Dernière mise à jour :
18 décembre 2019

Communauté d'Agglomération Sophia Antipolis

CHARTE DE BON USAGE DES SYSTEMES D'INFORMATION ET DE COMMUNICATION

Table des matières

1 Préambule

1. La présente charte de bon usage des *systèmes d'information et de communication* de la Communauté d'Agglomération Sophia Antipolis (ci-après « la C.A.S.A. ») a pour objet de fixer les règles d'utilisation des *systèmes d'information et de communication* mis à la disposition des *utilisateur*s, dans le cadre de leur activité professionnelle. Elle remplace la précédente charte de bon usage des technologies de l'information et de la communication du 1er janvier 2012.

2. Les règles ainsi définies sont destinées à assurer un niveau optimum de sécurité, de confidentialité et de performance d'usage des systèmes d'information et de communication, en conformité avec les dispositions légales et réglementaires applicables et avec la jurisprudence des Cours et Tribunaux.

3. La performance des services de la C.A.S.A. nécessite la mise en place régulière de nouveaux outils pour mieux gérer l'information. Ce déploiement d'équipements doit s'accompagner d'une maîtrise des risques, tant sur le plan de la sécurité informatique et technique, que sur le plan juridique et financier. Des solutions techniques sont mises en œuvre pour diminuer ces risques, mais le comportement des *utilisateur*s reste prépondérant.

4. La présente charte tient compte notamment des recommandations de la Commission nationale de l'informatique et des libertés (Cnil) et de celles de l'Agence nationale de la sécurité des systèmes d'information (Anssi).

5. La charte est rédigée dans le souci de concilier les intérêts de chaque *utilisateur* et ceux de la C.A.S.A.. Elle manifeste ainsi la volonté de la C.A.S.A. d'assurer un usage loyal, respectueux et responsable de ses systèmes d'information et de communication, ainsi que sa volonté de protéger son patrimoine et son image de marque.

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

7. La charte ne couvre pas de façon exhaustive tous les cas de figure susceptibles de se présenter dans le cadre de l'utilisation des *systèmes d'information et de communication* mis à la disposition des *utilisateur*s. Par conséquent, dans des situations non envisagées, c'est à l'esprit des règles édictées dans cette charte que chacun devra se conformer.

8. La charte pourra évoluer en fonction du contexte légal et de la politique de sécurité notamment applicable au sein de la C.A.S.A..

2 Définition

9. Les termes ci-dessous, au singulier ou au pluriel, ont la signification suivante :

- «*systèmes d'information et de communication*» : ressources et moyens informatiques et moyens de communication électroniques, recouvrant tout matériel informatique, câblage, périphériques (tels que les imprimantes simples ou multifonctions, les webcam, etc.), disquettes, disques durs externes ou internes, cartes mémoire, CD-Rom, clés USB, ordinateurs, tablettes, PDA, photocopieurs, routeurs, scanners, radiographies, etc… et toute ressource informatique de toute nature (logiciels, *application*s, bases de données, etc., et ce, qu'ils soient accessibles à distance, directement ou en cascade à partir d'un réseau ou d'un cloud), ainsi que les moyens de communication électronique recouvrant internet et les télécommunications (tels que les téléphones, les équipements sans fil, les cartes de communication sans fil, y compris les réseaux, les terminaux portables, les matériels nomades, les messageries, les forums, les sites web, etc.) ;

- « *administrateur* » : personne spécialement compétente en informatique, habilitée par la C.A.S.A. à assurer le fonctionnement normal de tout ou partie de ses *systèmes d'information et de communication* et à veiller à leur sécurité et/ou personne qui dispose de droits d'accès privilégiés sur tout ou partie des *systèmes d'information et de communication* de la CASA, dans la mesure où ces derniers sont supérieurs et plus étendus que les droits d'accès accordés aux *utilisateur*s ;

- « *utilisateur* » : toute personne autorisée à accéder aux *systèmes d'information et de communication*, faisant partie du personnel de la C.A.S.A, et ce, quel que soit son statut (agent de la fonction publique titulaire ou non titulaire, contractuel, stagiaire, apprenti, élus etc.) tel que visé à l'article 4.1 des présentes ;

- « *application* » : programme destiné à traiter une tâche donnée pour les besoins particuliers de l'*utilisateur* et les programmes exécutables associés, accessible via le réseau internet ou de télécommunication ;

- « *backup* » : solution de secours informatique en cas de défaillance du centre de traitements, présentant une configuration compatible avec celle de l'établissement, pouvant être hébergée sur un ou des site(s) géographique(s) différent(s) de celui de l'établissement ;

- « *code malveillant* » : logiciel développé dans le but de nuire à un système informatique (virus, vers, chevaux de Troie, keyloggers, etc.) ;

- « *consommable* » : produit ou constituant qui disparait par l'usage des *systèmes d'information et de communication* (*consommables* d'impression, cartouches d' encre, fournitures de bureau diverses, etc.) ;

- « *DPO* » : désigne le délégué à la protection des données, désigné par la C.A.S.A. chargé de conseiller, accompagné et contrôlé la C.A.S.A. et ses *utilisateur*s dans la cadre du traitement de données à caractère personnel ;

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

- « *filtrage* » : ensemble d'outils informatiques visant à limiter l'accès à certains sites Internet en raison de leurs contenus (contrôle des contenus, des URL, protocoles, etc.) ;

- « *matériel nomade* » : moyens informatiques et de communication électronique portables, pouvant en conséquence être utilisés à l'extérieur des locaux de la C.A.S.A. ;
- « moyen d'authentification » : moyen permettant l'accès aux systèmes d'information et de communication et pouvant prendre diverses formes : identifiant /mot de passe, biométrie, signature électronique, cartes avec ou sans contact, etc. ;

- « *RGPD* » : désigne le règlement (UE) du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement de données personnelles et à la libre circulation de ces données ;

- « *service en ligne* » : service de communication par voie électronique de mise à disposition du public ou de catégories de public, de signes, de signaux, d'écrits, d'images, de sons ou de messages de toute nature qui n'ont pas le caractère de correspondance privée ;

- « *trace informatique* » ou « *trace* » : donnée informatique témoignant de l'existence d'une opération au sein d'une *application* ou des *systèmes d'information et de communication*.

3 Portée et opposabilité

10. Conformément à l'article 8.4 du règlement intérieur, la présente charte est annexée à celui-ci et produit, à ce titre, les mêmes effets.

11. En conséquence, l'*utilisateur* est supposé en avoir pris connaissance.

12. La présente charte est publiée sur l'intranet de la C.A.S.A. et portée ainsi en permanence à la connaissance de tous les *utilisateur*s, y compris des nouveaux arrivants.

4 Champ d'*application*

4.1 Personnes concernées

13. La charte est applicable, et donc opposable, à toute personne, faisant partie du personnel de la C.A.S.A., quel que soit son statut (agent de la fonction publique titulaire ou non titulaire, contractuel, stagiaire, apprenti etc.). Elle est applicable également aux élus de la C.A.S.A.

14. La charte est complétée par la charte des *administrateur*s.

4.2 Moyens concernés

15. Sont visés par la charte :

- l'ensemble des *systèmes d'information et de communication* qui sont la propriété de la C.A.S.A. et/ou qui sont mis à la disposition des *utilisateur*s à des fins professionnelles ;

- l'ensemble des *systèmes d'information et de communication* qui sont la propriété personnelle de l'*utilisateur*, dès lors que ce dernier a obtenu une autorisation de les utiliser, dans le cadre de son activité professionnelle.

4.3 Usages concernés

16. La charte s'applique à tous les types d'usage, quelle que soit leur fréquence ou leur périodicité et qu'ils aient lieu :

- dans n'importe quel site ou local de la C.A.S.A.,
- dans le cadre d'un usage dit « nomade », quel qu'en soit le lieu,
- dans le cadre d'un accès distant, quel que soit le lieu de cet accès (domicile, etc.).

