Charte d'utilisation des ressources informatiques

Cadre des droits et devoirs des collaborateurs

1.1 Termes utilisés

Le groupe / l'entreprise : le groupe setec, dont les ressources informatiques sont gérées par la Direction des Systèmes d'Information Groupe (DSIG) et sont transverses aux sociétés du groupe.

Setec sécurité : l'équipe en charge de piloter la démarche de sécurisation et de maintien en conditions de sécurité du Système d'Information du groupe setec et de traiter les problématiques de cybersécurité (securite@setec.fr)

Société : filiale du groupe setec, disposant de ressources informatiques propres, gérées par un référent informatique, aussi appelé administrateur informatique. L'administration informatique d'une filiale peut également être déléguée à une autre société.

Ressource informatique setec : tout outil informatique fourni par le groupe ou les sociétés pour l'exercice des activités professionnelles. Ce terme regroupe les ressources physiques (PC, smartphones, téléphones, serveurs), virtuelles (comptes, licences, privilèges), et les outils (réseau interne, connexion internet, réseau téléphonique) mis à disposition des utilisateurs.

Utilisateur : toute personne amenée à utiliser les ressources informatiques setec.

1.2 Préambule

L'entreprise met en œuvre un système d'information et de communication nécessaire à son activité, comprenant notamment un réseau informatique et téléphonique. Les utilisateurs, dans l'exercice de leurs fonctions, sont conduits à accéder aux moyens de communication mis à leur disposition et à les utiliser.

Dans un but de transparence à l'égard des utilisateurs, de promotion d'une utilisation loyale, responsable et sécurisée du système d'information, la présente charte définit les règles relatives à l'utilisation de ces ressources. Sa mise en place permet d'éviter toute forme d'abus dans l'usage des outils informatiques et fournit une référence en cas de conflit.

La présente charte précise les droits et devoirs des utilisateurs des ressources informatiques de l'entreprise. Elle pourra évoluer en fonction du contexte légal et de la politique de sécurité notamment applicable au sein de l'entreprise.

Chaque utilisateur doit s'approprier les règles de sécurité et de bon usage définies pour l'utilisation des ressources réseau mises à disposition par l'entreprise dans un objectif professionnel, et dont l'utilisation négligente ou à des fins malveillantes, illicites ou déloyales risquent de mettre en jeu la responsabilité tant de l'entreprise que de l'utilisateur lui-même.

1.3 Champ d'application

La présente charte s'applique à tout collaborateur de l'entreprise ayant un profil d'utilisateur du Système d'Information et de communication de l'entreprise pour l'exercice de ses activités professionnelles.

Par utilisateur, on entend dans la présente charte toute personne autorisée à accéder au système d'information de l'entreprise, soit l'ensemble des personnels de l'entreprise, quels que soient leur contrat, leur fonction, leur niveau hiérarchique ou bien leur degré d'accès aux systèmes et réseaux informatiques et téléphoniques, en ce compris les intérimaires, les prestataires, les stagiaires, étudiants en alternance.

1.4 Usages concernés

La présente charte s'applique à tous les types d'usage qu'ils aient lieu dans les établissements de l'entreprise, dans le cadre d'un usage dit « nomade » quel qu'en soit le lieu, ou dans le cadre d'un accès distant, quel que soit le lieu d'accès.

Cette charte s'applique quelles que soient la fréquence et la périodicité de l'utilisation des ressources / moyens informatiques et de communication électronique.

1.5 Conditions d'utilisation

Tout utilisateur, quel que soit son niveau hiérarchique, est responsable de la protection de l'entreprise et de ses ressources informatiques, contre les pertes et les dégradations, y compris celles qui seraient dues à l'e-mail ou à l'Internet. A ce titre, tout utilisateur doit respecter les normes et pratiques qui suivent. Le non-respect de celles-ci pourrait être considéré comme fautif.

Il est strictement interdit à l'utilisateur de porter atteinte à l'intégrité et au bon fonctionnement des ressources informatiques individuelles ou collectives.

L'utilisation des ressources informatiques doit être effectuée exclusivement à des fins professionnelles.

Bien que les moyens informatiques et de communication électronique soient réservés à un usage professionnel, leur utilisation à des fins non professionnelles, pour répondre en cas d'urgence à des obligations socialement admises, est tolérée.

1.5.1 Téléphone fixe

1. L'utilisation du téléphone à titre privé est admise à condition qu'elle demeure raisonnable.
2. Des restrictions d'utilisation des téléphones fixes sont mises en place en tenant compte de la mission des utilisateurs. A titre d'exemple, certains postes sont limités aux appels nationaux alors que d'autres peuvent passer des appels internationaux.

