Annexe 3

Charte Informatique
CMA Ile-de-France

Diffusion du document :
CMA Ile-de-France

Objet du document :
Ce document a pour but de régir l'utilisation des ressources des Systèmes d'Information (ci-après nommé « SI ») mises à disposition de toutes les personnes appelées à collaborer aux missions de la CMA Ile-de-France (ci-après nommée « la Chambre »).

Table des mises à jour du document :

Version	Date	Objet de la mise à jour	Auteur(s)
1.0	01/12/2020	Création du document	Yann BOUJEANT Sébastien RENARD Aurélien DELAUNAY

Sommaire

Préambule

Le secteur d'activité de services consulaires est astreint à un important niveau de sécurité des systèmes d'information. C'est pourquoi la présente charte a été mise en place.
Celle-ci concerne les ressources informatiques (matériel, logiciel, support de transport et/ou stockage d'information, infrastructures, etc.), les services Internet, de messagerie et téléphoniques, ainsi que tout autre moyen de connexion à distance permettant d'accéder, via le réseau informatique, aux services de communication ou de traitement électronique interne ou externe. Il s'agit principalement des outils suivants : ordinateurs portables et fixes, tablettes tactiles, téléphones portables et fixes, imprimantes, logiciels.
Ces ressources font partie du patrimoine de la Chambre et sont sa propriété.
Avec l'évolution du numérique, il devient difficile de séparer la vie professionnelle et la vie privée. C'est pourquoi il est important de rappeler que ces ressources sont mises à disposition des utilisateurs à des fins strictement professionnelles.
Cette charte s'applique à l'ensemble des utilisateurs des SI de la Chambre, à savoir notamment :
- les agents soumis au statut du personnel, contractuels, stagiaires et titulaires, occupant un emploi permanent, à temps complet ou à temps partiel,
- les élus de la Chambre,
- toute personne appelée à consulter, créer ou mettre en œuvres ces ressources,
- de façon générale, toute personne appelée à collaborer aux missions de la Chambre, en vertu d'un engagement, accepté par ce dernier, ou en vertu d'un contrat de prestations de services.

La négligence ou la mauvaise utilisation des ressources fait courir des risques à l'ensemble de l'entreprise.
Par ailleurs, le Code de la Propriété Intellectuelle protège le droit de propriété attaché aux logiciels et aux données (textes, images et sons).
Concernant Internet, l'ensemble des règles juridiques existantes ont vocation à s'appliquer lors de son utilisation.
Il résulte, de l'application de ces dispositions légales, des règles internes qu'il est demandé à chacun de respecter.
Le non-respect de la présente charte peut être considéré comme une faute professionnelle susceptible d'entraîner pour l'utilisateur des sanctions disciplinaires, sans préjudice d'éventuelles actions pénales ou civiles à son encontre.
Cette charte peut être complétée par des chartes directionnelles, des annexes techniques ou des dispositions spécifiques à certains services.

1. Cadre juridique

Le cadre règlementaire de la sécurité de l'information est complexe. Chaque utilisateur se doit de respecter les règles juridiques applicables, notamment en matière :

- de respect des règles déontologiques et professionnelles,
- de respect des procédures de travail,
- de respect de l'organisation et des règles de délégation,
- de communication d'informations,
- d'utilisation des moyens informatiques mis à sa disposition dans le cadre de sa fonction.

L'utilisation de l'informatique est encadrée par une législation très stricte visant à protéger d'une part les atteintes aux droits de la personne résultant de l'utilisation des fichiers ou traitements informatiques, d'autre part les atteintes aux systèmes de traitement automatisé de données.
La Chambre applique notamment les textes portant sur :