5 Conditions générales

5.1 Usage professionnel

5.1.1 *Systèmes d'information et de communication* de la C.A.S.A.

17. Les *systèmes d'information et de communication,* quelle que soit leur nature et quel que soit leur usage, sont réservés à un usage professionnel et sont donc présumés avoir un caractère professionnel.

18. Selon la jurisprudence, sont présumés avoir un caractère professionnel, notamment :

- les fichiers créés par un *utilisateur* grâce aux *systèmes d'information et de communication* de la C.A.S.A. ou de ses moyens ou ressources, pour l'exécution de son travail, sauf lorsque celui-ci les identifie comme étant « privés » ou « personnels » ;

- les connexions établies par un *utilisateur* sur des sites internet pendant son temps de travail, grâce aux *systèmes d'information et de communication* de la C.A.S.A., pour l'exécution de son travail ;

- tous les supports de stockage de données, notamment externes et/ou amovibles, dès lors qu'ils sont connectés aux *systèmes d'information et de communication* de la C.A.S.A., tels que les clés USB, les disques durs externes, les cartes mémoire comme les cartes SD ou micro SD , lorsqu'elles sont, par exemple, insérées dans des appareils eux -mêmes connectés à un ordinateur de la CASA mis à la disposition de l'*utilisateur* par la C.A.S.A..

19. Il en résulte que :

- la C.A.S.A. peut y accéder hors de la présence de l'*utilisateur*, notamment pour des raisons de continuité d'activité ou par mesure de sécurité ;

- aucune information à caractère professionnel ne doit être ni stockée dans un répertoire informatique utilisé à des fins privées, ni émise, ou reçue, via la messagerie privée.

20. Messagerie électronique. En particulier, l'adresse de messagerie électronique, composée de [initiales(s)].[nom]@agglo-casa.fr est strictement professionnelle. Elle ne doit donc pas être utilisée dans un autre contexte, sauf dans les conditions visées à l'article 5.2. Elle ne doit pas être diffusée sur des services en ligne sans rapport avec l'activité professionnelle.

21. Il est rappelé qu'en vertu du Code Général des Collectivités Territoriales, seuls sont compétents pour engager la C.A.S.A. : le Président et/ou les Vice-présidents, le Directeur Général, les Directeurs Généraux Adjoints, les agents dûment autorisés ayant reçus une délégation de signature, chacun dans les domaines qui les concernent. Toute décision échappant à cette règle expose la C.A.S.A. à un recours pour incompétence. Ainsi, tout message électronique doit mentionner le prénom, le nom, la fonction, l'adresse administrative de l'*utilisateur* signataire et ceux de la personne qui suit l'affaire, si elle est distincte.

22. Les listes de diffusion, permettant la réception automatique et périodique d'informations, doivent être réservées à un usage professionnel.

23. L'inscription sur une liste de diffusion requiert une autodiscipline des *utilisateur*s. Afin de minimiser les conséquences négatives qu'elle peut avoir (fréquence de réception des messages, poids des messages, encombrement des réseaux, etc.), il incombe à chaque *utilisateur* de vérifier scrupuleusement que chaque liste de diffusion à laquelle il souhaite s'inscrire, ou qu'il utilise déjà, est pertinente et nécessaire, c'est-à-dire cohérente avec les missions qu'il exerce au sein de la C.A.S.A.. Dans la négative, chaque *utilisateur* est responsable de sa désinscription de la liste de diffusion. En cas de difficulté, il incombe à l'*utilisateur* d'informer la direction en charge des *systèmes d'information et de communication* de la C.A.S.A. Le *DPO* de la C.A.S.A. peut-être également contacté pour obtenir des conseils.

24. **Services en ligne et *application*s**. L'accès à des services en ligne et *application*s est également réservé à un usage professionnel, sauf dans les conditions visées à l'article 5.2.

5.1.2 Moyens personnels de l'*utilisateur* (BYOD)

25. L'*utilisateur* ne peut pas utiliser à des fins professionnelles des *systèmes d'information et de communication* qui sont sa propriété personnelle ou qu'il détient à titre privé, sauf autorisation de la C.A.S.A. et sous réserve du respect des prescriptions techniques exigées par la direction en charge des *systèmes d'information et de communication* de la C.A.S.A..

5.2 Usage privé

26. Bien que les *systèmes d'information et de communication* de la C.A.S.A. soient réservés à un usage professionnel, leur utilisation à des fins non professionnelles, c'est-à-dire privées, est tolérée, pour répondre en cas d'urgence à des obligations socialement admises et/ou pour des usages raisonnables.

27. Cette tolérance pourra être suspendue ou limitée en cas d'abus. Par ailleurs, l'utilisateur peut s'exposer à des sanctions disciplinaires.

28. En toutes hypothèses, il est interdit de procéder à une diffusion large de messages non professionnels notamment de type petites annonces, chaînes de bonheur. En revanche il est possible d'afficher une petite annonce sur le portail intranet de la C.A.S.A., dans la rubrique prévue à cet effet.

29. En tout état de cause, l'usage des *systèmes d'information et de communication* à titre privé ne doit pas :

- perturber le bon fonctionnement des systèmes d'information et de communication, du service, et de la C.A.S.A. en général ;

- compromettre les activités de la CASA et particulièrement ses missions d'intérêt général, ainsi que la continuité du service ;

- porter atteinte aux obligations qui incombent aux *utilisateur*s compte tenu de leur statut et, notamment, les obligations de dignité, d'impartialité, d'intégrité et de probité ;

- porter atteinte à la C.A.S.A. ou être susceptible d'engager la responsabilité de la C.A.S.A. ;

- poursuivre un but lucratif ou même ludique ;

- porter atteinte à l'image de marque ou à la réputation de la C.A.S.A..

30. De plus, que ce soit à titre professionnel ou privé, il est interdit à l'*utilisateur* de se connecter sur des sites à caractère pornographique, pédopornographique, zoophile, injurieux, violent, raciste, antisémite ou nazi, d'incitation à la haine ou à la violence ou à la commission d'acte illicite ou de terrorisme, discriminatoire, diffamatoire, faisant l'apologie du terrorisme, contrefaisant, ou manifestement contraire à l'ordre public ou de télécharger ou visionner ou stocker ou transmettre, etc. des contenus de telle nature.

31. Concrètement, à condition de respecter le présent article 5.2, pour les usages privés, l'*utilisateur* :

- a la possibilité de créer un répertoire informatique privé ou personnel sur les seuls disques locaux du ou des poste(s) informatique(s) (ex : PC, portable…) que la CASA met à sa disposition et sur d'éventuels supports externes qu'il peut connecté à ce ou ces postes informatique(s), et en aucun cas, pour des raisons liées à la gestion de la sécurité des systèmes d'information et de communication de la CASA, sur les disques durs des serveurs de la CASA (sur le « réseau » informatique de la CASA) ou dans les espaces de stockage du cloud privé de la CASA (espace de stockage attribué à chaque utilisateur du cloud privé de la CASA) ;

- a la possibilité d'utiliser, à des fins non professionnelles, la messagerie électronique professionnelle (pour rappel [initiale(s) prénom].[nom]@agglo-casa.fr) ;

- doit utiliser le terme « PRIVE » ou « PERSONNEL » :

    - sur le répertoire informatique qu'il aura créé à son nom;

- dans la zone objet du message électronique et informer le tiers destinataire du message de cet usage.
- Par ailleurs, si le moyen de communication utilisé ne comporte pas de champ « objet » (chat, messagerie instantanée, sms…), le message à caractère non professionnel doit débuter par le terme « PRIVE » ou « PERSONNEL ».
- L'utilisateur est entièrement responsable de l'usage des *systèmes d'information et de communication* de la C.A.S.A. à des fins privées ou personnelles et dégage en conséquence la C.A.S.A. de toute responsabilité.

