Dernière mise à jour :
18 décembre 2019

Communauté d'Agglomération Sophia Antipolis

CHARTE DES ADMINISTRATEURS DES SYSTEMES D'INFORMATION ET DE COMMUNICATION

Table des matières

1. Préambule

1. Certains employés de la C.A.S.A. disposent de droits d'accès et d'habilitation étendus ou élevés dans les *systèmes d'information et de communication* de la C.A.S.A..

2. La présente charte s'applique à toute personne spécialement compétente en informatique, membre du personnel de la C.A.S.A. (ou de ses instances), habilitée par cette dernière, disposant de droits d'accès privilégiés sur tout ou partie de ses s*ystèmes d'information et de communication*, dans la mesure où ces derniers sont supérieurs et plus étendus que les droits d'accès accordés aux *utilisateurs*.

3. En particulier, les administrateurs des systèmes et des réseaux peuvent, selon leur habilitation, être affectés à un certain nombre de missions comme :

- la gestion, l'exploitation et la maintenance des *systèmes d'information et de communication* ;
- le suivi et le contrôle de l'utilisation des *systèmes d'information et de communication* ;
- la mise en œuvre des logiciels et autres *applications* ;
- la gestion des anomalies et incidents ;
- la gestion des notifications de failles de sécurité, en lien avec le Délégué à la protection des données lorsque des données à caractère personnel sont concernées.

4. Dans le cadre de leur activité, ils bénéficient de droits spécifiques organisés par la C.A.S.A et peuvent être amenés à avoir accès aux informations et/ou aux données d'autres *utilisateurs* susceptibles de présenter un caractère confidentiel ou privé. C'est pourquoi, ils doivent respecter des règles complémentaires à celles prévues par la charte de bon usage des *systèmes d'informations et de communication* de la C.A.S.A.

2. Objet

5. La présente charte a pour objet de définir les principales prérogatives, les engagements et la responsabilité des *administrateurs*.

3. Référentiel

6. La présente charte prend place au sein d'un référentiel composé, par ordre de priorité décroissant, de :

- la Loi n°2016-483 du 20 avril 2016 relative à la déontologie et aux droits et obligations des fonctionnaires et ses éventuelles modifications ultérieures ;

- la présente charte des administrateurs ;
- la charte de bon usage des *systèmes d'information et de communication de* la C.A.S.A..

7. En cas de contradiction entre des documents de nature différente, ou de rang différent, il est expressément convenu, entre les parties, que les dispositions contenues dans le document de rang supérieur prévaudront pour les obligations se trouvant en conflit d'interprétation. En cas de contradiction entre les termes des documents de même ordre, les derniers documents en date prévaudront sur les autres.

4. Portée et opposabilité

8. La présente charte est annexée au règlement intérieur de la C.A.S.A..

9. En conséquence, *l'administrateur* est supposé en avoir pris connaissance.

10. 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 *utilisateurs*, y compris des nouveaux arrivants.

5. Définitions

11. Les termes définis dans la charte de bon usage des *systèmes d'information et de communication* de la C.A.S.A. s'appliquent à la présente charte. Ils apparaissent en caractère italique.

6. Champ d'application

12. Cette charte s'applique à tout *administrateur,* quelle que soit l'étendue des droits d'administration conférés, qu'il s'agisse :

- des membres de la direction en charge des *systèmes d'information et de communication* ;
- des *administrateurs* internes tels que les *administrateurs* réseaux et systèmes, les *administrateurs* de solutions logicielles, *d'applications*, du système d'information géographique (SIG), de système de gestion de bases de données, de la sécurité des *systèmes d'information et de communication* , ayant des compétences spécifiques en informatique et disposant d'habilitations leur conférant des droits et des accès particuliers sur ces systèmes ;
- de toute autre personne, membre du personnel ou des instances délibérantes, qui dispose d'un droit d'administration sur un poste, sur un serveur ou sur tout autre *systèmes d'information et de communication* fourni par la C.A.S.A.

13. Ces personnes sont dénommées « *administrateurs* » au sein de la présente charte.

14. En conséquence, la présente charte s'applique, pour chaque *administrateur*, à la mesure de l'étendue des droits d'accès et d'habilitation qui lui ont été accordés par la C.A.S.A.

7. Prérogatives de l'administrateur des systèmes d'information et de communication

15. Le rôle de l'*administrateur* a connu une importante évolution ces dernières années, en particulier avec le développement des risques, notamment des risques liés à la sécurité des moyens informatiques et de communication électronique. Sans que cette liste soit exhaustive, son rôle et ses prérogatives sont définis ci-après.

7.1 Condition d'accès et d'authentification

16. L'*administrateur* peut disposer de *moyens d'authentification* spécifiques différent de ses identifiants *utilisateur*, notamment sous la forme suivante :

- « adm.nomagent ».

