité ponctuel ou permanent, et sera soumis à l'ensemble des règles de la présente Charte.

A ce titre, le titulaire des Ressources concernées décharge le Groupement de toute responsabilité quant à toute conséquence préjudiciable liée à ces contrôles (effacement de données, dysfonctionnement, etc.).

ii) Accès à distance

Tous les Utilisateurs doivent s'authentifier pour accéder à distance aux Ressources du Système d'Information. Ils s'engagent à respecter leurs Habilitations et plus généralement toutes les recommandations de sécurité spécifiques aux accès distants.

iii) Indisponibilité des Accès

L'accès de l'Utilisateur aux Ressources du Groupement pourra être suspendu, limité ou réexaminé, pour des raisons de sécurité, notamment :

- dans le cadre de la maintenance des Ressources ;
- lors de la cessation de son activité professionnelle au sein de son service ou du Groupement (changement de service, mutation, etc.) ;
- dans certains cas de suspension temporaire de l'activité professionnelle (maladie, congé de maternité ou de paternité, etc.) ;
- dès lors qu'un usage abusif (manquements à la Charte, manquements aux lois et réglementations en vigueur, etc.) sera révélé.

La mise en œuvre de ces dispositions fait l'objet d'une information écrite et motivée à l'Utilisateur qui dispose d'un droit de réponse écrit et motivé dans les cinq (5) jours ouvrés.

ARTICLE 6 : CONDITIONS D'UTILISATION DES RESSOURCES

a) Principes

De manière générale, tout Utilisateur est responsable de l'usage qu'il fait des Ressources qui sont mises à sa disposition dans le cadre de son activité professionnelle au sein du Groupement.

L'Utilisateur doit en particulier :

- assurer la protection de ces Ressources en respectant les règles de sécurité applicables à celles-ci et en s'assurant de ne pas les mettre à disposition de personnes non autorisées, que ce soit des personnes internes ou externes au Groupement ;
- être vigilant et signaler, dans les meilleurs délais puis par écrit (courrier ou mail), toute anomalie ou tout constat, tentative ou soupçon de violation d'une Ressource du Groupement à sa hiérarchie et/ou à la Fonction Sécurité des Systèmes d'Information ;
- veiller, en toutes circonstances, à mettre en sécurité le matériel, notamment portable, mis à sa disposition ;
- verrouiller ou déconnecter son Équipement individuel en cas d'absence même temporaire.

b) Interdictions particulières

L'Utilisateur ne doit pas :

- introduire des failles de sécurité dans les architectures des Systèmes d'Information, par exemple par la connexion simultanée de son Équipement individuel au réseau du Groupement et à des réseaux et systèmes externes (raccordement à des réseaux sans-fil publics[1]…) ;
- tenter de lire, modifier, copier ou détruire des données ou Documents autres que ceux qui lui appartiennent en propre ou pour lesquels il dispose des droits correspondants (lecture, modification ou suppression) ;
- risquer d'engorger volontairement les réseaux et les Systèmes d'Information, en évitant – sauf impératif de service – d'échanger via la messagerie électronique, ou de télécharger, via Internet, des volumes de données trop importants ;
- contourner ou désactiver les dispositifs de sécurité de ses Équipements individuels, notamment les antivirus, par exemple en installant sur les serveurs de Ressources partagées des logiciels susceptibles de contourner, d'affaiblir ou de perturber la sécurité ou les performances du Système d'Information ;
- exploiter ou tenter d'exploiter une éventuelle faille de sécurité d'un Système d'Information ou en faire la publicité ou la diffuser ;
- apporter des perturbations au bon fonctionnement des Systèmes d'Information, que ce soit par des manipulations anormales des Ressources matérielles et/ou logicielles ou par l'introduction volontaire de programmes et codes malveillants (tels que des virus) ;

[1] Du type des réseaux Wi-Fi des hôtels, des restaurants ou des aéroports.

- contourner les restrictions d'utilisation des Ressources mises à sa disposition par le Groupement ;
- traiter des Informations professionnelles au travers d'outils ou de services qui n'aient pas été préalablement validés par la STIME.

L'Utilisateur ne doit pas déplacer, dupliquer ou détruire les fichiers ou les Documents sur lesquels sa fonction et ses missions le conduisent à intervenir avant de s'être assuré que cela ne porte aucun préjudice au Groupement. Il respectera les règles et modalités d'archivage dans la mesure où elles sont définies.

L'Utilisateur doit, en outre, enregistrer régulièrement les données qu'il exploite, qu'il crée ou qu'il transforme pour la continuité du service aux endroits adéquats. Toutefois, lorsque les Informations ou les données sont Classifiées, l'Utilisateur s'engage à ne pas les sauvegarder sur un espace de stockage partagé avec des personnes non habilitées à en connaître.

Les Ressources mises à disposition d'un Utilisateur, en particulier les Équipements individuels, sont configurés par la STIME de manière à assurer un niveau de sécurité et de fiabilité optimal. Aussi, l'Utilisateur ne doit jamais de lui-même :

- modifier ou tenter de modifier la configuration et les paramètres de ces Ressources, y compris par l'installation de logiciels ;
- désactiver ou tenter de désactiver les mécanismes de sécurité mis en œuvre (logiciel anti-virus, écran de veille automatique, outils d'authentification, outils de chiffrement de données ou de messages…), ou en changer les paramètres ;
- utiliser ou tenter d'utiliser des outils de sécurité non-fournis par le Groupement, notamment en termes de sécurité réseau ou de chiffrement de données ;
- connecter ou tenter de connecter aux Systèmes d'Information du Groupement des Ressources non fournies par le Groupement et, notamment : connexion partagée, périphérique, supports externes amovibles (disques durs externes, clés USB), graveurs, carte réseau Wifi, logiciel, sauf accord exprès préalable de la Fonction Sécurité des Systèmes d'Information.

c) Utilisation non-professionnelle

Un usage personnel ponctuel et raisonnable des Ressources (téléphones fixe et portable, messagerie électronique, accès Internet, stockage et échange de fichiers), dans le cadre des nécessités de la vie courante et familiale, est toléré à condition que cet usage soit strictement conforme aux législations et réglementations applicables et respecte la présente Charte, notamment qu'il ne porte pas préjudice à l'activité professionnelle et qu'il ne soit pas susceptible d'affecter le bon fonctionnement du service et des Ressources (perturbation ou limitation des capacités techniques mises à disposition de l'Utilisateur) ou de mettre en cause l'intérêt et / ou la réputation du Groupement.

Ainsi, seront présumés privés les fichiers et messages qui, lors de leur création, de leur Traitement ou de leur conservation auront été clairement identifiés par l'Utilisateur au moyen de la mention suivante et à l'exclusion de toute autre mention telle que « personnel » :

- pour les messages, aussi bien les messages émis que reçus, l'objet du message doit mentionner l'indication « PRIVÉ » ou « PERSO »[2],
- pour les fichiers, les noms des fichiers doivent mentionner l'indication « PRIVÉ » et ils doivent être conservés dans des répertoires spécifiques dont les noms mentionnent l'indication « PRIVÉ» ou « PERSO ».