32. A défaut d'utiliser le terme « PRIVE » ou « PERSONNEL », tous les répertoires informatiques et tous les messages électroniques sont considérés comme professionnels.

33. Par principe, la C.A.S.A. s'interdit d'accéder aux contenus ou donnés stockées ou échangées, dès lors qu'ils portent l'intitulé « PRIVE » ou « PERSONNEL ».

34. Toutefois le caractère privé du répertoire informatique ou des messages électroniques échangés, n'empêche pas que :

- la C.A.S.A. puisse accéder de manière exceptionnelle à ces éléments, lorsqu'il existe un risque avéré pour la C.A.S.A., en termes notamment de sécurité, de continuité de service, ou un risque grave de voir sa responsabilité engagée ;

- ces éléments fassent l'objet de conservation technique dans le cadre de la mise en œuvre des sauvegardes, soit dans le cadre de *backup* ou de plans de continuité ou de reprise d'activité, mis en œuvre au sein de la C.A.S.A.;

- en cas de détection ou de suspicion de la présence d'un *code malveillant* , un *administrateur* ou une personne habilitée procède à la mise en quarantaine ou, le cas échéant, à la suppression de l'élément quelconque qui comporte ou comporterait un *code malveillant* ;

- un *administrateur*, ou toute personne « habilitée », accède à ces contenus dans le cadre de sa mission consistant à assurer le fonctionnement normal et la sécurité des systèmes d'information et de communication, et cela, notamment, dans le cadre d'opérations de maintenance ;

35. Dans tous les autres cas non cités ci-dessus, la C.A.S.A. pourra pour des motifs légitimes, accéder aux éléments à caractère privés ou personnels :
- soit en présence de l'*utilisateur ;*
- soit en son absence, dès lors qu'il a été dûment invité à être présent et que ce dernier ne s'est pas présenté, ou bien dès lors que la C.A.S.A. y est autorisée par une décision de justice ou une autorité habilitée à cet effet (police, gendarmerie, douanes, Cnil, Direction générale de la concurrence, de la consommation et de la répression des fraudes, etc.).

5.3 Conditions d'accès et d'identification

5.3.1 Règles générales

36. Chaque *utilisateur* est doté d'un ou de plusieurs *moyens d'authentification* permettant l'accès aux systèmes d'information et de communication.

37. Le mot de passe est créé par l'*utilisateur* dans le respect des critères de sécurité imposés par la direction en charge *des systèmes d'information et de communication* de la C.A.S.A. Il est strictement personnel et confidentiel.

38. Il est, dès lors, interdit à l'*utilisateur* :

- de procéder à la moindre divulgation, même intra-service, de son ou de ses *moyens d'authentification* ;

- d'utiliser un *moyen d'authentification* autre que le sien, dans l'hypothèse où il en aurait eu connaissance ;

- de supprimer, masquer ou modifier son identité ou son identifiant ;

- d'user de son droit d'accès pour accéder à des *application*s, à des données ou à un compte informatique autres que ceux qui lui auront été éventuellement attribués, ou pour lesquels il a reçu l'autorisation d'accès ;

- lorsqu'un accès distant lui est accordé, d'utiliser d'autres *moyens d'authentification* que ceux qui lui sont remis à cet effet.

39. Les mots de passe doivent être modifiés selon une fréquence déterminée et exigée par la direction en charge des *systèmes d'information et de communication* de la C.A.S.A..

40. En termes de sécurité et de confidentialité, l'*utilisateur* devra suivre toutes les prescriptions complémentaires qui lui seront signifiées par la direction des *systèmes d'information et de communication* de la C.A.S.A..

41. Tout usage des *systèmes d'information et de communication* est imputé à l'*utilisateur* bénéficiaire du *moyen d'authentification* utilisé. *L'utilisateur* en assume donc toute conséquence, notamment juridique et financière, sauf s'il a engagé préalablement une demande de suspension ou de suppression d'autorisation, ou s'il est en mesure de démontrer qu'il n'est pas responsable de ces usages.

5.3.2 Perte ou vol

42. Si ces *moyens d'authentification* ont fait l'objet d'une communication à des tiers, ou qu'il existe un risque qu'ils soient communiqués, ou qu'ils aient été communiqués à des tiers ou captés par eux, à la suite notamment de leur perte, de leur vol ou encore de leur oubli, l'*utilisateur* concerné doit, sans délai :

- renouveler ses *moyens d'authentification* selon la procédure mise en place par la C.A.S.A. et, s'il rencontre des difficultés lors de cette opération de renouvellement, en faire état à la direction en charge des *systèmes d'information et de communication* de la C.A.S.A. ;
- dans tous les cas, aviser la direction en charge des *systèmes d'information et de communication* de la CASA de la perte ou du vol de ses *moyens d'authentification* , afin que celle-ci puisse, si nécessaire, diligenter une étude d'impact ;
- selon le cas, porter sa meilleure assistance à la C.A.S.A. lorsqu'elle doit mener des démarches (déclaration d'assurance, dépôt de plainte, etc.) rendues nécessaires à la

suite d'incidents liés à la perte ou le vol de ses *moyens d'authentification* , et cela quelle que soit la nature de ces incidents, ou réaliser, lui-même, ces démarches.

5.3.3 Modification/suspension des accès

43. En cas de suspicion de compromission de ses *moyens d'authentification*, l'*utilisateur* est tenu d'en aviser sans délai la direction en charge des *systèmes d'information et de communication.* Seul cet acte d'information est de nature à dégager la responsabilité de l'*utilisateur* pour les agissements qui auraient lieu post-déclaration.

44. La C.A.S.A. se réserve, pour quelque raison que ce soit, de manière temporaire ou définitive, le droit d'accorder, de refuser, de modifier ou de supprimer tout ou partie, le droit d'accès de toute personne aux *systèmes d'information et de communication*.

45. La C.A.S.A. s'efforcera, autant que faire se peut, de prévenir l'*utilisateur* concerné, dans des délais raisonnables, notamment en cas de maintenance.

5.3.4 Droit à la déconnexion

5.3.4.1 Principes directeurs

46. Le présent article a pour objet de synthétiser les recommandations applicables à tous les agents afin d'assurer l'effectivité du droit à la déconnexion ainsi que les modalités selon lesquelles ce droit sera garanti.

47. Par « droit à la déconnexion », il y a lieu d'entendre le droit pour l'employé de ne pas être connecté avec ses outils numériques professionnels tels que PC portables, tablettes, téléphones portables ou messageries en dehors de son temps de travail.

48. Le temps de travail s'entend comme les horaires de travail du salarié durant lesquels il est à la disposition de son employeur et comprenant les heures normales de travail du salarié et les heures supplémentaires et les temps d'astreinte, à l'exclusion des temps de repos quotidien et hebdomadaire, des congés payés, des congés exceptionnels, des jours fériés et des jours de repos.

5.3.4.2 Les personnels d'encadrement

49. Dans la mesure du possible et sauf urgence avérée ou nécessité de continuité du service public, les personnels d'encadrement doivent s'abstenir de contacter leurs subordonnés en dehors de leurs horaires de travail tels que définis au contrat de travail ou par accord collectif d'aménagement du temps de travail. Dans tous les cas, l'usage de la messagerie électronique ou du téléphone professionnels en dehors des horaires de travail doit être justifié par la gravité, l'urgence et/ou l'importance du sujet en cause.