1.5.2 Messagerie électronique

3. Les utilisateurs disposent, pour l'exercice de leur activité professionnelle, d'une adresse de messagerie électronique normalisée. La messagerie est accessible aussi bien à partir d'un logiciel de messagerie (sur ordinateur ou smartphone) qu'à partir d'un navigateur Internet grâce à un webmail.
4. L'adresse électronique est strictement professionnelle.
5. Néanmoins pour répondre à des besoins à caractère d'urgence et à titre exceptionnel, l'utilisateur peut émettre ou recevoir des courriers électroniques non professionnels sur son adresse électronique professionnelle. Afin que l'entreprise considère ses données comme personnelles les collaborateurs doivent intégrer dans l'objet des messages la mention « Personnel ». Les collaborateurs sont tenus d'informer leurs interlocuteurs pour qu'ils indiquent la même mention dans l'objet de leur mail.

6. Afin d'éviter l'interception de tout message destiné à une Institution Représentative du Personnel (IRP), les messages présentant une telle nature doivent être signalés et classés de la même manière que les messages à caractère personnel, mais en utilisant la mention « IRP » dans leur objet à l'émission et dans le dossier où ils doivent être classés. Les collaborateurs sont tenus d'informer leurs interlocuteurs pour qu'ils indiquent la même mention dans l'objet de leur mail.
7. Les messages électroniques reçus sur la messagerie professionnelle font l'objet d'un contrôle antiviral et d'un filtrage anti-spam. Les utilisateurs sont invités à informer l'administrateur informatique de leur société des dysfonctionnements qu'ils constatent dans le dispositif de filtrage, en particulier en cas de mise en quarantaine de messages dont ils sont certains de la légitimité. Ils sont en revanche autonomes pour déclarer comme indésirables des mails qui n'auraient pas été identifiés comme tel, et vice versa, directement depuis leur logiciel de messagerie.
8. La plus grande vigilance doit être de mise en cas de réclamations, de demandes de renseignements arrivant par e-mail (ex : demande de virement, …) ou de demande de connexion inattendue sur un portail autres que ceux gérés par l'entreprise. En cas de doute les utilisateurs doivent contacter leur référent informatique et ne surtout pas :
    a. Ouvrir de pièces jointes
    b. Cliquer sur un lien
    c. Renseigner le couple identifiant/mot de passe de leur compte informatique
9. Il est interdit d'envoyer des informations concernées par une obligation spécifique de secret (par exemple Confidentiel Défense, Diffusion Restreinte, Confidentiel Industrie, ...) sans cryptage adéquat. Internet et donc tous les outils de la suite Office 365 (Teams, Outlook, Sharepoint, etc.) ne sont pas des moyens d'échange sûrs.
10. En cas d'envoi à une pluralité de destinataires, l'utilisateur doit respecter les dispositions relatives à la lutte contre l'envoi en masse de courriers non sollicités. Il doit également envisager l'opportunité de dissimuler certains destinataires, en les mettant en copie cachée, pour ne pas communiquer leur adresse électronique à l'ensemble des destinataires.

1.5.3 Internet

11. L'accès à des services en ligne (sites web, blogs, forums, chats, etc.) est strictement réservé à un usage professionnel.
12. Il est notamment strictement interdit d'utiliser les moyens de l'entreprise pour se connecter à des sites présentant un risque pour le système d'information de l'entreprise, à caractère pornographique, raciste, sexiste ou ayant un contenu contraire à la loi.
13. L'utilisateur peut toutefois utiliser internet dans un cadre personnel pendant les pauses tant qu'il est raisonnable et ne met pas en danger les données et équipements de l'entreprise.
14. En particulier, l'utilisation de l'Internet à des fins commerciales personnelles en vue de réaliser des gains financiers ou de soutenir des activités lucratives est strictement interdite. Il est aussi prohibé de créer ou de mettre à jour, au moyen de l'infrastructure de l'entreprise, tout site internet, notamment des pages personnelles.
15. L'équipe informatique de la DSIG et setec sécurité ont défini, appliquent et maintiennent à jour une politique de filtrage web afin de bloquer l'accès à certaines catégories de sites (contenu à caractère pornographique, raciste, terroriste, etc.). L'autorisation d'accès à un site bloqué par la politique de filtrage web de l'entreprise doit faire l'objet d'une demande écrite via l'administrateur informatique, après validation formelle de la Direction Générale

de la filiale concernée. En cas de validation de la demande par le groupe, celle-ci sera traitée comme une exception et son maintien pourra être réévalué régulièrement.

16. Les utilisateurs sont informés que toutes les activités sur internet sont enregistrées et que ces traces pourront être exploitées par la DSIG et setec sécurité à des fins de statistiques, de contrôle, de vérifications dans les limites prévues par la loi et en particulier pour limiter les usages abusifs du réseau.
17. L'usage de solutions de type VPN (réseau privé virtuel) permettant de masquer les informations de connexion, autres que celle mise en œuvre par l'entreprise (ex : NordVPN, Mozilla VPN, VPN Opéra, etc.) est interdit pour un usage professionnel.