Tout message et fichier ne correspondant pas à ces règles est considéré comme professionnel[3].

d) *Usage abusif*

Par rapport aux règles de bon usage des Ressources, seront notamment considérés comme abusifs au sens de la Charte les comportements visant à organiser la réception, consulter ou tenter de consulter, télécharger, conserver, publier, diffuser ou distribuer, en toute connaissance de cause au moyen des Systèmes d'Information du Groupement, tous programmes, logiciels, Documents électroniques, messages, Informations, données :

- à caractère violent, pornographique, pédopornographique, zoophile, xénophobe, négationniste, raciste, homophobe, terroriste et, plus généralement, contraire à la réglementation en vigueur ;
- susceptibles de porter atteinte au respect de la personne humaine, de sa dignité ou de sa vie privée ;
- à caractère diffamatoire, insultant, malveillant ;
- ayant pour objet le harcèlement, la menace ou l'injure ;
- contenant des éléments protégés par les lois et les conventions internationales sur la propriété intellectuelle et le droit à l'image, sauf à posséder les autorisations nécessaires ;
- incitant à la commission d'un délit ou d'un crime et, de manière générale, d'actions illicites ou contraires à l'ordre public ;

Les éléments ci-dessus constituent un rappel de la législation française, plus large que le cadre de cette Charte et qui vont par nature au-delà du contrôle du Groupement. Les tribunaux pourront donc également, le cas échéant, prononcer des sanctions relatives aux comportements abusifs en question.

[2] L'Utilisateur devra informer ses correspondants de l'existence de cette règle lors de la communication de son adresse de messagerie à titre privé, et s'assurer du respect de ladite règle dans le cadre de ses communications privées via son adresse de messagerie professionnelle.

[3] Par exemple, la fonctionnalité « Critères de diffusion » présente dans le logiciel Outlook de Microsoft Office et permettant à l'Utilisateur de choisir entre les valeurs « normal », « personnel », « privé » ou « confidentiel » n'est pas, pour des raisons techniques, considérée dans la présente Charte comme permettant clairement une identification privée.

Par ailleurs, en raison des risques spécifiques encourus par le Groupement, seront également considérés comme abusifs au sens de la Charte les comportements visant à organiser la réception, consulter ou tenter de consulter, télécharger, conserver, publier, diffuser ou distribuer, en toute connaissance de cause au moyen des Systèmes d'Information du Groupement, tous programmes, logiciels, Documents électroniques, messages, Informations, données :

- contenant des codes malveillants ou des données contaminées ;
- portant sur des Informations internes au Groupement ou confidentielles, au mépris des dispositions internes relatives à la Confidentialité des échanges, de l'obligation de loyauté et de discrétion professionnelle, et du secret professionnel ;
- manifestement attentatoires à l'image de marque interne ou externe du Groupement ou à sa réputation.

Seront également considérés comme abusifs : l'utilisation des services Internet à des fins commerciales, ludiques (ex : jeux, paris en ligne) ou illicites, ainsi qu'un usage privé inapproprié des services Internet, du fait notamment de la durée et du volume de connexion.

ARTICLE 7 : SECURITE

La sécurité est l'affaire de tous. Ne pas la respecter fait courir un danger au Groupement et à l'Utilisateur lui-même.

a) Administrateurs des Systèmes d'Information

Afin de conduire les actions correspondant à leurs missions (maintenance, configuration, évolution, supervision, etc.), les Administrateurs des Systèmes d'Information (Administrateurs de réseau, Système, base de données, téléphonie, messagerie, etc.) disposent de droits d'accès privilégiés au Système d'Information du Groupement.

Ces droits d'accès privilégiés peuvent présenter des risques spécifiques, car donnant la possibilité technique d'accéder à des informations confidentielles, d'altérer voire de supprimer des données, de modifier des droits d'accès au Système d'Information ou des mécanismes de protection, de réaliser des contrôles ne respectant pas le cadre légal et règlementaire.

Chaque Administrateur doit avoir conscience de ses responsabilités en matière de sécurité du Système d'Information, et des risques que présente une utilisation abusive des droits d'accès privilégiés qui lui sont confiés.

Les Administrateurs des Systèmes d'Information doivent notamment :

- Limiter leurs accès aux seules Ressources nécessaires justifiées par la nature de la tâche à accomplir, à l'exclusion de toutes autres et ce, même si cet accès est techniquement possible ;
- Se limiter à la gestion des contenants sans prendre connaissance des contenus au-delà du strict nécessaire afférent aux opérations effectuées ;
- Se limiter à des contrôles justifiés par la mission d'administration à accomplir et proportionnés au but recherché ;
- Ne pas exploiter, ni divulguer les informations confidentielles, dont ils pourraient avoir connaissance dans l'exercice de leurs fonctions en particulier lorsque celles-ci sont couvertes par le secret des correspondances ou relèvent de la vie privée des utilisateurs.

b) Obligation de vigilance

- L'utilisation de ces Ressources nécessite, de la part des Utilisateurs, une grande vigilance tant à l'intérieur du Groupement, qu'à leur domicile ou à l'occasion de tout déplacement sur le territoire national ou à l'étranger, et en particulier, dans les transports individuels ou collectifs.

En plus des obligations générales, ils doivent :

- s'assurer de la protection des matériels contre le vol, par l'utilisation, sur leur lieu de travail d'un système antivol qui leur est fourni et, en cas de non utilisation, de le ranger dans un endroit sécurisé et fermé à clé la nuit ;

- ne pas laisser ces matériels sans surveillance (par exemple dans un véhicule stationné) et en particulier ne pas laisser apparent un ordinateur portable confié par le Groupement dans un bureau non verrouillé ou un moyen de transport (voiture, train, avion ...) ;

- s'assurer de la protection des Informations en leur possession, en verrouillant ou fermant notamment leur session lorsqu'ils s'éloignent du matériel ;

- ne pas utiliser ces Équipements individuels s'ils sont susceptibles d'être surveillés, principalement lorsqu'ils saisissent des mots de passe ou consultent des Informations Classifiées ;

- informer, le plus rapidement possible via la procédure de déclaration d'incident prévue du vol, de la perte ou d'une possible utilisation par un tiers de ces outils et données (suspicion d'usurpation d'identité) ;

- en cas de vol de l'équipement, une déclaration doit être effectuée sans délai au commissariat de police le plus proche du lieu du vol, avec copie adressée au Groupement. Toute déclaration volontairement fausse est passible de sanctions disciplinaires et/ou de poursuites pénales. Parallèlement, il rendra compte à sa hiérarchie de l'évènement afin qu'une évaluation puisse être faite quant au préjudice potentiel pour le Groupement ;

- en tout état de cause, éviter d'y conserver des Documents confidentiels et des Données à caractère personnel.

ARTICLE 8 : CONTROLE – TRACABILITE – FILTRAGE

a) Contrôle

Des mesures de contrôle et de suivi sont mises en œuvre dans le strict respect des principes de transparence et de proportionnalité des moyens de collecte, ceci à des fins de sécurité et de vérification du bon accès et usage des Ressources. Ces Traitements de données automatisés font l'objet des formalités conformément aux dispositions relatives à la protection des Données à caractère personnel.

L'ensemble des outils de sécurité déployés dans les Systèmes d'Information du Groupement (antivirus, Filtrage des flux, lutte contre la fuite d'Information…) participent à ce contrôle. Outre leur fonction première qui est de mettre un terme aux menaces qu'ils détectent, ces outils génèrent des événements de sécurité qui sont agrégés dans un environnement technique dédié, permettant leur corrélation et leur analyse par les personnes habilitées du centre opérationnel de sécurité. En cas de nécessité de preuves et de traces numériques plus complètes, le Groupement peut également mettre en œuvre des outils d'investigations avancées (dits « forensic »).