5.3.5 Lutte contre la surcharge informationnelle liée à l'utilisation de la messagerie électronique professionnelle

50. Afin d'éviter la surcharge informationnelle, il est recommandé à tous les employés :

- de s'interroger sur la pertinence de l'utilisation de la messagerie électronique professionnelle par rapport aux autres outils de communication disponibles ;
- de s'interroger sur la pertinence des destinataires du courriel ;
- d'utiliser avec modération les fonctions « CC » ou « Cci » ;
- d'éviter l'envoi de fichiers trop volumineux ;
- d'indiquer un objet précis permettant au destinataire d'identifier immédiatement le contenu du courriel.

5.3.6 Lutte contre le stress lié à l'utilisation des outils numériques professionnels

51. Afin d'éviter le stress lié à l'utilisation des outils numériques professionnels, il est également recommandé à tous les employés :

- de s'interroger sur le moment opportun pour envoyer un courriel ou appeler un collaborateur sur son téléphone professionnel (pendant les horaires de travail) ;
- de ne pas solliciter de réponse immédiate si ce n'est pas nécessaire ;
- de définir le « gestionnaire d'absence au bureau » sur la messagerie électronique et indiquer les coordonnées d'une personne à joindre en cas d'urgence.

5.4 Gestion des absences et des départs

52. Chaque *utilisateur* doit veiller à ce que la continuité du service soit assurée, conformément aux modalités d'organisation définies par la C.A.S.A.. Il doit, soit paramétrer le reroutage automatique de ses messages vers son supérieur hiérarchique, soit paramétrer un message automatique d'absence.

53. En cas d'absence prolongée ou de départ de l'*utilisateur* de la C.A.S.A., la C.A.S.A. se réserve le droit de mettre en place une solution de reroutage des messages électroniques, ou toute autre solution technologique permettant d'assurer la continuité de l'activité du service.

54. En cas d'absence de l'*utilisateur*, pour quelque raison et durée que ce soit, la C.A.S.A. se réserve le droit d'accéder directement aux différents dossiers, répertoires, messages électroniques et, plus généralement, à tout document à caractère professionnel de l'*utilisateur* ayant recours, en tant que de besoin, aux codes administrateurs systèmes.

55. A l'annonce du départ de la C.A.S.A. d'un *utilisateur*, et pour des raisons légitimes de protection des intérêts de la C.A.S.A., les droits d'accès et les conditions d'utilisation des *systèmes d'information et de communication* pourront être modifiés. De même, des règles particulières de traçabilité pourront être mises en œuvre.

56. Lors de son départ, l'*utilisateur* doit :

- remettre en bon état général de fonctionnement et déverrouillés l'ensemble des *systèmes d'information et de communication* qui lui ont été fournis ;

- restituer ses *moyens d'authentification et les éventuels matériels mis à disposition (par exemple dans le cadre du télétravail)* ;

- supprimer, la veille de son départ, le répertoire et les messages électroniques nommés « PRIVE » ou « PERSONNEL », ainsi que tous les documents de même nature. A défaut, et sauf procédure judiciaire ou enquête administrative, ces éléments sont automatiquement supprimés le lendemain du départ de l'*utilisateur* de la C.A.S.A., sans être consultés et sans qu'aucune copie ne soit réalisée.

57. Sauf nécessité liée à la continuité du service et pour un temps raisonnable, qui ne saurait excéder trois (3) mois, le compte messagerie de l'*utilisateur*, ainsi que ses *moyens d'authentification*, sont désactivés après son départ.

6 Conditions d'utilisation spécifique

6.1 Mobilité et accès distant

58. Dans le cadre de ses déplacements professionnels ou de ses accès à distance aux *systèmes d'information et de communication* de la C.A.S.A., quelles que soient leurs durées ou leurs fréquences, l'*utilisateur* assure la garde et la responsabilité des *systèmes d'information et de communication* qu'il utilise.

59. Les usages dits « nomades » et/ou à distance imposent à l'*utilisateur* un niveau de surveillance et de confidentialité renforcé.

60. Ainsi, l'*utilisateur* se doit d'adopter une attitude de prudence et de réserve au regard des informations, données et ressources des *systèmes d'information et de communication* de la C.A.S.A. qu'il pourrait être amené à manipuler ou à échanger.

61. Il doit également veiller à ce que des tiers non autorisés ne puissent pas accéder aux *systèmes d'information et de communication*, les utiliser ou accéder à leurs contenus.

62. En cas d'incident avéré ou de doute, l'*utilisateur* doit immédiatement en aviser la C.A.S.A.

6.2 Télétravail

63. La C.A.S.A. se réserve la possibilité de mettre en œuvre du télétravail, selon la législation en vigueur.

64. Dans ce cas, un *utilisateur* autorisé à recourir au télétravail doit respecter les dispositions de cette présente charte et de ses compléments, ainsi que l'ensemble des procédures et instructions données par la C.A.S.A. pour l'utilisation des *systèmes d'information et de communication.*

6.3 Gestion des connaissances et de l'espace collaboratif

65. La C.A.S.A. privilégie, autant que faire se peut, le partage et la capitalisation des connaissances. Elle est amenée à mettre en place des espaces collaboratifs de travail.

66. La qualité des informations ainsi disponibles est un objectif élevé. Chaque *utilisateur* s'engage à être attentif à la pertinence des informations diffusées au sein de ces espaces et à travers les outils de gestion des connaissances mis à sa disposition.

67. Par souci de qualité, de responsabilité et de protection du patrimoine informationnel de la C.A.S.A., l'utilisation de ces mêmes espaces et outils peut faire l'objet d'opérations renforcées de contrôle, d'audit, de modération et de traçabilité.

68. Aux mêmes fins, la C.A.S.A. a mis en place des outils de marquage de tout ou partie des éléments des bases de données constituées dans ce cadre, pour éviter toute extraction. Les *utilisateur*s sont avertis de la présence de tels outils.

6.4 Médias sociaux

69. La C.A.S.A. estime que les réseaux sociaux extérieurs à la C.A.S.A. occupent une place grandissante dans la vie professionnelle. Ces réseaux permettent aux *utilisateur*s de créer de nouvelles relations professionnelles et d'optimiser les échanges professionnels autour de leurs projets.

70. Cependant, l'utilisation des réseaux sociaux peut être source de risques et de responsabilité, notamment en termes d'image, ou de fraude. Aussi, afin de limiter les risques encourus, les règles suivantes ont été arrêtées.

71. Ces règles s'appliquent en sus et en cohérence avec les obligations et principes issus de la loi relative à la déontologie et aux droits et obligations des fonctionnaires et ses décrets d'*application*[1].

6.4.1 Usage professionnel

72. L'*utilisateur* pourra utiliser les réseaux sociaux dans le cadre de son activité professionnelle au sein de la C.A.S.A. sous réserve du respect des obligations qui incombent aux fonctionnaires et aux agents contractuels, et notamment des règles suivantes :

- s'abstenir de publier un contenu de façon anonyme et, au contraire, s'identifier clairement, en précisant sa fonction au sein de la C.A.S.A. ;

- répondre aux contributions des tiers avec pertinence, exactitude, en s'efforçant de promouvoir l'image de la C.A.S.A. ;

- respecter les conditions générales d'utilisation du réseau social et l'ensemble des lois applicables (notamment en matière de concurrence, de consommation et de propriété intellectuelle, de droit de la presse, de propos illicites) ;

- utiliser uniquement les outils de communication de l'établissement, selon les instructions qui lui ont été données et valoriser la visibilité du site web ;

- s'abstenir de consulter ou d'utiliser tout réseau social illicite ;

[1] Loi n°2016-483 du 20 avril 2016 relative à la déontologie et aux droits et obligations des fonctionnaires

- respecter les obligations qui lui incombe compte tenu de son statut et notamment, les obligations de dignité, d'impartialité, d'intégrité et de probité ;

- respecter le principe de neutralité ;

- utiliser les réseaux sociaux dans le respect du principe de laïcité ;

- plus généralement, prendre toutes les précautions utiles pour que son utilisation des réseaux sociaux soit sans danger pour les *systèmes d'information et de communication* de la C.A.S.A.