- la protection des données personnelles au titre de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés ainsi que du règlement européen 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 » [UE 2016/679] 2 ;
- les droits et obligations des fonctionnaires, au titre des lois n° 83-634 du 13 juillet 1983 et n° 2016-483 du 20 avril 2016 ;
- l'obligation de collecte de traces sur internet au titre de la loi n° 2006-64 du 23 janvier 2006 relative à la lutte contre le terrorisme et portant dispositions diverses relatives à la sécurité et aux contrôles frontaliers ;
- le respect du droit d'auteur au titre de la loi n° 2006-961 du 1er août 2006 relative au droit d'auteur et aux droits voisins dans la société de l'information (DADVSI);
- la législation sur la propriété intellectuelle (code de la propriété intellectuelle) ;
- la lutte contre le téléchargement illégal au titre de la loi n° 2009-669 du 12 juin 2009 favorisant la diffusion et la protection de la création sur internet (dite loi HADOPI).
- L'accessibilité pour tous aux informations diffusées par les services de communication publique en ligne de l'Etat, des collectivités territoriales et des établissements publics qui en dépendent au titre de l'article 47 de la loi n°2005-102 du 11 février 2005 pour l'égalité des droits et des chances, la participation et la citoyenneté des personnes handicapées ;
- L'ordonnance n°2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives ;
- L'interopérabilité au sein des systèmes d'information de l'administration au titre de l'arrêté du 9 novembre 2009 (modifié par l'arrêté du 20 avril 2016) portant approbation du référentiel général d'interopérabilité (RGI) ;
- Les règles de sécurité au titre de l'arrêté du 6 mai 2010 (modifié par l'arrêté du 10 juin 2015) portant approbation du référentiel général de sécurité (RGS) ; l'administration assure le respect des objectifs et principes généraux de la politique générale de sécurité des systèmes pour l'administration (PGSSI des MEF du 1er août 20163). Elle met notamment en place un processus de gestion des risques de sécurité des SI. Chaque entité administrative applique des procédures de surveillance afin de détecter les événements pouvant porter atteinte à la sécurité de ses SI et assure une gestion des incidents de sécurité ;
- Les règles de protection appropriée des SI sensibles contre toutes les menaces, qu'elles soient d'origine humaine ou non (Instruction interministérielle n°901 relatives à la protection des systèmes d'informations sensibles.

2. Confidentialité de l'information et obligation de discrétion

L'utilisateur est soumis, en fonction de son emploi, au secret professionnel ou à une obligation de discrétion professionnelle. L'utilisateur doit assurer la confidentialité des données qu'il détient.
La création et l'utilisation de fichiers contenant des informations nominatives doivent être réalisées en conformité avec les dispositions du règlement général à la protection des données (RGPD).
Une utilisation des matériels mis à disposition et une communication (orale ou écrite, téléphonique ou électronique) appropriée est exigée dans toute communication, que ce soit lors d'échanges professionnels ou au cours de discussions relevant de la sphère privée.
L'accès par les utilisateurs aux informations et documents conservés sur les systèmes informatiques doit être limité à ceux qui leur sont propres, ainsi que ceux publics ou partagés. Il est ainsi interdit de prendre connaissance des informations détenues par d'autres utilisateurs, même si ceux-ci ne les ont pas explicitement protégées. Cette règle s'applique en particulier aux données couvertes par le secret professionnel, ainsi qu'aux conversations privées de type courrier électroniques dont l'utilisateur n'est ni directement destinataire, ni en copie.
A l'exception des agents dûment habilités par la Chambre, la participation des agents sur les réseaux sociaux, forums de discussion, blogs, etc. est fortement déconseillée. Il est rappelé que les agents s'expriment au nom de la Chambre, dans la limite de leur fonction et dans le respect du secret professionnel. De plus, ils doivent faire preuve de modération et de courtoisie dans leur propos.
L'utilisateur doit assurer la confidentialité des données qu'il détient. En particulier, il ne doit pas diffuser à des tiers, au moyen d'une messagerie non sécurisée, des informations nominatives et/ou confidentielles couvertes par le secret professionnel.
Dans certains services comportant des données sensibles, la Chambre édicte des règles auxquelles les utilisateurs sont tenus de se conformer. Les informations classifiées, en particulier, font l'objet de dispositions spécifiques.
Lorsqu'ils traitent d'informations qualifiées de « sensibles » ou « confidentielles » par l'administration ou par ses interlocuteurs (partenaires, fournisseurs, usagers…), les utilisateurs doivent avoir recours aux moyens de chiffrement mis à leur disposition par ceux-ci afin de les protéger d'un risque de compromission.