Les données et traces informatiques enregistrées dans le cadre de ces mesures portent sur l'identification du compte de l'Utilisateur, la date et heure de l'action considérée, la nature et les résultats de l'action.

Ces données et traces informatiques sont conservées pendant une période maximale d'un an (sauf obligations légales ou règlementaires particulières de conserver ces données sur une durée plus longue ; ex : délais de prescription) et font l'objet de mesures de protection adaptées contre tout risque avéré de divulgation et d'utilisation abusive.

Par la présente Charte, l'Utilisateur est donc informé de la mise en place de dispositifs de sécurité visant à collecter des Informations concernant son usage des Ressources mises à sa disposition ou auxquelles il a accès conformément à la réglementation en vigueur, avec comme objectifs :

- de garantir le bon fonctionnement de ces Ressources,
- de lutter contre la fuite d'Informations Classifiées ou la violation de la sécurité et de la Confidentialité des Données à caractère personnel,
- de pouvoir identifier et, le cas échéant, sanctionner des usages contraires à la présente Charte, aux législations et réglementations applicables,
- de traiter les procédures juridictionnelles (judiciaire et administrative) comme notamment pouvoir répondre aux requêtes des autorités compétentes (services de police, autorités judiciaires…).

i) Journal d'exploitation

Le Système d'Information génère des journaux d'événements (dits « logs ») créés automatiquement par les équipements informatiques et de communications électroniques. Ils permettent de retracer la vie du Système d'Information du Groupement et les actions qui y sont menées, et sont stockés sur les postes informatiques et le réseau. Ils contribuent à assurer le bon fonctionnement du système et la sécurité des Informations du Groupement, à travers la détection des erreurs matérielles ou logicielles, et le contrôle des actions des Utilisateurs et des Tiers accédant au Système d'Information.

Sont notamment surveillées et conservées les données relatives :

- à l'utilisation des Ressources, pour contrôler l'accès, les modifications et suppressions de données ;
- aux connexions entrantes et sortantes au réseau interne, aux applications, à la messagerie et à l'Internet, afin de détecter les anomalies liées à l'utilisation des Ressources et prévenir les activités malveillantes.

ii) Navigation sur Internet

Outre le blocage des sites non autorisés, chaque connexion ou tentative de connexion pour la navigation sur Internet fait l'objet d'un contrôle : sites visités, durées de connexion, éléments téléchargés ainsi que leur type.

iii) Interruption des flux chiffrés

Dès lors qu'une procédure ou qu'une politique est définies par la STIME et qu'elle est applicable au sein du Groupement, afin de permettre la recherche de logiciels malveillants et de lutter contre la fuite d'Information, les flux chiffrés (repérables par une URL commençant par « https://... ») seront systématiquement interrompus par le Groupement le temps d'opérer ces contrôles de sécurité, puis seront à nouveau chiffrés pour en assurer la protection sur le reste de leur parcours.

iv) Statistiques

Les données et traces informatiques font l'objet de Traitements automatisés à des fins statistiques (nombre de messages émis vers ou reçus d'Internet, volumes occupés par l'ensemble des boîtes aux lettres, sites Internet les plus visités, taille des espaces sur les serveurs de fichiers, durées totales des connexions distantes, etc.).

b) Filtrage

Des systèmes de Filtrage peuvent être mis en œuvre pour analyser les entrants et sortants (contrôle antiviral, contrôle anti-spam, contrôle de la taille, liste des destinataires, etc.) et également pour bloquer, notamment sur la base de listes de mots-clefs, des actions non autorisées (envois de messages électroniques, copies de fichiers, impressions de Documents…), ainsi que les contrôles de flux par le biais des firewalls ou des enregistrements par des « bastions ».

c) Investigations (forensic)

L'Utilisateur est informé que des contrôles individualisés pourront être diligentés, suite à un dysfonctionnement des Systèmes d'Information du Groupement, à une alerte de sécurité et également en cas de suspicion d'un usage non conforme de ces Systèmes d'Information, sous réserve du respect des dispositions légales applicables et des procédures internes le cas échéant.

Dans ce cadre, les constatations matérielles ont pour but de relever les diverses circonstances qui éclaireront l'incident sur l'éventuelle réalisation d'un fait constitutif d'une faute et sur l'identification de ses auteurs.

Lors de ces investigations, menées par la Fonction Sécurité des Systèmes d'Information du Groupement, le concours de l'Utilisateur pourra être sollicité afin d'accélérer l'analyse de la situation et ainsi préserver le fonctionnement du Système d'Information.

Au besoin, et en fonction du résultat des contrôles opérés, l'accès à certaines Ressources (sites visités depuis le réseau du Groupement, partages de fichiers, etc.) pourra être interdit sans préavis ni Information.

d) Spécificité des Informations marquées « PRIVÉ » OU « PERSO »

En cas d'alerte de sécurité, de dysfonctionnement ou d'anomalie, de risques ou d'événements particuliers identifiés, il peut être procédé à un contrôle manuel et à une vérification de toutes opérations effectuées par un ou plusieurs Utilisateurs.

Tout message et tout fichier qui n'est pas explicitement identifié comme « PRIVÉ » ou « PERSO » étant présumé professionnel, le Groupement peut y accéder pour les besoins exceptionnels rappelés ci-dessus, via des personnels habilités, dans le strict respect de la règlementation applicable ainsi que des règles de sécurité supplémentaires que s'impose le Groupement.

S'agissant des messages et fichiers « PRIVÉ » OU « PERSO », en cas d'alerte de sécurité, de dysfonctionnement ou d'anomalie, de risques ou d'événements particuliers identifiés, ils ne peuvent être ouverts qu'en présence de l'Utilisateur en cause ou si ce dernier a été dument appelé. Ou à défaut par le biais de la procédure de droit commun.

- Autres situations

Les communications émises ou reçues dans le cadre d'une activité protégée par des dispositions légales (ex : secret médical) et les données et fichiers qui en résultent sont également considérées « PRIVE » ou « PERSO » au sens de la présente Charte, même si elles ne sont pas explicitement identifiées comme telles.

e) Lutte contre la fraude informatique

La STIME, dans le cadre de la lutte contre la fraude et en conformité avec les dispositions du code pénal relatives à la fraude informatique qu'il s'agisse, notamment, de l'intrusion dans un système de Traitement automatise de données et/ou du maintien sans Habilitation dans tout ou partie d'un système de Traitement automatisé de données, de l'entrave au fonctionnement de ce système ou de l'altération des éléments et, en particulier, des données qu'il contient (ex : sur les cartes de fidélité) informera les autorités compétentes en la matière. Si, par erreur ou suite à un dysfonctionnement, un Utilisateur accède à des informations ou à des Traitements, systèmes internes ou externes qui ne lui sont pas autorisés, l'Utilisateur s'engage à ne pas s'y maintenir et à le signaler au RSSI ou à son représentant. Les tentatives d'accès non autorisé, d'intrusion ou de contournement des sécurités d'accès sont interdites et susceptibles de mettre en cause la responsabilité pénale de tout Utilisateur qui s'y livrerait.