73. En cas de doute sur l'utilisation d'un réseau social, l'*utilisateur* devra immédiatement consulter son supérieur hiérarchique.

6.4.2 Usage privé

74. Dans le cadre de la sphère privée et hors les murs de la C.A.S.A., l'*utilisateur* est bien évidemment libre d'utiliser les réseaux sociaux. Cependant, il s'interdit de communiquer la moindre information sur son activité professionnelle, en particulier des informations confidentielles, des informations relatives aux conditions de travail, à l'organisation générale, au calendrier d'évènements, à la rémunération, etc..

75. L'*utilisateur* n'est autorisé à faire mention de son rattachement à la C.A.S.A. que sur les réseaux sociaux à caractère professionnel (par exemple, LinkedIn et Viadeo).

6.4.3 Signalement

76. Dans le cadre de la protection des lanceurs d'alerte et, plus généralement, lorsqu'un *utilisateur* utilise les réseaux sociaux à titre professionnel ou non, celui-ci peut informer la C.A.S.A. d'un agissement de tiers susceptible de porter atteinte à la réputation de la C.A.S.A. ou à un droit de la C.A.S.A. (notamment de propriété intellectuelle), dont il aurait connaissance.

(cf. procédure décrite dans la charte des ressources humaines.)

7 Le référent déontologue

77. Conformément à l'article 28 bis Loi n° 2016-483 du 20 avril 2016 relative à la déontologie et aux droits et obligations des fonctionnaires, un référent déontologue a été nommé.

78. Conformément à cette même loi, tout agent exerçant dans la fonction publique, peut exercer son droit de consulter un référent déontologue. Ce dernier a pour mission de lui apporter tout conseil utile au respect des obligations et des principes déontologiques mentionnés dans le statut général des fonctionnaires.

79. L'*utilisateur* peut donc s'adresser au référent déontologue pour toute question d'ordre déontologique liée à l'utilisation des *systèmes d'information et de communication* de la C.A.S.A. et en particulier à l'utilisation des messageries électroniques et des réseaux sociaux.

80. Le référent exerce ses missions sans préjudice de la responsabilité et des prérogatives du chef de service de l'*utilisateur*.

(cf. procédure décrite dans la charte des ressources humaines.)

8 Protection de la propriété intellectuelle, des informations et des données

8.1 Propriété intellectuelle et droit à l'image

81. L'utilisation des *systèmes d'information et de communication* de la C.A.S.A. implique le respect des droits de propriété intellectuelle et du droit à l'image.

82. Sans que cette liste soit exhaustive, l'*utilisateur* s'engage à :

- utiliser les logiciels et *application*s, dans les conditions de la licence souscrite par la C.A.S.A. ;

- ne pas effectuer de copie illicite de logiciel ou d'*application*s et, a fortiori, ne pas tenter d'installer des logiciels ou *application*s pour lesquels la C.A.S.A.ne possèderait pas un droit d'usage ;

- obtenir une autorisation écrite ou expresse préalable de la direction en charge des *systèmes d'information et de communication* de la C.A.S.A. pour la copie, le téléchargement, l'achat, l'installation ou l'utilisation de logiciels de commerce, logiciels à contribution (« shareware »), logiciels gratuits (« freeware ») ou tout autre logiciel ;

- ne pas reproduire, copier, utiliser remettre à des tiers ou diffuser, des bases de données, des pages web, des dessins, des modèles, des logos ou d'autres créations de la C.A.S.A., ou de tiers, protégés par le droit d'auteur, ou un droit privatif, sans avoir obtenu préalablement l'autorisation du titulaire de ces droits ;

- ne pas reproduire, copier ou diffuser des textes, des images, des photographies, des œuvres musicales, audiovisuelles ou multimédia et, plus généralement, toute création ou invention provenant du réseau internet, d'applications web ou mobiles sans respecter scrupuleusement les licences d'utilisation qui y sont attachées ;

- ne pas reproduire, copier, utiliser ou diffuser des éléments susceptibles de porter atteinte à l'image ou à la vie privée des *utilisateur*s ou de toute autre personne.

83. En toutes hypothèses, l'*utilisateur* s'interdit d'installer des logiciels à caractère non professionnel, notamment des logiciels à caractère ludique.

8.2 Préservation du secret et de la confidentialité

8.2.1 Règles générales

84. Le respect de la confidentialité des données est une exigence essentielle de la C.A.S.A. En effet, la C.A.S.A. est soumise à des obligations légales particulières en termes de secret et est susceptible d'être exposée à des risques particuliers.

85. La sauvegarde des intérêts de la C.A.S.A. nécessite le respect, par l'*utilisateur,* d'une obligation générale et permanente de confidentialité, de discrétion et de secret professionnel à l'égard des informations et des données dont il a connaissance dans le cadre de l'exercice de son activité professionnelle.

86. Le respect de cette obligation implique notamment de :

- veiller à ce que les tiers non autorisés n'aient pas connaissance de telles informations et données ;

- n'accéder qu'aux informations et données en rapport direct avec sa fonction et ne pas chercher, en conséquence, à prendre connaissance d'informations réservées à d'autres *utilisateur*s ;

- ne pas extraire ces informations et données confidentielles et ne pas les reproduire sans l'accord préalable du supérieur hiérarchique et/ou les détourner de leur utilisation normale, à des fins non professionnelles ;

- d'une manière générale, respecter les règles d'éthique professionnelle, de déontologie, ainsi que les obligations de réserve, de devoir et de discrétion en usage au sein de la C.A.S.A.

87. L'obligation de confidentialité, ici décrite, ne s'applique pas lorsque la diffusion de l'information est réalisée :

- dans le cadre de l'exercice d'un droit prévu par des dispositions légales, notamment celles relatives à la libre rediffusion de certaines données publiques prévues dans le Code des relations entre le public et l'administration, ou dans toute réglementation encadrant l'ouverture des données produites par le secteur public.;

- avec l'habilitation de l'émetteur, pour un destinataire autorisé désigné et dans le respect d'une procédure sécurisée.

8.2.2 Chiffrement

88. Il est interdit aux *utilisateur*s de chiffrer les répertoires, dossiers ou boites ou libellés à caractère privé ou non professionnel.

89. L'utilisation de procédés de chiffrement est une fonction restreinte à certains cas autorisés. Il est interdit d'utiliser des moyens de cryptologie autres que ceux expressément autorisés par la C.A.S.A.

8.3 Protection des données à caractère personnel

8.3.1 Devoirs

90.Les *utilisateur*s sont informés de la nécessité de respecter les dispositions légales en matière de traitements, automatisés ou manuels, de données à caractère personnel prévues, pour l'essentiel, dans le règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016, applicable depuis le 25 mai 2018 aussi appelé RGPD.

91.Dans ce cadre, les *utilisateur*s devront se conformer à la procédure en vigueur pour la mise en œuvre d'un traitement de données à caractère personnel.

92. Conformément à la législation applicable à la protection des données à caractère personnel, les principes directeurs à respecter dans le cadre de la mise en œuvre d'un traitement de données à caractère personnel sont les suivants :

- Informer, en amont de sa mise en place, la direction en charge des *systèmes d'information et de la communication* ainsi que le DPO de la CASA.
- une collecte licite, loyale et transparente ;
- l'acquisition et le traitement de données pour des finalités déterminées, explicites et légitimes ;
- l'obtention d'un consentement pour des finalités spécifiques ;
- le respect des droits des personnes concernées, tels que le droit de questionnement, d'accès, de modification ou d'opposition ;
- la durée de conservation limitée ;
- la protection des données dès la conception et par défaut ;
- le contrôle des destinataires et notamment le respect des règles relatives aux flux transfrontaliers de données à caractère personnel.