3. Protection de l'information

Les documents bureautiques produits doivent être stockés sur des serveurs de fichiers ou dans les environnements Cloud mis à disposition par la Chambre (Teams, OneDrive, etc.).
Ces espaces sont à usage professionnel uniquement, le stockage de données privées sur ces espaces est interdit.
Les médias de stockage amovibles (clefs USB, CD, disques durs, etc…) présentent des risques très forts vis-à-vis de la sécurité : risques importants de contamination par des programmes malveillants ou risque de perte de données. Leur usage doit donc être fait avec une très grande vigilance. La Chambre se réserve le droit de limiter voire d'empêcher l'utilisation de ces médias en bloquant les ports de connexion des outils informatiques.

4. Usage des ressources informatiques

A. Mesures de la Chambre

Seules les personnes autorisées par la Direction des Systèmes d'Information (ci-après nommée « DSI ») ont le droit de :

- installer de nouveaux logiciels ou matériels,
- connecter de nouveaux équipements au réseau,
- déménager des équipements informatiques (hors PC portables).

Les matériels et logiciels informatiques sont réservés à un usage exclusivement professionnel et ne doivent pas être utilisés à des fins personnelles, sauf autorisation préalable de la DSI.
Par défaut, les usages et contenus sont considérés professionnels ; seuls les espaces, répertoires, fichiers et/ou messages qualifiés expressément de « personnels » ou de « privés » seront considérés comme tels.
Dans tous les cas, y compris pour un usage privé, l'utilisation doit être conforme à l'ordre public et ne doit pas mettre en cause ou porter atteinte à l'intégrité, à la réputation ou à l'image de la Chambre.
Conformément aux dispositions légales et réglementaires, il est également interdit à tout utilisateur de copier un logiciel informatique, d'utiliser un logiciel "piraté", et plus généralement, d'introduire au sein de la chambre un logiciel qui n'aurait pas fait l'objet d'un accord de licence. La Chambre se réserve le droit de détruire le logiciel utilisé en violation de ces dispositions.
La Chambre peut limiter ou interdire le téléchargement de certains fichiers volumineux ou présentant un risque pour la sécurité des SI (virus susceptibles d'altérer le bon fonctionnement du système d'information, codes malveillants, programmes espions, etc.) ou l'accès à certaines ressources en *streaming*.
L'utilisation de services sur Internet non mis à disposition par la DSI tels que des outils de stockage (par exemple, de manière non exhaustive : Google Drive, Dropbox, etc.), de rédaction communautaire ou d'assistance à distance (prise en mains à distance) ou de visioconférence est interdite. L'utilisation de solution de visioconférence en tant que participant est autorisée dès lors qu'il n'y a pas de logiciel spécifique sur le poste de travail.
Même si l'accès aux sites est possible, l'utilisateur doit faire preuve de vigilance lorsqu'il télécharge un fichier provenant d'une source non professionnelle. Par exception, les projets collaboratifs conduits avec certains acteurs (tiers de confiance, entreprises partenaires, etc.) pourront justifier la levée totale ou partielle des restrictions d'accès à ces outils de stockage ou de partage, sous réserve de la validation de la DSI.
A l'exception des ordinateurs portables mis à la disposition des salariés, aucun matériel ni logiciel informatique appartenant à la Chambre ne peut être sorti de celle-ci sans autorisation préalable écrite de la Direction du site concerné et après une information préalable de la DSI.
Lors de son départ définitif de la Chambre, chacun est tenu de restituer les matériels, logiciels et documentations informatiques, qui lui auront été confiés en vue de l'exécution de son travail, et ce, en bon état (en tenant compte de l'usure et de la vétusté).