ARTICLE 9 : PATRIMOINE INFORMATIONNEL

Lorsque les processus et procédures relatives au Marquage et à la Classification des Documents du Groupement seront entrés en vigueur, les dispositions ci-après s'appliquent.

a) Marquage

Chaque Utilisateur doit s'assurer que les Documents qu'il traite sont classifiés en évaluant l'incidence (financière, organisationnelle, juridique, sociale et d'image) d'une divulgation (en interne ou externe) de ces Informations en suivant la politique de lutte contre la fuite d'Informations ou la politique de Confidentialité. Un Marquage visuel correspondant à la Classification sera systématiquement apposé sur les Documents.

b) Protection

L'Utilisateur doit veiller à protéger les Informations qu'il manipule avec les Ressources mises à sa disposition et à adapter le niveau de protection qui leur est appliqué en fonction du contexte d'utilisation (restriction des accès, diffusion, chiffrement, destruction).

Les Utilisateurs doivent utiliser les logiciels, les outils de protection et les outils de chiffrement attribués ou agréés par le Groupement selon la Confidentialité des Informations.

La mise en place de mesures de contrôle spécifiques permet de lutter contre la fuite d'Information. Ainsi des outils de détection (ex : le DLP – Data Leaks Prevention) associés aux mécanismes de supervision des incidents doivent permettre de s'assurer que les Informations Classifiées ne sont pas manipulées de manière inappropriée (notamment leur diffusion), que ce soit en externe ou en interne au Groupement.

c) Obligation de discrétion

L'obligation de discrétion s'impose à l'Utilisateur qui n'a pas à accéder à des Informations qui ne sont pas nécessaires à l'exercice de ses fonctions, ni à faire circuler les Informations détenues par le Groupement, par les adhérents, tant à l'extérieur de l'entité du Groupement dans laquelle il exerce ses fonctions qu'aux collaborateurs qui ne sont pas concernés.

d) Sauvegardes

Les sauvegardes automatiques faites par le Groupement sont notamment réalisées pour se prémunir d'actes de malveillance ou d'une corruption généralisée du système.

Les dispositifs de sécurité informatique du Groupement permettent une conservation d'une durée conforme à la loi en vigueur, des Informations relatives aux :

- Messages électroniques (adresse mail des correspondants, dates et heures d'envoi et de réception, textes des messages transmis et reçus, pièces jointes, etc.) ;
- Données de connexion à Internet (durées de connexion, demandes d'accès refusées par les mécanismes de Filtrage...) ;
- Données de connexion au réseau, applications et serveurs de fichiers (dates et heures de connexion, opérations effectuées, références du poste connecté, etc.).

Les Utilisateurs sont informés qu'en utilisant de façon ponctuelle, à titre privé, les Ressources du Groupement, ils acceptent tacitement les principes et les durées de conservation desdites Ressources en vigueur dans le Groupement.

La durée de conservation est celle indiquée dans les registres de Données à caractère personnel. Les durées de conservation peuvent évoluer en fonction de la règlementation[4].

ARTICLE 10 : RESSOURCES UTILISEES

a) Poste de Travail et équipement de connexion

L'Utilisateur qui dispose d'un Équipement individuel pour se connecter, confié par le Groupement, s'interdit de l'utiliser d'une manière qui pourrait mettre en danger les données qu'il contient ainsi que le Système d'Information du Groupement.

Dans ce contexte, pour en protéger l'accès du poste de travail vis-à-vis d'un Tiers, quel qu'il soit, y compris de manière ponctuelle, chaque Utilisateur devra :

- appliquer la politique du Groupement relative aux mots de passe (renouvellement, longueur suffisante, complexité, etc.) pour l'accès aux Ressources ;
- garder secrets les mots de passe qui ne doivent en aucun cas être cédés, prêtés ou transmis de quelque façon que ce soit à un Tiers interne ou externe au Groupement, même temporairement (sous réserve des nécessités de service) ;
- verrouiller son poste de travail lorsqu'il s'absente et l'éteindre en fin de journée et le week-end, sauf impératif technique lié à la maintenance des Ressources ou nécessité opérationnelle ;
- utiliser les moyens mis à sa disposition par le Groupement pour sécuriser les postes informatiques ;
- s'assurer que les Documents de travail sont sur des espaces sauvegardés. En cas de dysfonctionnement, il en informera la STIME.

L'Utilisateur ne doit pas apporter de perturbations au fonctionnement des Ressources, il s'interdit notamment :

- D'installer des logiciels qui n'auraient pas été approuvés formellement par la STIME ;
- D'ajouter ou de supprimer des équipements, matériels ou logiciels ou de modifier les données nécessaires à leur fonctionnement ;
- De contourner ou inhiber les systèmes de protection installés sur les postes de travail (antivirus, pare-feu, etc.) ;
- D'introduire des logiciels malveillants (virus, cheval de Troie, bombe logique, etc.) ou d'empêcher le bon fonctionnement ou la mise à jour du logiciel antivirus ;
- D'exploiter et/ou publier toute faille de sécurité éventuelle touchant les Ressources mises à sa disposition dont il aurait connaissance et informer la STIME dans les meilleurs délais ;

[4] Chaque entité doit disposer d'un registre qui consigne l'ensemble des Traitements de données.

- De bloquer les processus automatiques de mises à jour des logiciels.

L'Utilisateur doit informer immédiatement la STIME en cas de connaissance de toute faille de sécurité.

Les configurations logicielles sont définies par le Groupement pour répondre à la majorité des besoins des Utilisateurs. Toute tentative de modification de la configuration initiale est proscrite car susceptible de provoquer des dysfonctionnements importants des Ressources (atteinte à la performance, à la sécurité, etc.).

Dans le cas où il n'existerait pas de configuration prédéfinie pour un besoin spécifique, l'Utilisateur doit se rapprocher de la STIME pour étudier la meilleure solution permettant de répondre au besoin exprimé.

En ce qui concerne l'intervention à distance sur la session d'un Utilisateur, celle-ci ne pourra être opérée qu'en cas de demande préalable d'assistance de l'Utilisateur ou sur demande préalable de la STIME et avec l'autorisation de la hiérarchie concernée.

Seuls les personnels habilités par le Groupement sont autorisés à intervenir sur les Ressources mises à disposition des Utilisateurs.

Conformément à la législation en matière de propriété intellectuelle, le Groupement s'acquitte de droit d'usage et de licence des logiciels et progiciels.

En conséquence, il est interdit de prêter, vendre ou céder à des Tiers, les logiciels, licences, programmes d'installation et outils fournis par le Groupement. Cette interdiction concerne également les logiciels développés par les équipes informatiques internes au Groupement.

L'Utilisateur veillera également à limiter le stockage d'Information à caractère professionnel, sur un poste de travail ou sur des serveurs de fichiers autres que ceux mis à sa disposition par le Groupement.

Aucun ordinateur et autre équipement de connexion quel qu'il soit, non confié ou validé par le Groupement, ne doit être connecté physiquement au réseau interne du Groupement.

b) Outils de Nomadisme

Les terminaux mobiles, nomades et supports de stockage amovibles peuvent être des vecteurs d'entrée de virus informatiques sur les postes de travail et le réseau. Il est obligatoire d'en faire usage avec prudence et en particulier lorsqu'ils proviennent de l'extérieur du Groupement. En cas de doute, l'Utilisateur devra contacter la STIME qui effectuera les contrôles de sécurité adéquats. Par ailleurs, compte tenu de leur petite taille qui les expose facilement à la perte ou au vol, il est impératif d'en supprimer les fichiers une fois que le transfert des données est terminé.