17. Les fonctionnalités associées à son identifiant dépendent de l'étendue des droits d'administration qui lui ont été accordés.

7.2 Administration des *systèmes d'information et de communication*

7.2.1 Prérogatives

18. Le bon fonctionnement général des *systèmes d'information et de communication,* notamment en ce qui concerne leurs performances, leurs disponibilités et leurs interopérabilités, est assuré par un *administrateur*.

19. A cette fin :

- il procède à des opérations de maintenance préventive des *systèmes d'information et de communication* et notamment des serveurs et des réseaux. Il maintient le bon état de fonctionnement de ces outils ;
- il paramètre et analyse les fichiers d'historisation (fichiers logs) pour identifier, le cas échéant, des dysfonctionnements ou des fonctionnements anormaux ;
- il assure la gestion de la messagerie et des accès internet ;
- il met en œuvre les profils *utilisateurs* et en contrôle le bon usage ;
- il procède à un archivage régulier des dossiers, fichiers et données, activité qui comprend l' archivage électronique sécurisé sur des supports fidèles et durables ;
- il assure la gestion de l'évolution du réseau, notamment par l'installation d'éventuels points d'accès Wi-Fi ou le paramétrage des routeurs.

7.2.2 Obligations

20. Les cas de non-respect des dispositions contenues dans la charte de bon usage des *systèmes d'information et de communication* de la C.A.S.A. devront être signalés par l'*administrateur* à la direction en charge des *systèmes d'information et de communication*.

21. Lorsqu'il procède à des interventions à distance sur l'outil d'un *utilisateur*, l'*administrateur* doit, dans la mesure du possible, requérir la présence de *l'utilisateur*.

7.3 Participation à la politique de sécurité

7.3.1 Prérogatives

22. L'*administrateur* participe activement à la sécurité des *systèmes d'information et de communication.* Dans ce cadre :

- il met en œuvre une maintenance curative des *systèmes d'information et de communication*, en corrigeant toute anomalie et en préservant la continuité des services et en utilisant tous les moyens de sécurité mis à sa disposition ;
- il procède aux sauvegardes prescrites par la direction des *systèmes d'information et de communication* de la C.A.S.A. ;
- il contribue, à travers notamment ses actions de support, de sensibilisation, de formation et de paramétrage, au respect, par les *utilisateurs*, des consignes de sécurité figurant dans la charte de bon usage des *systèmes d'information et de communication de la C.A.S.A. ;*
- il protège la sécurité des données et des bases de données de C.A.S.A. et met en place une veille des *applications* techniques de sécurité.

7.3.2 Audit et contrôles

23. L'*administrateur* pourra, sur demande de la direction en charge des *systèmes d'information et de communication*, procéder à un audit interne de ces *systèmes*.

24. L'audit interne est diligenté par la direction en charge des *systèmes d'information et de communication* dûment mandatée par la direction générale des services (DGS) afin de vérifier l'utilisation faite par les *utilisateurs* des *systèmes d'information et de communication* dans le but de maintenance préventive ou curative, ou en cas d'urgence.

25. À cette fin, l'*administrateur* pourra notamment :

- vérifier le trafic informatique entrant et sortant de la C.A.S.A. (durée de connexion, sites internet visités, heure des visites, éléments téléchargés, éléments envoyés...) et le trafic interne sur le réseau ;
- vérifier certains types de contenu qui sont souvent à l'origine d'incidents (espace de stockage insuffisant, encombrement du réseau, diffusion en chaîne, « cookies », etc...) ;
- contrôler l'origine licite des logiciels installés ;
- prendre connaissance des méls professionnels (sont identifiés comme personnels les méls dont l'objet précise clairement qu'il s'agit d'un message privé ou personnel) uniquement sur demande de la direction générale, de la direction des ressources humaines et de la direction des audits ;
- consulter les fichiers de journalisation des *traces* de connexion globales ;

- contrôler l'usage de la messagerie, en termes de volume et de nombre de messages échangés, de taille des messages, de format des pièces jointes, de quantité d'espace disque utilisée et procéder à l'analyse de messages afin de veiller à la sécurité des échanges (recherche de mots à caractère pornographique, raciste, etc…).

26. L'*administrateur* assurera la mise à disposition des *moyens d'authentification* ou de trafic sur demande de toute autorité indépendante compétente, ou sur demande des autorités judiciaires, en accord avec la direction en charge des *systèmes d'information et de communication.*

7.4 Gestion des risques et des menaces

7.4.1 Prérogatives

27. La maintenance préventive et curative du *système d'information et de communication* de la C.AS.A. est assurée par l'*administrateur*. Dans ce cadre, il procède à la correction de toute anomalie des *systèmes d'information et de communication*, préconise et met en place des solutions de contournement permettant d'assurer la continuité des services.