B. Engagements de l'utilisateur

Chaque utilisateur s'engage à :

- Ne pas modifier la configuration des ressources (matériel, réseaux, etc…) mise à sa disposition, sans avoir reçu l'accord préalable et l'aide des personnes habilitées dans la Chambre,
- Ne pas faire de copies des logiciels commerciaux acquis par la Chambre,
- Ne pas installer, télécharger ou utiliser sur le matériel des logiciels ou progiciels dont les droits de licence n'ont pas été acquittés, ou ne provenant pas de sites dignes de confiance, et sans autorisation la DSI,
- Ne pas apporter volontairement des perturbations au bon fonctionnement des ressources informatiques et des réseaux que ce soit par des manipulations anormales du matériel ou par l'introduction de logiciels parasites (virus, chevaux de Troie, etc…),
- Ne pas empêcher ou différer les mises à jour des systèmes d'exploitation et des logiciels, notamment de sécurité sur son poste de travail,
- Ne pas connecter directement aux réseaux locaux des matériels autres que ceux confiés ou autorisés,
- Informer immédiatement la DSI de toute perte, anomalie ou tentative de violation de ses codes d'accès personnels,
- Effectuer une utilisation rationnelle et loyale des services et notamment du réseau, de la messagerie, des ressources informatiques, afin d'en éviter la saturation ou l'abus de leur usage à des fins personnelles,
- Limiter les impressions papier à ce qui est nécessaire,
- Récupérer sur les matériels d'impression (imprimantes, télécopieurs) les documents sensibles envoyés, reçus, imprimés ou photocopiés,
- Ne pas quitter son poste de travail en laissant accessible une session en cours et à ne pas se connecter sur plusieurs postes à la fois,
- Ne pas empêcher l'accès à son poste de travail professionnel aux utilisateurs chargés de la maintenance des matériels,
- Respecter les modalités de sollicitation de la DSI pour la résolution des problèmes techniques qu'ils constatent,
- En cas de prise en main de son poste de travail par le Support Informatique :

    ·autoriser l'agent de la DSI à prendre en main à distance son poste de travail (sans autorisation, la connexion n'aura pas lieu),

    ·être vigilant et notamment rester présent devant son poste de travail durant l'intervention,

    ·fermer les applications informatiques et les fichiers ouverts sur son poste de travail, notamment les documents sensibles ou classifiés,

    ·mettre fin à la prise ne main s'il estime qu'il existe un risque de sécurité,

    ·s'assurer que la session de prise en main est fermée en fin d'intervention.

5. Respect du réseau informatique

L'utilisation du réseau doit se faire dans le respect des autres utilisateurs.
Il est demandé à chacun de ne pas effectuer d'opérations qui pourraient avoir pour conséquence :

- d'interrompre ou de perturber le fonctionnement du réseau ou d'un système connecté au réseau,
- d'accéder à des informations privées d'autres utilisateurs du réseau,
- de modifier ou de détruire des informations sur un des systèmes connectés au réseau.

L'accès au réseau est soumis à une identification préalable de l'utilisateur, qui dispose alors d'un "compte d'accès personnel" aux ressources et services.
Ce dernier est constitué d'un identifiant et d'un mot de passe strictement personnel et confidentiel.
L'utilisateur est responsable de son compte et de son mot de passe, et de l'usage qu'il en fait. Il ne doit pas masquer son identité sur le réseau local ou usurper l'identité d'autrui en s'appropriant le mot de passe d'un autre.

Un mot de passe solide :

- est généralement constitué d'au moins 12 caractères de 4 types différents : des minuscules, des majuscules, des chiffres et des caractères spéciaux,
- ne fait pas référence à des données qui vous sont personnelles (ex : prénom de votre enfant, votre date de naissance etc.),
- doit être à usage unique (chaque site ou application possède son propre mot de passe),
- ne doit pas être écrit sur un post-it, un fichier texte, etc.,
- ne doit pas être enregistré sur le navigateur d'un ordinateur partagé,
- doit être renouvelé avec une fréquence raisonnable (90 jours maximum).