Sauf agrément ou validation du Groupement, l'utilisation des terminaux mobiles personnels sur le lieu du travail est soumise aux restrictions suivantes :

- Ils ne doivent pas être connectés au Système d'Information du Groupement (par Wifi, par USB, Bluetooth...) ;
- L'Utilisateur ne doit pas utiliser l'espace de stockage de ces appareils pour transporter des Documents de travail.

L'utilisation de terminaux mobiles personnels pour accéder, stocker ou traiter des Informations du Groupement est strictement interdite (exemple : utilisant un ordinateur portable personnel à partir d'un accès des locaux Groupement ou à domicile) à l'exception des services autorisés par le Groupement utilisés dans le cadre fixé par le Groupement.

L'usage dans le cadre professionnel des appareils photo, vidéo et de l'enregistreur sonore intégrés aux appareils mobiles personnels ou professionnels est interdit, sauf autorisation expresse de la hiérarchie ou du responsable du site ou de l'entité concernée et/ou de la Direction de la communication et avec accord écrit des personnes concernées.

c) BYOD /CYOD / COPE

Afin de diversifier les ressources utilisées par l'Utilisateur, et afin qu'il puisse exercer ses fonctions dans un environnement qu'il maîtrise, le Groupement a mis en place la possibilité de recourir aux solutions suivantes BYOD, CYOD, COPE.

Ces solutions sont proposées individuellement aux Utilisateurs selon leurs fonctions par les autorités compétentes du Groupement. Leur mise en œuvre est expressément stipulée dans leur contrat de travail ou dans un Document émanant de la hiérarchie de l'Utilisateur. Si ce n'est pas le cas, tout Utilisateur qui s'arrogerait le droit d'avoir recours à celles-ci viole la présente Charte.

d) Internet

L'accès à l'Internet est attribué individuellement aux Utilisateurs et mis à disposition pour un usage professionnel. Il est paramétré et administré à cet effet.

L'accès à l'Internet n'est autorisé qu'au travers des dispositifs de sécurité mis en place par le Groupement, via ses Administrateurs dès que l'on est sur un site sur lequel sont proposés ces dispositifs de sécurité.

D'une manière générale, il est rappelé que l'Utilisateur s'engage à adopter un comportement vigilant et responsable dans l'environnement internet.

L'Utilisateur doit faire usage des services de l'internet dans le respect des règles propres aux sites visités et ne doit pas :

- se connecter ou essayer de se connecter sur l'internet autrement que par l'accès internet officiel fourni à travers le réseau du Groupement dès que l'on est sur un site sur lequel sont proposés ces dispositifs de sécurité, afin de ne pas affaiblir le niveau général de sécurité des Ressources ;
- consulter des sites susceptibles de comporter un risque pour la sécurité des Ressources du Groupement, permettant de contourner les dispositifs de protection techniques (et notamment les dispositifs de Filtrage) ou de porter atteinte à la Confidentialité des Informations ;
- consulter des sites proposant illicitement la consultation ou le téléchargement de contenus multimédias (photos, textes, vidéos, musique, etc.) ou autres (logiciels, etc.) protégés par les droits de propriété intellectuelle ;
- télécharger des contenus multimédias (photos, textes, vidéos, musique, etc.) ou autres (logiciel, jeux, contenus pornographiques, zoophiles etc.) ne rentrant pas dans le cadre d'un accès professionnel ;
- de manière générale, utiliser des services de l'internet à des fins commerciales, ludiques ou illicites, étant précisé que les sites pornographiques, zoophiles, et de jeux sont strictement prohibés.

L'Utilisateur engage sa responsabilité vis-à-vis du Groupement et des Tiers au titre des propos émis sur ce canal.

Le téléchargement de fichiers est autorisé, dans la mesure ou l'émetteur est identifié et reconnu et où cela n'affecte ni les règles de sécurité ni la performance des Ressources. Le téléchargement doit être légal et donc conforme à la réglementation applicable et notamment à la loi Hadopi. L'Utilisateur est informé que le Groupement met en œuvre des outils de Filtrage et de contrôle permettant de détecter les téléchargements illégaux.

Le Groupement pourra bloquer l'accès à certains sites Web dont le contenu serait illégal ou déplacé ou s'ils présentent des risques pour sa sécurité informatique. Ce blocage peut être mis en œuvre à travers une analyse de chaque demande de connexion Internet par chaque Utilisateur.

De nombreux services Internet innovants, des services aussi nommés « informatique en nuage » ou « cloud » sont disponibles aujourd'hui. Ces services (par exemple : stockage de fichiers, partage de contenu, solutions collaboratives, messagerie instantanée) sont de plus en plus utilisés mais peuvent entraîner des vols d'Informations. A ce titre, seuls les services sélectionnés et autorisés par le Groupement peuvent être utilisés par les Utilisateurs. Le stockage ou le partage de contenu numérique par le biais de services non autorisés ou sur des services autorisés mais par le biais d'accès non autorisés par le Groupement est strictement interdit

e) Réseaux sociaux

Utilisation à titre professionnel

Si, pour des raisons professionnelles, l'Utilisateur doit accéder aux réseaux sociaux[5], qu'ils soient internes ou externes, il s'engage à respecter scrupuleusement la procédure d'autorisation mise en place au sein du Groupement et les éventuelles chartes des bons usages.

Réseaux sociaux d'entreprise

Les réseaux sociaux d'entreprise permettent aux personnes physiques et morales du Groupement de se réunir de manière exclusive au sein d'une Ressource dédiée.

L'Utilisateur s'engage à ne pas utiliser les réseaux sociaux d'entreprise en dehors de toute activité professionnelle et/ou nécessaire à l'accomplissement de ses missions.

Il est interdit de diffuser tout contenus appartenant à la sphère privée et familiale qui révèle notamment l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques, l'appartenance syndicale, la santé, la vie sexuelle ou l'orientation sexuelle d'une personne physique. Et ce, que ce soit de manière implicite ou explicite.

Réseaux sociaux externes

Les réseaux sociaux externes s'entendent comme ceux étant accessibles par le grand public.

S'il est amené à créer sur les réseaux sociaux un compte professionnel, celui-ci doit être distinct de son compte privé, le compte professionnel étant le seul utilisé pour diffuser des contenus. Il devra choisir des identifiants permettant de reconnaître clairement le caractère professionnel du compte utilisé sur les réseaux sociaux.

L'Utilisateur s'engage à utiliser une présentation loyale et claire. Lorsque le caractère publicitaire d'un contenu ne ressort pas directement, d'adjoindre une indication explicite permettant d'identifier la publicité en tant que telle.

Lorsque le contenu renvoie à une offre commerciale ou à une page permettant d'y accéder, de mentionner explicitement l'intention commerciale de l'offre si elle ne ressort pas clairement du contenu.

[5] Liste non exhaustive de réseaux sociaux sur Internet : Facebook, Twitter, LinkedIn, Instagram, Workplace by Facebook …

Il doit veiller au caractère équilibré du contenu, notamment au regard des avantages et conditions mises en avant ; dans le cas d'un partage, d'assurer ce caractère équilibré en contrebalançant le cas échéant le contenu initial par tout moyen.