8.3.2 Droits des *utilisateurs*

93. La C.A.S.A. met en œuvre des traitements de données à caractère personnel concernant l'usage des *systèmes d'information et de communication* couverts par la présente charte. La C.A.S.A. s'engage à ce que les données concernant les *utilisateur*s soient collectées et traitées de manière loyale et licite, dans les conditions exposées.

94. La C.A.S.A. a désigné un *DPO* en la personne morale du syndicat mixte d'ingénierie pour les collectivités et territoires innovants des alpes et de la méditerranée (SICTIAM) dont les coordonnées sont

A l'attention du DPO de la CASA
SICTIAM
Business Pôle 2, 1047 route des Dolines

L'utilisateur est informé

- d'une part, que la CASA se réserve le droit de modifier, en cas de nécessité (changement de DPO), sans formalité particulière et préalable, les coordonnées du DPO indiquées dans cette charte,
- d'autre part, que le DPO de la CASA peut-être contacté également par courriel à l'adresse suivante : dpo@agglo-casa.fr.

95.Les catégories suivantes de données sont traitées :

- Informations professionnelles ;
- Informations relatives à l'identité ;
- Coordonnées professionnelles ;
- Logs de connexion et autres *traces informatiques* ;
- Informations sur l'utilisation des *systèmes d'information et de communication.*

96. Ces catégories de données proviennent essentiellement des *systèmes d'information et de communication* ainsi que des annuaires informatiques.

97.Les données personnelles sont conservées uniquement le temps nécessaire à l'accomplissement des finalités poursuivies au moment de la collecte.

98. Ces données sont destinées à la C.A.S.A. ainsi qu'aux personnes habilitées au sein de C.A.S.A. et aux autorités habilitées.

99. Les traitements concernant l'usage des *systèmes d'information et de communication* de la C.A.S.A. ont pour finalité :

- le suivi et la maintenance des systèmes d'information et de communication, qu'il s'agisse des *application*s informatiques internes ou des accès vers l'extérieur (soit notamment l'accès à internet) ;

- la gestion des annuaires permettant de définir les autorisations d'accès aux *application*s et réseaux ;

- la mise en œuvre de dispositifs destinés à assurer la sécurité et le bon fonctionnement des *systèmes d'information et de communication*, notamment la conservation des logs de connexion, des *traces informatiques* et des données de toute nature ;

- le suivi de la consommation des *consommables* ;

- le suivi des coût des télécommunications ;

- la gestion de la messagerie électronique ;

- le suivi et la maintenance des outils bureautiques administratifs (type planning, calendrier, gestion des tâches, gestion de projets, gestion des carnets de contacts,

agendas …) et des logiciels métiers (type solution logicielles finances, solutions logicielles drh…) ;

- le respect de cette charte.

100. Ces finalités permettent à la C.A.S.A. de poursuivre, dans le respect des droits des *utilisateur*s, des intérêts légitimes liés à la bonne utilisation et à la sécurité de ses *systèmes d'information et de communication*.

101. A toutes fins utiles, il est rappelé que les données collectées auprès des *utilisateur*s sont utilisées à des fins de bonne gestion, d'organisation et de *sécurité des systèmes d'information et de communication.*

102. Conformément au Règlement Général de Protection des Données, les *utilisateur*s sont informés, en particulier, qu'ils disposent d'un droit d'information, d'accès, de limitation, d'effacement, de rectification et d'opposition au traitement des données les concernant qui s'exerce auprès de la direction en charge des *systèmes d'information de de communication de la CASA*. Par ailleurs, les *utilisateur*s disposent d'un droit de réclamation auprès de la Cnil.

103. Conformément à la loi « Informatique et Libertés », les personnes peuvent donner des directives relatives à la conservation, à l'effacement et à la communication de leurs données après leur décès. Une personne peut être désignée pour exécuter ces directives et elle aura alors qualité, lorsque la personne est décédée, pour prendre connaissance des directives et demander leur mise en œuvre aux responsables de traitement concernés. Lorsqu'il s'agit de directives particulières, elles peuvent également être confiées aux responsables de traitement en cas de décès.

8.4 Enregistrements

8.4.1 Vidéo-surveillance

104. Les *utilisateur*s sont informés de la mise en place d'un dispositif de vidéosurveillance dans les locaux de la C.A.S.A. à des fins de sécurité et de prévention des atteintes aux biens et/ou aux personnes.

105. L'enlèvement ou la neutralisation, sans justificatif, de tout ou partie de ce dispositif de vidéosurveillance sont strictement interdits.

8.4.2 Enregistrements audio/visuels

106. Dans le cadre professionnel et dans l'objectif d'atteindre une certaine qualité de service, des outils techniques d'enregistrements vidéo et sonores pourront être mis en place.

107. Pourront être soumises à des enregistrements notamment les webconférences, les visio-conférences, les conférences téléphoniques.

108. Les utilisateurs sont informés de l'existence de ces outils d'enregistrement et peuvent exercer leur droit d'opposition avant la fin de la conversation téléphonique. L'utilisateur

chargé de l'organisation de la conférence doit énoncer clairement en début de session que la conversation sera enregistrée.

9 Sécurité et vigilance

9.1 Sécurité

109. Les *systèmes d'information et de communication* sont exclusivement installés, configurés et paramétrés par le personnel habilité par la C.A.S.A.

110. Lorsqu'il s'agit de moyens personnels de l'*utilisateur*, ceux-ci sont nécessairement autorisés, voire contrôlés, par ce même personnel.

111. A des fins de précaution, certaines configurations peuvent être verrouillées par la C.A.S.A. (poste de travail, accès internet, etc.).

112. La mise en place d'outils de sécurité par la C.A.S.A. ne dispense pas les *utilisateur*s d'une obligation de vigilance.

113. En effet, tout *utilisateur* a la charge, à son niveau, de contribuer à la sécurité des *systèmes d'information et de communication* mis à sa disposition, principalement en évitant l'introduction de *codes malveillants* susceptibles d'endommager les *systèmes d'information et de communication* de la C.A.S.A.

114. Chaque *utilisateur* doit veiller à se tenir informer sur les techniques de sécurité implémentées au sein de la C.A.S.A. et à maintenir son niveau de connaissance, en fonction de l'évolution des techniques.

115. Au titre de cette vigilance, l'*utilisateur* doit se conformer notamment, mais non limitativement, aux règles de conduite suivante :

- ne pas ouvrir les pièces jointes reçues de l'extérieur lorsque l'émetteur du message est inconnu ou douteux ;

- détruire les messages du type « chaîne de solidarité » ;

- ne pas stocker et router des gadgets, widgets ou autres *application*s ludiques reçus ou trouvés sur internet ;

- ne pas faire suivre les messages d'alerte de l'arrivée d'un virus mais prévenir la direction en charge des *systèmes d'information et de communication* ;

- ne pas modifier les *systèmes d'information et de communication* mis à sa disposition notamment par l'installation de logiciels, même gratuits, ou de matériels non expressément autorisés par la direction en charge des *systèmes d'information et de communication*, et ce, pour quelque raison que ce soit ;

- ne pas modifier ou détruire, ou tenter de modifier ou de détruire, des fichiers sur lesquels il ne dispose d'aucun droit, en particulier les fichiers contenant des informations comptables ou d'identification ;

- ne pas mettre à la disposition d'*utilisateur*s non autorisés un accès aux *systèmes d'information et de communication,* ou aux réseaux, à travers les matériels dont il a usage ;

- ne pas utiliser ou tenter d'utiliser des comptes autres que ceux qui lui sont attribués ou encore masquer son identité ;

- ne pas effectuer des opérations pouvant nuire aux relations internes ou externes de la C.A.S.A.