Il faut modifier systématiquement et au plus tôt tous les mots de passe généré par défaut par les systèmes initialement.

6. Usage des outils de communication

Les outils de communication tels que le téléphone, le fax, Internet ou la messagerie électronique sont destinés à un usage exclusivement professionnel et ne doivent pas être utilisés à des fins personnelles.
La Chambre tolère un usage exceptionnel, à des fins autres que professionnelles, des ordinateurs et des technologies de l'information et des communications, notamment Internet et des courriers électroniques ne mettant pas en cause le temps de travail, n'affectant pas le bon fonctionnement et ne portant pas atteinte à l'intérêt collectif de la Chambre.
Cette utilisation, à des fins personnelles, depuis le lieu de travail, est tolérée pendant les temps de pause ou pour des besoins urgents de la vie privée du salarié.
Elle doit être occasionnelle et raisonnable (tant dans la fréquence que dans la durée), conforme à la législation en vigueur et ne pas porter atteinte à la sécurité et à l'intégrité des SI ainsi qu'à l'image de marque de la Chambre.
Dans le cadre de la téléphonie, il est interdit de transférer la ligne fixe vers un numéro externe à la Chambre sauf en cas d'autorisation explicite et écrite de la Direction du site concerné, par exemple dans le cadre du télétravail.
A l'exception des téléphones et tablettes portables mis à la disposition des salariés, aucun matériel de communication appartenant à la Chambre ne peut être sorti de celle-ci sans autorisation préalable de la Direction.

A. Accès à Internet – navigation sur le WEB

Les données concernant l'utilisateur (sites consultés, messages échangés, etc…) peuvent être enregistrées par des tiers, analysées et utilisées à des fins notamment commerciales. Il est donc recommandé à chaque utilisateur de ne pas fournir son adresse électronique professionnelle, ni aucune coordonnée professionnelle sur Internet, si ce n'est strictement nécessaire à la conduite de son activité professionnelle.
En dehors des connexions directes au réseau professionnel, les accès aux réseaux en mobilité (wifi ou autres) ne sont autorisés que via des logiciels fournis par la Chambre.
Par exemple, la navigation sur le Web est interdite dans un café, ou sur un autre wifi public, sans connexion préalable au VPN.

L'utilisateur est informé que les traces de la navigation sont temporairement archivées. En effet, à la demande d'une autorité judiciaire ou administrative, la DSI devra fournir les informations de la navigation web.
La Chambre se réserve le droit de :

- contrôler le contenu de toute page Web hébergée sur ses serveurs en vue de s'assurer du respect des conditions d'utilisation des services énoncées par la présente Charte,
- suspendre l'usage du service d'hébergement des pages Web par un utilisateur en cas de non-respect de la Charte et notamment dans l'hypothèse où l'utilisateur aurait diffusé sur ses pages Web un contenu manifestement illicite.

L'utilisateur s'engage à respecter les règles suivantes :

- Interdiction de consulter ou télécharger du contenu de sites web à caractère pornographique, pédophile ou tout autre site illicite ou contraire aux bonnes mœurs,
- Interdiction de télécharger des fichiers musicaux ou vidéo hors contexte professionnel,
- Pour participer à des forums, l'utilisateur doit disposer d'autorisations internes afin de s'exprimer au nom de la Chambre,
- Les téléchargements de contenu illicite sont interdits (contrefaçon de marque, copie de logiciels commerciaux, etc.).

De manière générale, les utilisateurs sont invités à faire preuve de sens critique vis-à-vis des contenus disponibles sur Internet hors sources réglementaires fiables (législation européenne, nationale, information institutionnelle).

Il est également rappelé que certains sites Internet sont régis par le droit d'autres États n'offrant pas de garanties de protection des données personnelles. L'utilisateur est incité à prendre toutes les précautions utiles lorsqu'il les consulte.

La consultation de sites Web à titre privé est tolérée à titre exceptionnel et à condition que la navigation n'entrave pas l'accès professionnel et qu'elle s'effectue hors du temps de travail de l'utilisateur.