Pour les contenus diffusés sur un réseau social présentant des limites objectives d'espace ou de temps, de mentionner de manière apparente l'existence d'Informations complémentaires et de les rendre directement accessibles par un renvoi vers un autre support digital, pour peu qu'à la lecture du contenu, les principes d'équilibre et de clarté soient préservés.

L'Utilisateur engage sa responsabilité en cas de pratique commerciale trompeuse.

Il s'engage notamment à ne pas intervenir de façon anonyme, ni utiliser de pseudonyme ou emprunter une quelconque identité fictive.

L'Utilisateur doit mettre en œuvre une politique d'archivage de ces contenus. Le cas échéant, il pourra recourir aux techniques d'archivage proposées par le réseau social, s'il estime que ces moyens lui permettent de répondre de manière satisfaisante à ses besoins et sont conformes aux dispositions législatives et règlementaires en vigueur.

L'Utilisateur devra veiller à ce que les procédures organisant les modalités de communication à des fins commerciales par un professionnel au nom ou pour le compte d'un autre professionnel incluent les réseaux sociaux.

Utilisation à titre privé

Sur les réseaux sociaux externes et sauf autorisation formelle, l'Utilisateur s'engage à ne pas diffuser d'Informations confidentielles sur le Groupement.

L'Utilisateur se connectant à des forums, réseaux sociaux ou encore des sites collaboratifs est pleinement responsable des propos et des messages qu'il échange vis-à-vis du Groupement. Dans ce contexte, il est rappelé que l'Utilisateur est susceptible d'engager également la responsabilité du Groupement et qu'il doit toujours veiller à ne pas porter atteinte aux intérêts à la réputation ou à l'image du Groupement. De même, et conformément à l'article 5, il doit s'assurer de ne pas porter atteinte à la Confidentialité des Informations du Groupement (pas de publication d'Informations internes, techniques, commerciales ou organisationnelles par exemple).

L'Utilisateur, utilisant les réseaux sociaux internes du Groupement, veillera à en respecter strictement les conditions générales d'utilisation et, en particulier :

- Ne pas faire figurer de Documents confidentiels du Groupement ;
- Veiller à la sécurité des Documents qu'il publie.

f) Messagerie électronique

Les dispositions qui suivent sont applicables à tous les dispositifs de messagerie électronique que leur support soit fixe ou mobile.

L'accès à la messagerie électronique du Groupement est mis à disposition des Utilisateurs pour un usage professionnel. Il est paramétré et administré à cet effet.

Pour des impératifs de disponibilité, de performance des Ressources, les messages doivent rester limités en volume et en nombre. La STIME se réserve le droit de limiter la taille maximum des messages, des boîtes aux lettres et de certains types de fichiers attachés.

La diffusion d'un message doit faire l'objet d'une attention particulière quant à la pertinence de la liste des destinataires, sa présentation, son contenu, sa taille. L'Utilisateur veillera à appliquer les règles suivantes :

- Libeller explicitement l'objet du message ;
- Utiliser les listes de diffusion internes et externes avec précaution dans le cadre strict fixé par le Groupement. Toute utilisation des listes de diffusion internes et externes en dehors de leur finalité initiale, à des fins privées ou qui ne correspondent pas aux activités professionnelles nécessaires à l'accomplissement des missions de l'Utilisateur est interdite.

La messagerie n'est pas un canal de communication sécurisé dès lors qu'un message est adressé à l'extérieur du Groupement.

Si le Groupement a la capacité de maîtriser son réseau interne, il n'a en revanche aucune visibilité ni moyen d'action dès lors que les données transitent sur le réseau Internet public. Il convient donc de mesurer la sensibilité des Informations avant leur transmission à des Tiers à l'extérieur du Groupement avec ce moyen de communication.

Par ailleurs, il convient de noter que les mécanismes de protection de fichiers bureautiques par des mots de passe proposés dans les applications d'édition (Word, Excel, Powerpoint, PDF, etc.) n'apportent aucune protection efficace dans la mesure où de nombreux logiciels librement accessibles sur l'internet permettent de les outrepasser aisément. Seul le chiffrement offre des solutions adéquates.

Ainsi, si des impératifs professionnels nécessitent que l'Utilisateur échange avec un Tiers à l'extérieur du Groupement des Informations particulièrement Confidentielles, il s'adressera à la STIME pour obtenir une solution adaptée au besoin de Confidentialité attendu et compatible avec les Ressources du Groupement.

L'Utilisateur ne doit pas :

- Ouvrir les fichiers joints ni cliquer sur les liens issus de messages électroniques douteux et non sollicités. Tout message douteux, non légitime, non sollicité (expéditeur et nom de domaine inconnu, message sans objet, sujet racoleur ou séduisant etc..) devra être supprimé sans l'ouvrir ;
- Rediriger sa messagerie vers d'autres adresses appartenant ou non au Groupement ;
- Fournir des Informations personnelles en particulier si les Informations sont demandées dans un courrier électronique ou sur un site dont il n'a pas une confiance absolue ;
- Envoyer hors du réseau du Groupement des messages ou des pièces jointes avec des Informations à contenu classifié, sauf accord de sa hiérarchie, dans ce cas, les messages et pièces jointes devront être chiffrés, (en cas de besoin contacter la STIME) ;
- Utiliser la messagerie électronique professionnelle à des fins de « spamming » (envoi massif de messages électroniques non sollicités). L'envoi de messages électroniques en masse à l'ensemble de la collectivité des Utilisateurs est interdit sauf autorisation formelle de la direction des ressources humaines ou de la direction de la communication et de l'Information ;
- Répondre ni faire suivre les courriers électroniques alarmistes de provenance douteuse qui sont souvent des tentatives d'escroquerie (exemples : « chaines » de messages à vocation prétendument charitable) ou concernant de prétendus virus (en cas de doute contacter la STIME).

Le transfert automatique de messages électroniques vers une messagerie externe est interdit.

En cas de besoin, l'Utilisateur pourra solliciter un accès à distance à sa messagerie ou en déléguer l'accès.

L'envoi de nombreux messages sur des périmètres spécifiques doit respecter les procédures édictées localement et être autorisé par la hiérarchie.

L'utilisation des systèmes de courrier électronique basés sur le Web tels que les messageries Google, Yahoo, etc... n'est autorisée qu'au travers des dispositifs d'accès mis en place par le Groupement.

g) Messageries instantanées

Les forums de discussion, la messagerie instantanée et le « chat » fournis par le Groupement sont réservés à un usage exclusivement professionnel.

Hors les outils fournis par le Groupement, l'Utilisateur se connectant à un forum de discussion, messagerie instantanée ou « chat » est pleinement et seul responsable des propos et messages qu'il échange tant vis-à-vis du Groupement que des Tiers, extérieurs à cette dernière. II est toutefois informé qu'il agit au nom du Groupement et qu'il doit, en conséquence, veiller en permanence à ne pas porter atteinte aux intérêts de ce dernier. Sa participation doit toujours s'effectuer dans le cadre d'une totale transparence et, à ce titre, l'Utilisateur s'engage à ne pas intervenir de façon anonyme, ni utiliser de pseudonyme, ou emprunter une quelconque identité fictive.

h) Logiciels, programmes et Fichiers

Le téléchargement, installation, utilisation des logiciels, programmes et fichiers exécutables à titre professionnel sur les appareils nécessaires à l'accomplissement de ses fonctions sont strictement interdit sauf respect des exigences de Sécurité de la présente Charte et de l'autorisation de sa hiérarchie.

i) Périphériques nomades

Les Utilisateurs de périphériques nomades (ex : ordinateurs portables, tablettes, …) s'engagent à sécuriser et protéger scrupuleusement leur matériel et l'accès aux données qu'il contient, quel que soit l'endroit où ils se trouvent conformément à l'obligation de vigilance de l'article 7 b) de la présente Charte.