- Verrouiller son poste de travail en cas d'absence

116. En cas de réception de messages non sollicités (spams), l'*utilisateur* veille à :

- ne pas l'ouvrir sans s'être assuré préalablement de son innocuité ;
- ne pas y répondre ;
- ne pas le transférer ;
- informer la direction en charge des *systèmes d'information et de communication* de la C.A.S.A. en cas de suspicion ;
- paramétrer son compte pour bloquer l'adresse indésirable (utilisation de la fonction de traitement des messages indésirables, utilisation d'outils de type «mail in black» ou autre outils équivalents mis à sa disposition), seul ou avec l'aide de la direction en charge des *systèmes d'information et de communication* de la C.A.S.A..

117. Dans l'hypothèse d'une cyber-attaque l'*utilisateur* suit scrupuleusement les conseils de sécurité transmis par la direction en charge des *systèmes d'information et de communication* de la C.A.S.A..

118. L'*utilisateur* est tenu d'informer, sans délai, la C.A.S.A. de tout dysfonctionnement, altération, perte, vol, destruction et autre événement pouvant affecter les systèmes d'information et de communication. Il est tenu, en particulier, de signaler toute tentative d'intrusion extérieure, de falsification ou de présence de virus dont il aurait connaissance et qui pourraient nuire à la C. A.S.A, notamment en altérant le fonctionnement de ses *systèmes d'information et de communication*.

9.2 Traçabilité

119. Pour satisfaire aux obligations légales qui lui incombent, tenant à sa capacité à apporter la preuve, le cas échéant, du bon usage des *systèmes d'information et de communication* mis à la disposition des *utilisateur*s, la C.A.S.A. se réserve le droit de mettre en œuvre des outils de traçabilité tels que des journaux de connexions de l'ensemble des *systèmes d'information et de communication*.

120. En cas de nécessité, notamment en cas d'obligation, les *traces informatiques* sont conservées pour une durée limitée déclarée conformément à la réglementation en vigueur.

121.Il est strictement interdit de détourner, d'altérer ou de modifier les outils de traçabilité ou les données recueillies grâce à ces outils.

9.3 *Filtrage*

120. Pour satisfaire aux obligations légales qui lui incombent, tenant à sa capacité de tenter de prévenir tout usage illicite de ses *systèmes d'information et de communication,* la C.A.S.A. se réserve le droit de mettre en place des outils de *filtrage* permettant d'analyser les conditions d'utilisation de ces systèmes, d'interdire tel ou tel protocole, ou encore de restreindre la consultation de certaines catégories de sites internet ou d'*application*s.

121. Ces outils permettent un contrôle des connexions des *utilisateur*s car ils portent, entre autres, sur l'accès à internet.

122. Il est strictement interdit de détourner, d'altérer ou de modifier les outils de filtrage ou les données recueillies grâce à ces outils.

9.4 Scan informatique

123. Le scan informatique consiste à contrôler, à travers des outils informatiques, la présence de mots clés dans des contenus professionnels des *systèmes d'information et de communication* de la C.A.S.A.

124. La C.A.S.A. se réserve le droit de mettre en œuvre des opérations de scan des *systèmes d'information et de communication,* tels que le scan des éléments professionnels de l'*utilisateur*, et notamment des documents, des dossiers, des messages électroniques, pièces jointes, fichiers.

125. Les outils de scan informatique n'ont pas pour objet l'ouverture des éléments identifiés. Ils permettent à la C.A.S.A. de disposer d'un dispositif d'alerte prudentiel, et rapide.

126. Les documents, dossiers, messages électroniques, pièces jointes, etc., identifiés comme « PRIVE » ou « PERSONNEL » ne seront pas consultés par la CASA, sauf dans le cadre des dispositions légales particulières de la jurisprudence en la matière et des dispositions de cette charte.

127. Une liste de mots clés permettant les scans informatiques est déterminée par la C.A.S.A.. Cette liste n'est ni accessible par les *utilisateur*s, ni communiquée à eux, car elle dépend de la politique de sécurité de la C.A.S.A.

9.5 Mesures d'urgence et plan de continuité d'activité

128. L'*utilisateur* est informé qu'en cas de sinistre, d'incident majeur ou de nécessité impérative, la C.A.S.A. peut mettre en œuvre un certain nombre de mesures exceptionnelles visant à assurer la continuité de son activité et le respect de ses engagements contractuels ou légaux.

131. Ces mesures exceptionnelles peuvent inclure, notamment, une dégradation de service sur tout ou partie des ressources des *systèmes d'information et de communication* (temps de réponse, capacité de stockage, d'accès ou de traitement de l'information, etc.), la suppression temporaire de l'accès à certaines ressources des *systèmes d'information et de communication* (messagerie, connexion internet, accès applicatifs, éléments relatifs au poste de travail, etc.) ou la mise en œuvre de contraintes exceptionnelles (restriction temporaire de l'accès au site ou aux *systèmes d'information et de communication*, télétravail, déplacement sur des sites de secours tiers, etc.).

132. Dans cette hypothèse, l'*utilisateur* pourra être amené, à la demande de la C.A.S.A., à prendre des mesures d'urgence et de sécurité spécifiques, qu'il s'engage à appliquer sans délai.

10 Contrôle, maintenance et gestion des ressources

10.1 Contrôle et audit

133. Les opérations de contrôle et d'audit portent sur la régularité de l'utilisation *des systèmes d'information et de communication*. Elles se justifient par les obligations incombant à la C.A.S.A.

134. En effet, de par son activité, la C.A.S.A. est soumise à une obligation générale de sécurité, en *application* des dispositions du Code pénal relatives à la protection des systèmes de traitement automatisés de données, et des dispositions de la réglementation propre à la protection des données à caractère personnel, principalement constituée de la loi dite « Informatique et Libertés » et du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016.

135. La C.A.S.A., en tant qu'employeur, dispose également d'un pouvoir de contrôler l'activité des *utilisateur*s et en particulier, le respect par eux de cette charte.

136. La C.AS.A. pourra mettre en place un système de surveillance automatique afin de détecter toute activité d'*utilisateur* en violation de la présente charte.

137. La C.A.S.A. se réserve ainsi le droit, notamment :

- de vérifier le trafic informatique entrant et sortant, ainsi que le trafic transitant sur le réseau interne ;

- de diligenter des audits pour vérifier que les consignes d'usage et les règles de sécurité et de sûreté sont appliquées sur les ressources des *systèmes d'information et de communication* ;

- de contrôler l'origine licite des logiciels installés ;

- de conserver des fichiers de journalisation, des *traces informatiques,* en fonction des besoins propres de chaque système d'information ;

- de transmettre aux autorités judiciaires, sur requête, tout ou partie des enregistrements disponibles.

138. En cas d'incident de toute nature sur *les systèmes d'information et de communication*, la C.A.S.A. se réserve le droit de :

- surveiller le contenu des informations qui transitent sur ses *systèmes d'information et de communication* ;

- vérifier le contenu des disques durs, des ressources des *systèmes d'information et de communication* attribuées aux *utilisateur*s ;

- procéder à toutes copies utiles pour faire valoir ses droits.

139. Ces opérations de contrôle et d'audit relèvent des fonctions de la direction des *systèmes d'information et de communication*, car elle a en charge la qualité, la protection et la sécurité des *systèmes d'information et de communication* fournis aux *utilisateur*s.

140. En particulier, dans le cadre de ses fonctions, elle exerce un contrôle notamment des durées de connexion et des sites les plus visités.

141. Tout intervenant en charge de contrôles ou d'audits doit impérativement respecter la confidentialité des échanges électroniques et des fichiers des *utilisateur*s.