B. Messagerie électronique

Elle est réservée à un usage professionnel.
La messagerie électronique peut être utilisée exceptionnellement à des fins personnelles à la condition de ne pas affecter le trafic normal des messages professionnels.
Il appartient à l'utilisateur d'identifier les messages qui sont personnels par la mention « personnel » ou « confidentiel » dans l'objet du message.
A défaut d'une identification, les messages sont présumés être professionnels. La Direction se réserve le droit de contrôler le nombre de messages échangés, la taille des messages échangés et le format des pièces jointes.
Toutefois, l'inscription volontaire à une liste de diffusion sans lien avec l'activité professionnelle est interdite.
Afin de ne pas surcharger les serveurs de messagerie, il est attendu de chaque utilisateur, une gestion des messages (suppression, effacement périodique) et de la taille des pièces jointes envoyées.
L'utilisateur doit également veiller à bien cibler les destinataires et à éviter les envois inutiles, notamment avec des pièces jointes volumineuses.

L'utilisateur ne doit pas télécharger de pièces jointes de messages électroniques dont le contenu ou l'origine paraissent douteux, et ne pas cliquer sur des liens qui leur paraîtraient suspects. En cas de doute, l'utilisateur doit interroger le Support Informatique.

Il est interdit diffuser de messages de type canulars (hoax), chaînes, escroquerie par hameçonnage (phishing), jeux, paris, etc.

Il est important que l'utilisateur n'emploie pas son adresse électronique professionnelle dans un contexte non professionnel, en particulier, ne pas l'utiliser sur des sites internet (groupes de discussion (chats), commerce, forums, blogs, etc…), sans rapport avec l'activité professionnelle.

Rediriger manuellement ou automatiquement les messages professionnels qu'il reçoit sur sa messagerie professionnelle vers une messagerie personnelle n'est pas permis à l'utilisateur.

Tout constat de vol de matériel ou de données, d'usurpation d'identité, de détournement de moyen, de réception de messages interdits, de fonctionnement anormal ou de façon plus générale toute suspicion d'atteinte à la sécurité ou manquement substantiel à cette charte doit être signalé à son responsable hiérarchique.

L'utilisateur doit respecter les libertés individuelles et la protection des informations individuelles : est interdit tout message à caractère diffamatoire, insultant, malveillant, menaçant, violent, pornographique qui pourrait porter atteinte à l'intégrité ou la sensibilité des personnes.

7. Droit à la déconnexion

Le droit à la déconnexion, introduit par la loi du 8 août 2016 et l'article L 2242-17 du code du travail, s'entend comme le droit de chaque utilisateur de ne pas répondre aux courriels et autres messages en dehors des heures de travail, afin de garantir l'équilibre entre vie professionnelle et vie privée, les temps de repos et de récupération, de réguler la charge mentale et réduire les risques de burn-out.

8. Utilisation des outils numériques pour favoriser le droit d'expression

Le droit d'expression directe et collective des utilisateurs vise à définir les actions à mettre en œuvre pour améliorer l'organisation et les conditions de travail, ainsi que la qualité du travail réalisée au sein de l'équipe ou de la Chambre.
Les outils numériques disponibles dans la Chambre peuvent être utilisés pour favoriser ce droit d'expression. Il en est ainsi notamment :

- des outils comme les réseaux sociaux de la Chambre ou les forums,
- pour des échanges en direct : des outils de visioconférence ou de messagerie instantanée avec vidéo,
- d'autres modalités de recueil d'expression comme les baromètres sociaux.

9. Cas du personnel de la DSI

Le personnel de la DSI met en œuvre et assure le bon fonctionnement des SI, et notamment des dispositifs de sécurité de l'accès aux données.

Les exploitants et administrateurs qui assurent le fonctionnement des SI mettent en œuvre des outils de supervision technique en conformité avec les règles de sécurité des SI et celles relatives à la protection de la vie privée.