Tout Utilisateur devra connecter son ordinateur portable au réseau du Groupement aussi régulièrement que possible afin que les opérations de maintenance, de mise à niveau des moyens de protection soient effectuées conformément à la politique de sécurité du Groupement ou aux bonnes pratiques existantes en la matière.

Comme pour les postes fixes et dans les mêmes conditions, l'Utilisateur est informé que des contrôles périodiques sont effectués pour vérifier la bonne application des règles définies.

j) Téléphonie

L'Utilisateur s'engage à utiliser à des fins professionnelles les outils de téléphonie (téléphone fixe, mobile, télécopie, etc.) mis à sa disposition par le Groupement à ces fins.

Par exception au principe d'utilisation à des fins professionnelles, il toutefois est toléré un usage à titre privé des outils de téléphonie mis à disposition de l'Utilisateur par le Groupement, sous réserve que cet usage soit raisonnable et limité (notamment en volume), s'inscrive strictement dans le cadre des nécessités de la vie courante et familiale et soit conforme aux conditions précisées dans la présente Charte (ne pas gêner ou limiter en aucun cas l'usage professionnel de ces Ressources, leur maintenance ou leur sécurité, etc.).

Sur les télécopies ou fax qu'il transmet, l'Utilisateur veillera à vérifier avec attention les coordonnées du ou des destinataires, ainsi qu'à indiquer le cas échéant, le caractère confidentiel qu'ils revêtent conformément aux procédures mis en œuvre par le Groupement.

Le Groupement dispose d'un éventuel outil de gestion de flotte mobile qui doit permettre en cas de vol ou de perte d'effacement du contenu du terminal.

k) Réseaux sans fil

La technologie sans fil est une porte d'accès aux Ressources du Système d'Information du Groupement.

A ce titre, il est interdit à tout Utilisateur :

- De connecter des équipements sans fil non agréés au réseau interne du Groupement ;
- De configurer les matériels informatiques de manière à ce que ces derniers puissent être utilisés par d'autres équipements pour accéder aux Ressources du Groupement sans connexion filaire, par exemple en créant un réseau Wifi ;
- Dès lors qu'un matériel informatique est connecté au réseau filaire du Groupement, tout autre moyen de connexion sans fil, tels les dispositifs Bluetooth et Wifi, doit alors être désactivé.

l) Outils collaboratifs

Le Groupement met à la disposition de ses collaborateurs, partenaires, fournisseurs un espace collaboratif dont la fonction est de retrouver l'environnement de travail en mobilité, d'échanger des Documents et Informations avec des Tiers. On accède à cet espace collaboratif par des Moyens d'authentification ou si l'accès s'opère à partir de l'internet par des moyens renforcés (MFA, Authentification Multi-facteurs). Cet espace collaboratif se compose d'espaces internes réservés aux Utilisateurs qui disposent d'adresses électroniques mousquetaires et des espaces pour tous.

Les contenus publiés par les Utilisateurs de ces espaces collaboratifs le sont sous leur entière responsabilité. Ces informations doivent être conformes aux textes légaux et règlementaires.

De plus, dès lors qu'ils publient une photographie, ils en acceptent la publication ; dès lors qu'ils publient une photographie de groupe ils sont censés avoir recueilli le consentement des personnes figurant sur la photographie du groupe. Dans les deux hypothèses, les personnes représentées disposent d'un droit de retrait des photographies ou de floutage.

ARTICLE 11 : ACCES AUX RESSOURCES DES UTILISATEURS EN CAS D'ABSENCES ET DE DEPARTS

Chaque Utilisateur doit veiller à ce que la continuité de service soit assurée.

- En cas d'absence temporaire de l'Utilisateur

Pour des raisons de continuité de service, l'Utilisateur, lorsqu'il est absent, doit mettre en œuvre les délégations nécessaires permettant d'accéder à ses données professionnelles mais il ne doit pas communiquer ses propres codes d'accès à des Tiers.

L'Utilisateur doit, en outre, sauvegarder et archiver régulièrement les données qu'il exploite, qu'il crée ou qu'il transforme pour la continuité du service en utilisant les logiciels, matériels et/ou procédures mis à disposition par le Groupement et notamment les espaces réseaux.

Lorsque l'Utilisateur est absent, pour quelle que cause que ce soit (congés, maladie...), le Groupement pourra avoir accès, dans le respect de la présente Charte, à ses données de travail présumées professionnelles aux seules fins d'assurer la continuité du Service. Dans cette hypothèse, le Groupement tiendra informer l'Utilisateur de cet accès.

- En cas de départ définitif d'un Utilisateur

L'Utilisateur, lors de son départ définitif du Groupement doit notamment :

- Restituer les dossiers, répertoires, fichiers, courriers électroniques et plus généralement tout Document électronique à caractère professionnel afin de permettre la continuité du service ;
- Restituer, en bon état général de fonctionnement, l'ensemble des Équipements individuels et des moyens de connexion qui lui ont été remis ;
- Récupérer puis détruire ses données privées (répertoire personnel, fichiers, dossiers et messages électroniques identifiés par lui comme « privé »).

En cas de décès de l'Utilisateur, les données privées de l'Utilisateur sont conservées par le Groupement pendant une durée de six (6) mois.

Le départ définitif d'un Utilisateur entraine la suspension et/ou la suppression immédiate de son compte de messagerie ainsi que de ses accès et Habilitations selon les procédures en vigueur.

Si l'Utilisateur n'a pas procédé à la restitution, le Groupement pourra avoir accès, dans le respect de la présente Charte, à ses données de travail présumées professionnelles aux seules fins d'assurer la continuité du Service.

ARTICLE 12 : RESPONSABILITE DE L'UTILISATEUR

Outre le respect des dispositions de l'article 6 de la présente Charte relatif aux conditions d'utilisation des Ressources, l'Utilisateur est responsable :

- Dans le cadre de son activité professionnelle, de l'utilisation des Ressources du Groupement en conformité avec la présente Charte ;
- Dans la sphère de sa vie privée résiduelle, à l'exclusion de toute responsabilité du Groupement, de tout usage à caractère non professionnel des Ressources.

Le Groupement peut être amené à bloquer ponctuellement tout ou partie des Ressources mises à disposition de l'Utilisateur pour protéger son Système d'Informations ou dans un cadre disciplinaire.

Le Groupement déclare mettre en œuvre, par le biais notamment de la présente Charte, tous les efforts nécessaires à un bon usage de ses Ressources et n'assumer aucune responsabilité au titre des agissements fautifs et délictueux des Utilisateurs auxquels elle fournit un droit d'accès.

Le non-respect des règles et des mesures figurant dans la présente Charte peut engager la responsabilité personnelle de l'Utilisateur ou dans le cas d'un prestataire, la responsabilité de la société qui l'emploie. Dès lors qu'il est prouvé que des manquements lui sont personnellement imputables, l'Utilisateur s'expose à d'éventuelles sanctions disciplinaires, voire à des poursuites judiciaires conformément au droit applicable.