28. A ce titre, l'*administrateur* utilise tous les moyens de sécurité mis à sa disposition pour procéder à cette maintenance curative. Il met notamment en place les patchs de sécurité nécessaires à la maintenance des *systèmes d'information et de communication.*

29. Il peut, à cette occasion, identifier des comportements anormaux de la part des utilisateurs.

7.4.2 Obligations

30. Lorsqu'il constate un dysfonctionnement des *systèmes d'information et de communication*, il informe immédiatement la direction en charge des *systèmes d'information et de communication*.

31. Puis, sur instruction de la direction en charge des *systèmes d'information et de communication,* il peut être autorisé à poursuivre ses investigations sur l'origine et les causes du dysfonctionnement, ainsi que sur l'identification des remédiations possibles.

32. Dans cette circonstance, il met en œuvre les mesures prescrites par la direction en charge des *systèmes d'information et de communication* de la C.A.S.A..

33. Uniquement en cas de force majeure, ou en cas d'urgence, l'*administrateur* peut intervenir seul et prendre les mesures nécessaires au maintien de la sécurité, à la sauvegarde et au bon fonctionnement des *systèmes d'information et de communication.*

34. Dans ces cas de figure, il informe immédiatement la direction en charge des *systèmes d'information et de communication* des conséquences des actions qu'il met en œuvre, notamment lorsque celles-ci impactent le fonctionnement de la messagerie ou, plus largement, la continuité du service. Par ailleurs, il expose, sans délai, à cette même direction les solutions alternatives qu'il déploie afin d'aboutir, dès que possible, à la remise en œuvre complète des *systèmes d'information et de communication* de la C.A.S.A.

35. En cas de présomption basée sur des indices de violation de la charte de bon usage des *systèmes d'information et de communication* de la C.A.S.A.*,* ou pour des raisons de gestion des absences, *l'administrateur* pourra prendre la main sur le poste *utilisateur* avec ses propres *moyens d'authentification*.

36. L'*administrateur* devra utiliser les moyens à sa disposition pour empêcher l'activation de virus, de bombes logiques, de chevaux de Troie, provenant notamment de l'ouverture de messages reçus par les systèmes de messagerie ou lors de l'accès à internet.

37. En cas de doute sur l'efficacité des mesures, l'*administrateur* devra appliquer le principe de précaution et mettre en quarantaine ou à défaut détruire les fichiers qu'il estimerait pouvoir porter atteinte à l'intégrité et à la sécurité des *systèmes d'information et de communication.*

38. L*'administrateur* devra rendre compte de toute mise en quarantaine ou destruction de fichiers à la direction des *systèmes d'information et de communication* dans un délai de 48 heures.

8. Engagements de l'*administrateur*

8.1 Collaboration

39. Tout *administrateur* coopère étroitement dans le cadre de l'exécution de ses obligations avec la direction en charge des *systèmes d'information et de communication* de la C.A.S.A. A cette fin, il procède à un échange permanent d'informations en vue de contribuer à la bonne exécution de ses obligations et au fonctionnement des *systèmes d'information et de communication*.

40. Tout *administrateur* collabore étroitement avec les autorités compétentes, notamment la Commission nationale informatique et libertés, et avec toute autorité judiciaire qui pourrait requérir la communication d'informations.

41. Dans le cas où l'*administrateur* aurait le moindre doute sur la légitimité d'une demande ou d'une transmission d'informations, il ne doit pas transmettre ces informations et s'en référer à sa hiérarchie et à la direction en charge des affaires juridiques qui lui donneront les instructions à suivre.

8.2 Information, conseil et alerte

42. Tout *administrateur* s'engage à informer, conseiller, alerter et mettre en garde la direction en charge des *systèmes d'information et de communication* de la C.A.S.A..

43. Aucune action qui pourrait avoir pour conséquence de détruire ou corrompre des éléments de preuve ne doit être engagée sans validation de la direction en charge des *systèmes d'information et de communication* de la C.A.S.A..

8.3 Confidentialité renforcée

44. Tout *administrateur* s'engage à prendre toutes les mesures de sécurité nécessaires à la protection des informations et au maintien de leur confidentialité.

45. Tout *administrateur* s'engage à garder confidentielles, et à ne pas divulguer à des tiers, toutes les informations qui lui ont été révélées et dont il a eu connaissance dans le cadre de ses missions ou de son travail, ce qui implique notamment que *l'administrateur* doit :

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

- respecter les règles d'éthique professionnelle, de déontologie, l'obligation de réserve et le devoir de discrétion, en usage au sein de la C.A.S.A. ;

- respecter une taille et complexité de mot de passe assurant un haut niveau de sécurité pour la structure ;

- respecter strictement la confidentialité des mots de passe des *utilisateurs* et garder strictement confidentiel son mot de passe *administrateur*, ne le dévoiler à personne, ni l'écrire, ni l'enregistrer sur un support quelconque pour la mémorisation sauf en cas de nécessité de continuité de service en utilisant un trousseau sécurisé (solution logicielle par exemple) ;

- ne pas porter atteinte, sous quelque forme que ce soit et pour quelque motif que ce soit, au secret des correspondances privées des *utilisateurs*.