Seuls les personnels de la DSI qui contribuent à la sécurité des SI peuvent mettre en œuvre des outils d'analyse, de surveillance et de contrôle de sécurité dans le cadre défini par leur hiérarchie, en conformité avec les règles de sécurité des SI.
Les personnels de la DSI ne peuvent divulguer des informations professionnelles ou relatives à des utilisateurs, sauf dans le cadre de demandes d'autorités dûment habilitées (autorités judiciaires notamment).

Les services en charge des SI signalent à leur hiérarchie tout usage abusif des ressources informatiques mises à disposition des utilisateurs : surcharge de la bande passante, téléchargements massifs, saturation des espaces disques partagés, etc.

10. Cas du télétravail

Le télétravail désigne une forme d'organisation du travail dans laquelle un travail, qui aurait pu être exécuté dans les locaux de la Chambre, est effectué par un agent hors de ces locaux, de façon régulière et volontaire en utilisant les technologies de l'information et de la communication. Il se pratique au domicile de l'agent – entendu comme le lieu de sa résidence habituelle – ou, le cas échéant, dans des locaux professionnels distincts de son lieu d'affectation.
Le télétravailleur bénéficie des mêmes droits et est soumis aux mêmes obligations que les agents travaillant sur site, tels que décrits dans la présente charte.
La Chambre met à la disposition de l'agent le matériel lui permettant d'exercer son activité professionnelle à son domicile et en assure la maintenance. Les équipements fournis restent la propriété de la Chambre.
Le télétravailleur ne peut utiliser un autre matériel que celui fourni par la Chambre. Il s'engage à réserver l'usage des équipements mis à disposition par la Chambre à un usage strictement professionnel et à prendre soin de l'équipement qui lui est confié.
Les règles relatives à la sécurité des SI et de protection des données pour les agents en fonctions sur le site s'appliquent aux agents en télétravail. Ainsi, ceux-ci doivent se conformer aux règles relatives à la sécurité des SI et veiller à l'intégrité et à la bonne conservation des données auxquelles ils ont accès dans le cadre professionnel.
Les télétravailleurs ne doivent pas installer de logiciels non autorisés par la DSI sur le matériel qui leur a été fourni.
Ils s'engagent également à respecter la confidentialité des informations détenues ou recueillies dans le cadre de leur activité et à veiller à ce qu'elles ne soient pas accessibles à des tiers.
Ils informent sans délai leur responsable hiérarchique ainsi que le Support Informatique en cas de panne, de mauvais fonctionnement, de détérioration, de perte ou de vol du matériel mis à disposition.

11. Informatique et libertés

Un recours croissant à l'usage des technologies de l'information exige que chacun respecte les principes du droit à la protection des données personnelles dans ses deux volets : droits individuels et obligations.
Toute création ou modification de fichier comportant des données nominatives ou indirectement nominatives doit, préalablement à sa mise en œuvre, être déclarée auprès d'un des correspondants RGPD (via les adresses emails disponibles) qui étudie alors, avec l'aide du délégué à la protection des données (DPO) si nécessaire, les éléments suivants :

- pertinence des données recueillies ;
- finalité du fichier ;
- durées de conservation prévue ;
- destinataires des données ;
- moyen d'information des personnes fichées ;
- mesures de sécurité à déployer pour protéger les données.

Le délégué à la protection des données permet de garantir la conformité de la Chambre à la loi Informatique et Libertés et au règlement général de protection des données.
Cette maîtrise des risques juridiques est d'autant plus importante que la plupart des manquements à la loi du 6 janvier 1978 sont pénalement sanctionnés.
En cas de non-respect des obligations relatives à la loi informatique et libertés, le délégué à la protection des données sera informé et pourra prendre toutes mesures nécessaires pour mettre fin au traitement illégal ainsi qu'informer le responsable hiérarchique de l'utilisateur à l'origine du traitement illégal.