142. Les *utilisateur*s sont toutefois informés que les *administrateur*s systèmes et réseaux sont conduits, de par leurs fonctions, à avoir accès à l'ensemble des informations relatives aux *utilisateur*s (messages, connexions à internet, etc.), y compris à celles qui sont enregistrées sur le disque dur de leurs postes de travail.

143. Néanmoins, ces *administrateur*s systèmes et réseaux sont tenus aux obligations de la charte *administrateur* qui leur est applicable.

144. En cas de faisceau d'indices laissant supposer qu'un *utilisateur* met en cause les intérêts et la sécurité de la C.A.S.A. en ne respectant pas les règles instituées par cette charte, la direction en charge des *systèmes d'information et de communication* de la C.A.S.A. se réserve le droit de fournir à la direction des ressources humaines, sur sa demande écrite et motivée, les *traces* individuelles des connexions incriminées.

145. En cas de non-respect avéré de cette charte par un *utilisateur*, la direction en charge des *systèmes d'information et de communication* de la C.A.S.A. se verra dans l'obligation d'avertir le supérieur hiérarchique de l'*utilisateur,* pour que celui-ci décide de la suite à donner.

146. Suivant la gravité des faits, les droits d'accès de l'*utilisateur* concerné pourront être suspendus, temporairement ou définitivement.

147. Tous les matériels, les logiciels ou les *applications* installées illicitement seront supprimés ou désactivés par la direction en charge des *systèmes d'information et de communication* de la C.A.S.A. dès le constat de leurs présences sur des postes de travail ou des *matériels nomades*, ou le simple constat de leurs accessibilités.

10.2 Maintenance

148. La mise à disposition des *systèmes d'information et de communication* implique nécessairement des opérations de maintenance technique (maintenance corrective, maintenance préventive ou évolutive), et ce, pour assurer le bon fonctionnement et la sécurité de ceux-ci.

149. Ces opérations prennent la forme de « prises de main sur des postes informatiques » effectuées par une « personnes habilitée ». Celle-ci intervient soit sur site (dans les locaux de la C.A.S.A.), soit à distance (en dehors des locaux de la CASA).

150. En aucun cas, ces opérations, quel que soit leur mode opératoire, ne justifient le fait pour l'*utilisateur* de communiquer ses *moyens d'authentification*.

151. Dans ce cadre, la « personne habilitée » peut être amenée à prendre connaissance de l'ensemble des éléments présent sur le poste ou le *matériel nomade* de l'*utilisateur*, ainsi que des données de connexion, qu'il s'agisse d'un usage professionnel ou privé.

152. Si, à l'occasion d'opérations de maintenance, des utilisations anormales ou des contenus illicites ou préjudiciables sont identifiés, la C.A.S.A. en tirera toute conséquence.

10.3 Consommations

153. Pour la bonne gestion des ressources liées aux *systèmes d'information et de communication* :

- un suivi des *consommable*s de chaque *utilisateur* est effectué et comprend le détail de sa consommation (date, heure, nombre de feuille etc.) ;

- pour la téléphonie fixe et mobile, les éléments de la communication (date, heure, durée, coût et numéros appelés), le contrôle des consommations peut être effectué sur la base des factures détaillées ;

- pour les *systèmes d'information et de communication nomades*, le contrôle des consommations peut être effectué sur les éléments de la communication (date, heure, durée, coût et numéros appelés), à travers les services de suivi des consommations que proposent les opérateurs téléphoniques.

154. L'enregistrement des conversations téléphoniques est strictement interdit, sauf à en informer préalablement l'interlocuteur, ou dans le cadre des enregistrements autorisés et prévus à l'article « enregistrements ».

155. Les informations ainsi disponibles, qui sont principalement dédiées à l'analyse des consommations, peuvent, en tout état de cause, être utilisées pour démontrer toute utilisation contrevenante aux obligations, droits et devoirs prévus dans cette charte ou pour servir de preuve d'un fait manifestement illicite.

10.4 Règles de conservation, de sauvegarde et d'archivage électronique

156. Chaque *utilisateur* doit mettre en œuvre et organiser, dans le respect des instructions de sa hiérarchie, les moyens nécessaires à la conservation des messages, des informations et des données de toute nature, lorsque cela est nécessaire.

157. Si la CASA met en œuvre une politique de conservation et d'archivage, l'*utilisateur* est dans l'obligation de la respecter.

158. Les *traces* détaillées d'activité sont conservées pendant les durées légales ou conventionnelles, à l'issue desquelles elles sont détruites.

159. Ces *traces* valent preuve de l'utilisation des *systèmes d'information et de communication.*

160. Ces *traces* peuvent faire l'objet d'un traitement statistique.

161. Ces *traces* peuvent être fournies aux autorités compétentes selon les dispositions légales et réglementaires en vigueur.

162. Les sauvegardes, *backup* et archivages électroniques réalisés par la C.A.S.A. ne concernent pas les éléments du répertoire et les messages nommés « PRIVE » ou « PERSONNEL », qui sont donc conservés sous la seule et entière responsabilité de l'*utilisateur*.

163. Par ailleurs, il est précisé que la C.A.S.A. est soumise au respect des dispositions suivantes et leurs éventuelles modifications ultérieures :

- à l'instruction DAF/DPACI/RES/2009/018 du 28 août 2009, relative au tri et à la conservation des archives produites par les services communs à l'ensemble des collectivités territoriales (communes, départements, régions) et structures intercommunales ;
- aux préconisations relatives au tri et à la conservation des archives produites par les communes et structures intercommunales, dans leurs domaines d'activité spécifiques (DGP/SIAF/2014/006 du 22 septembre 2014).

11 Responsabilité et sanctions

164. L'*utilisateur* est responsable :

- dans le cadre de son activité professionnelle, de l'utilisation des *systèmes d'information et de communication* en conformité avec la présente charte ;

- dans la sphère de sa vie privée résiduelle, seul, à l'exclusion donc de toute responsabilité de la C.A.S.A., de tout usage à caractère non professionnel ou privé.

165. En cas de manquement grave d'un *utilisateur* à l'une des dispositions de la charte, l'*administrateur* ou la direction en charge des *systèmes d'information et de communication*

de la C.A.S.A. rend compte immédiatement à l'autorité d'emploi, en communiquant les éléments de preuve nécessaires.

166. Toute mauvaise utilisation ou utilisation non conforme aux conditions et limites définies par cette charte est constitutive d'une faute.

167. En conséquence, le non-respect des dispositions légales et règlementaires, ainsi que de cette charte, expose l'*utilisateur* en cause à des sanctions disciplinaires, prévues notamment dans le règlement intérieur, et/ou à des poursuites judiciaires.

168. En outre, l'*utilisateur* s'expose à des sanctions concernant son droit d'utiliser les *systèmes d'information et de communication*, notamment, le contrôle renforcé, la suspension, le blocage, le retrait et même la suppression pure et simple de son droit d'utiliser tout ou partie des *systèmes d'information et de communication*, des sites web et des *application*s, ou l'exclusion.

169. La C.A.S.A., pour sa part, déclare mettre en œuvre, par le biais notamment de cette charte, tous les efforts nécessaires à un bon usage des *systèmes d'information et de communication* et n'assumer aucune responsabilité au titre des agissements fautifs ou délictueux des *utilisateur*s auxquels elle fournit un droit d'accès.

12 Entrée en vigueur

170. Dans le cadre de sa fonction consultative, le comité technique de la C.A.S.A., qui s'est réuni en date du 2 décembre 2019, a examiné le respect des dispositions légales et réglementaires de la présente et a donné un avis favorable pour son *application*. La présente charte est depuis publiée sur l'intranet de la C.A.S.A. Sa date d'entrée en vigueur est le 1er janvier 2020.