46. Un *administrateur* ne pourra transmettre des informations dont il aurait eu connaissance que à la direction générale des services de la C.A.S.A., soit dans le cadre d'une alerte de sécurité ou de violation de la charte de bon usage *des systèmes d'informations et de communication,* soit sur instruction de celle-ci.

8.4 Sécurité

47. Tout *administrateur* s'engage à :

- n'utiliser que les moyens informatiques et de communication autorisés par la direction *des systèmes d'information et de communication* de la C.A.S.A. et s'interdit d'utiliser toute autre solution, notamment dans le cadre d'opérations de contrôle ou d'audit ;
- à documenter :
  - toute action et intervention qui s'écartent des procédures internes de la C.A.S.A. ;
  - toute action de suppression de données ou de *traces*, ou tout autre action impactant le niveau de sécurité *du système d'information et de communication* de la C.A.S.A. ;
- à ne pas porter atteinte à l'intégrité des fichiers de journalisation ;
- à ne pas procéder, ou faire procéder par l'intermédiaire d'un prestataire, à des changements de configuration permettant de supprimer les *traces informatiques* sans autorisation hiérarchique, ou en dehors des cas prévus par la politique de sécurité des *systèmes d'information et de communication* de la C.A.S.A. ;

- à n'utiliser les comptes privilégiés que pour les activités et les besoins directement liés aux tâches d'administration ou d'exploitation dont il a la charge ;
- à ne prendre aucune consigne d'une personne non identifiée et, le cas échéant, à transmettre à la direction en charge des *systèmes d'information et de communication* toute requête lui paraissant inappropriée.

8.5 Respect des droits de propriété

48. Dans le cadre de l'exercice de ses missions, l'*administrateur* s'engage à ne pas porter atteinte à des droits de propriété intellectuelle.

49. Il s'engage notamment à :

- ne pas installer et ne pas utiliser, sur les matériels informatiques, un logiciel et/ou un progiciel, sans qu'une licence d'utilisation appropriée n'ait été préalablement souscrite ;
- ne pas pratiquer des téléchargements illicites ;
- ne pas reproduire, ou utiliser, des créations protégées par le droit de la propriété intellectuelle sans autorisation ;
- maintenir les formules de copyright.

8.6 Obligation de respecter la vie privée des *utilisateurs*

50. *L'administrateur* s'engage à respecter la vie privée des *utilisateurs* qui disposent notamment d'un droit à une vie privée résiduelle lorsqu'ils utilisent les *systèmes d'information et de communication* de la C.A.S.A. tel que prévu par la charte *de bon usage des systèmes d'information et de communication.*

51. L'administrateur qui est amené à accéder, dans le cadre de ses missions et prérogatives, à des fichiers, des données et des messages des utilisateurs comportant les mentions « PERSONNEL » ou « PRIVE » et pouvant être contenus dans tout ou partie des *systèmes d'information et de communication*, s'engage à en assurer la confidentialité et l'intégrité.

52. Il ne pourra les communiquer qu'à la direction générale des services et sur instruction écrite de celle-ci, uniquement dans le cadre d'une instruction pénale ou d'une décision de justice.

8.7 Respect de la règlementation sur la protection des *données à caractère personnel*

53. Conformément à la charte de bon usage des *systèmes d'information et de communication*, l'*administrateur* reconnait la nécessité de respecter les dispositions légales en matière de traitements automatisés ou manuels de *données à caractère personnel*, prévues pour l'essentiel dans la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, dite loi « Informatique et libertés » et dans le règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 (RGPD).

54. Il s'engage en outre à respecter la confidentialité des *données à caractère personnel*, la finalité pour lesquelles elles sont traitées et les mesures de sécurité qui y sont associées.

9. Responsabilité de l'administrateur du système d'information et de communication

55. Les moyens mis à la disposition de l'*administrateur* le sont à des fins exclusivement professionnelles.

56. A défaut du respect des obligations lui incombant dans le cadre de sa mission, ou dans le cas de dépassement non justifié de ses prérogatives, l'*administrateur* engage sa responsabilité.

57. Le non-respect de tout ou partie des règles définies dans la présente charte pourra entraîner pour l'*administrateur* la suppression immédiate de tout ou partie de ses droits d'accès et habilitation sur les *systèmes d'information et de communication* ainsi que des sanctions disciplinaires et/ou des poursuites judiciaires.

10. Entrée en vigueur

58. 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.