12. Surveillance du système d'information

C. Contrôle

Pour des nécessités de maintenance, de gestion, et des conditions d'usages professionnels optimales, l'utilisation des ressources matérielles ou logicielles, les échanges via le réseau, ainsi que les rapports des télécommunications peuvent être analysés et contrôlés dans le respect de la législation applicable, et notamment de la loi Informatique et Libertés.
L'utilisateur est informé que pour effectuer la maintenance corrective, curative ou évolutive, le personnel de la DSI dispose de la possibilité de réaliser des interventions (le cas échéant à distance) sur les ressources mises à sa disposition, et qu'une maintenance à distance est précédée d'une information de l'utilisateur.
Réseau : La Chambre peut vérifier à posteriori l'identité de l'utilisateur ayant accédé ou tenté d'accéder à une application au moyen du compte utilisé pour cet accès ou cette tentative d'accès.
Internet : La Chambre dispose des moyens techniques pour procéder à des contrôles de l'utilisation de ses services.
Ces contrôles techniques peuvent être effectués dans un souci de sécurité du réseau et/ou des ressources informatiques.
Pour des nécessités de maintenance et de gestion technique, l'utilisation des services et notamment des ressources matérielles et logicielles, ainsi que des échanges via le réseau peuvent être analysés et contrôlés dans le respect de la législation applicable et notamment dans le respect des règles relatives à la protection de la vie privé et au respect des communications privées.
La Chambre se réserve, dans ce cadre, le droit de recueillir et de conserver les informations nécessaires à la bonne marche du système. Elle se réserve la possibilité de procéder à un contrôle des sites visités afin d'éviter l'accès à des sites illicites ou requérant l'âge de la majorité. L'usage privé

des ressources informatiques peut être restreint par la Chambre, notamment dans un souci de bon usage des ressources.

D. Traçabilité

La Chambre assure une traçabilité sur l'ensemble des accès aux applications et aux ressources informatiques qu'elle met à disposition pour des raisons d'exigence règlementaire de traçabilité, de prévention contre les attaques et de contrôle du bon usage des applications et des ressources.
Par conséquent, les applications de la Chambre, ainsi que les réseaux, messagerie et accès Internet intègrent des dispositifs de traçabilité permettant le contrôle si besoin de :

- L'identifiant de l'utilisateur ayant déclenché l'opération,
- L'heure de la connexion,
- Le logiciel ou programme utilisé.

Le personnel de la DSI respecte la confidentialité des données et des traces auxquelles il est amené à accéder dans l'exercice de ses fonctions, mais peut être amené à les utiliser pour mettre en évidence certaine manquements commis par les utilisateurs.

13. Alertes

Tout constat de vol de matériel ou de données, d'usurpation d'identité, de détournement de moyen, de réception de messages interdits, de fonctionnement anormal ou de façon plus générale toute suspicion d'atteinte à la sécurité ou manquement substantiel à cette charte doit être signalé à son responsable hiérarchique et au délégué à la protection des données.

14. Responsabilités

L'attention du personnel est attirée sur le fait qu'en cas d'atteinte à un de ces principes protégés par la loi, la responsabilité pénale et civile de la personne, ainsi que celle de la Chambre est susceptible d'être recherchée.
L'utilisateur qui ne respectera pas les règles juridiques applicables, notamment celles rappelées ci-dessus, verra sa responsabilité juridique personnelle engagée non seulement par toute personne ayant subi un préjudice du fait du non-respect de ces règles, mais aussi de la Chambre en sa qualité d'employeur.
La Chambre ne pourra être tenue pour responsable des détériorations d'informations ou des infractions commises par un utilisateur qui ne se sera par conformé aux règles d'accès et d'usage des ressources informatiques et des services internet décrit dans la Charte.

15. Statut de la charte

La présente charte est annexée au règlement des services. Elle a été préalablement soumise pour avis à la commission paritaire locale lors de sa séance du 30/11/2020.
Sa date d'entrée en vigueur est fixée au 01/01/2021.
Un exemplaire sera mis à disposition de chaque utilisateur. Elle pourra être librement consultée sur l'« espace Ressources Humaines » de la Chambre.