En conséquence, le non-respect par l'Utilisateur des principes susvisés et de la réglementation applicable, l'expose à des sanctions disciplinaires prévues et/ou à des poursuites judiciaires.

II en sera de même si le non-respect des présentes règles conduit la Haute Autorité pour la Diffusion des Œuvres et la Protection des droits sur Internet (L'Hadopi) ou la Commission Nationale de l'Informatique et des Libertés (CNIL) à adresser au Groupement plusieurs avertissements pour non-respect de la loi et/ou à prononcer une ou plusieurs sanctions à l'encontre de celle-ci.

ARTICLE 13 : CONVENTION DE PREUVE

Les registres informatisés, les registres d'exploitation, ainsi que tout autre élément de preuve informatique (traces informatiques, logs, etc.) dans les Systèmes d'Information du Groupement seront

conservés dans des conditions raisonnables de sécurité et seront considérés comme les preuves de son Utilisation.

ARTICLE 14 : LOI ET REGLEMENTATION APPLICABLE

Dans le cadre de l'usage des Ressources mises à sa disposition par le Groupement, l'Utilisateur s'engage au respect de la Charte, mais également au respect des dispositions législatives et réglementaires en vigueur.

Tout Utilisateur doit notamment respecter, sans que cette liste ait un caractère exhaustif, les règlementations précisées ci-après dont le non-respect peut être passible de sanctions disciplinaires et/ou à des sanctions pénales.

L'Utilisateur doit notamment respecter :

- L'image du Groupement Les Mousquetaires, et les dispositions en vigueur en matière de diffamation et de contenus manifestement illicites ;
- La réglementation relative aux libertés individuelles et les règles d'ordre public qui interdisent la mise en ligne sur le réseau du Groupement ou sur le réseau Internet d'Informations relatives, notamment, à la race ou à l'ethnie, aux opinions politiques, philosophiques ou religieuses, à l'appartenance syndicale, aux mœurs et à la vie sexuelle, ou encore portant atteinte à l'intégrité, à la réputation, à la vie privée ou à la sensibilité d'un autre Utilisateur, notamment par la mise en ligne de messages, de photographies, d'images de toute nature ou de textes provoquant ou incitant à la haine, à la violence, à la discrimination ou qui sont à caractère pornographique ;
- Les dispositions relatives au secret professionnel ;

- Les dispositions relatives aux droits de propriété intellectuelle. Dans ce cadre l'Utilisateur s'engage à :
    - Utiliser les logiciels, applications dans les conditions de la licence souscrite par le Groupement ;
    - Ne pas reproduire et utiliser les bases de données, pages web ou autres créations du Groupement ou de Tiers protégés par le droit d'auteur sans avoir obtenu préalablement l'autorisation du titulaire de ces droits ;
    - Ne pas diffuser toutes œuvres protégées par le droit d'auteur, telles que photographies, images, bases de données, œuvres audiovisuelles ou musicales, textes, etc. et, plus généralement toute création copiée sur le réseau internet sans vérifier qu'ils sont libres de droit ;
    - Ne pas copier, charger, télécharger, reproduire, diffuser ou exploiter, stocker, utiliser ou transmettre sous quelque forme que ce soit des programmes, logiciels, progiciels, enregistrements, fichiers, base de données, données et contenus de toute nature autres que ceux autorisés expressément par le Groupement, en l'absence d'autorisation expresse de ce dernier ;
    - Ne pas utiliser, de manière générale, les Ressources du Groupement pour copier, charger, télécharger, reproduire, diffuser ou exploiter, stocker, utiliser ou transmettre, par quelque moyen que ce soit, tous programmes, logiciels, progiciels, enregistrements, fichiers, base de données, données ou contenus protégé par des

droits de propriété intellectuelle sans avoir, au préalable, obtenu l'autorisation du titulaire de ces droits ;

- De manière générale, les Ressources ne doivent en aucune manière être utilisées à des fins de reproduction, de représentation, de mise à disposition ou de communication au public d'œuvres ou d'objets protégés par un droit d'auteur ou par un droit voisin, tels que des textes, images, photographies, œuvres musicales, œuvres audiovisuelles, logiciels et jeux vidéo, sans l'autorisation des titulaires des droits prévus dans le code de la propriété intellectuelle lorsque cette autorisation est requise.

- La réglementation relative à la protection des Données à caractère personnel, qui interdit notamment toute collecte et Traitement de données à l'insu des personnes concernées et encadre la notification des violations de Données à caractère personnel telle que prévue par la loi du 6 janvier 1978 modifiée, dite « Informatique et Libertés » (et par le Règlement européen de protection des données du 27 avril 2016).
- La réglementation relative aux atteintes aux Systèmes d'Information (articles 323-1 à 323-7 du code pénal) qu'il s'agisse notamment de manière frauduleuse de l'accès, du maintien, de l'entrave d'un système de Traitement automatisé de données, de l'extraction, de la reproduction, de la transmission de données ou de l'altération des éléments qu'il contient, étant précisé que ces actes sont passibles d'amendes et de peines de prison.

ARTICLE 15 : DROIT À LA DÉCONNEXION

Afin de garantir la protection de la santé ainsi que la vie privée et familiale des Utilisateurs, le Groupement les encourage à respecter leur droit à la déconnexion pendant leur temps de repos et pendant leurs congés. Une vigilance particulière doit être apportée aux outils et périphériques nomades. Pour ce faire, les Utilisateurs se reporteront le cas échéant aux procédures ayant fait l'objet d'un accord au sein de l'entité à laquelle ils appartiennent.

ARTICLE 16 : ENTREE EN VIGUEUR

La présente Charte annule et remplace toutes les précédentes Chartes de même nature émises par le Groupement relatives à l'utilisation Ressources. La présente Charte est un Document distinct de celui qui fixe les règles d'utilisation des moyens de communication électronique par les organisations syndicales et les instances représentatives du personnel.

Conformément aux dispositions du Code du travail, la présente Charte a été soumise, pour avis, préalablement à son entrée en vigueur, aux instances représentatives du personnel compétentes qui ont respectivement rendu des avis.

Ces avis ont été adressés à l'inspecteur du travail compétent en même temps que deux exemplaires de la présente Charte.

Cette Charte a été déposée en double exemplaire au secrétariat du greffe du Conseil de prud'hommes de LENS.

Enfin, celle-ci a été affichée sur les panneaux d'affichage obligatoire dans les locaux. Elle est disponible sur l'Intranet du Groupement, conformément aux dispositions du Code du travail. En complément, un mail a été adresse à l'ensemble des salaries avec un lien vers l'intranet leur permettant de consulter la Charte. En outre, la Charte sera remise lors de l'embauche de tout nouveau salarié, ainsi que de la réception de tout stagiaire, apprenti ou travailleur temporaire.

La Charte sera également annexée aux contrats de prestations de services et de propriété intellectuelle (prestataires externes et consultants).

La présente Charte entre en vigueur le 01 septembre 2023

L'Utilisateur a lu et approuvé les présentes le : …… à ……

En deux exemplaires originaux dont un (1) est remis à STIME et à l'Utilisateur.

Nom, Prénom et signature de l'Utilisateur :