1.5.4 Poste de travail et fichiers informatiques

18. Les postes de travail sont équipés par le service informatique d'un antivirus mis à jour régulièrement. Les utilisateurs ne doivent pas le désactiver.
19. Il est interdit de modifier le paramétrage et la configuration du poste informatique mis à sa disposition, et notamment de désactiver le verrouillage automatique de la session du poste informatique ou du moyen de communication électronique ou le chiffrement des lecteurs de données sur le poste de travail.
20. Les fichiers et répertoires créés par le salarié à l'aide de l'outil informatique mis à sa disposition par l'entreprise sont présumés avoir un caractère professionnel.
21. La création de répertoire informatique privé sur les postes de travail est tolérée. Ce répertoire, utilisé dans des limites raisonnables pour stocker des documents personnels, doit être identifié par le terme : « PRIVE ou PERSONNEL ». Il n'y a pas de garantie de restauration de ces données.
22. Il est interdit de stocker des données personnelles sur les serveurs de fichier partagés de l'entreprise.
23. Seuls les logiciels faisant l'objet de licences acquises par la société devront être utilisés. Toute copie ou utilisation de licences non autorisées est strictement interdite et peut faire l'objet de sanctions allant jusqu'à l'exclusion. Les utilisateurs fautifs seront responsables face aux éventuelles actions judiciaires engagées par l'éditeur du logiciel.
24. En cas de perte ou de vol de son poste de travail, un signalement doit être fait dans les plus brefs délais par l'utilisateur auprès de l'administrateur informatique de sa société.

1.5.5 Licence d'application et téléchargement

25. La récupération de fichiers auprès de sources inadéquates n'est pas autorisée, car elle présente le risque d'introduire des virus ou des logiciels piratés ou sans licence (jeux, économiseurs d'écran, exécutables, …).
26. Toute installation de logiciel, d'application, de programme ou de fichier exécutable doit être effectuée avec l'accord du référent informatique de la société.

1.5.6 Stockage

27. Les périphériques utilisés pour les échanges de donnée doivent être maîtrisés (clef USB, Disque Dur, …). Il est interdit d'utiliser des périphériques dont la provenance est inconnue.
28. D'une manière générale, il est recommandé de séparer les usages entre les périphériques de stockage professionnels et privés.
29. L'utilisateur doit mettre en œuvre les moyens nécessaires à la conservation des messages et fichiers qui pourraient être indispensables à son activité conformément aux recommandations de son service informatique ou de son responsable hiérarchique.

30. Les données stockées sur les périphériques de stockage (clefs USB, disques durs, …) sont sous la responsabilité des utilisateurs. Ces périphériques étant plus vulnérables (vol, perte) les utilisateurs devront y apporter une attention particulière. En cas de perte ou de vol, un signalement doit être fait par l'utilisateur auprès de l'administrateur informatique de sa société dans les plus brefs délais.

1.6 Paramètres d'accès

31. Les accès à certains éléments du système d'information (comme la messagerie électronique ou téléphonique, les sessions sur les postes de travail, certaines applications) sont protégés par des noms de compte ("login" ou identifiant) ainsi que par des mots de passe (modifiables) fournis à l'utilisateur lors de son arrivée.
32. Des contraintes de complexité, de longueur et de durée de vie sont imposées sur les mots de passe afin de garantir leur unicité, leur confidentialité et leur résistance face à des tentatives d'usurpation.
33. Les mots de passe sont personnels et doivent être gardés confidentiels.
34. Les comptes sont nominatifs et permettent en particulier de contrôler l'activité des utilisateurs.
35. Il est demandé de fermer la session en cours lors d'une absence (déjeuner, rendez-vous) et d'éteindre l'ordinateur le soir.
36. Il est dès lors interdit à l'utilisateur de :
    a. procéder à la moindre divulgation, même intra-service, de son ou de ses identifiants ;
    b. d'utiliser un identifiant autre que le sien, dans l'hypothèse où il en aurait eu connaissance ;
    c. de supprimer, masquer ou modifier son identité ou son identifiant ;
    d. d'user de son droit d'accès pour accéder à des applications, 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.
37. Si ces identifiants, par nature confidentiels ont été communiqués, ou encore s'ils ont été oubliés, l'utilisateur concerné doit, selon la procédure mise en place, renouveler ses identifiants. S'il existe une difficulté à ce renouvellement, ce dernier doit se rapprocher de son référent informatique.
38. Ces identifiants doivent être mémorisés par l'utilisateur ou conserver dans un endroit sûr (coffre-fort, base de données chiffrées, …). En tout état de cause, ils ne doivent pas être transmis à des tiers ou aisément accessibles.
39. Lorsqu'un accès à distance (VPN) est accordé à un utilisateur, celui-ci s'engage à utiliser, à l'exclusion de tout autre, les moyens techniques d'authentification qui lui seront remis. L'accès à distance n'est autorisé que depuis un poste maîtrisé par l'entreprise.

1.7 Protection des données à caractère professionnel

40. Chaque utilisateur est responsable pour ce qui le concerne du respect du secret professionnel et de la confidentialité des informations qu'il est amené à détenir, consulter ou utiliser.
41. En particulier il est tenu de respecter les mesures de confidentialités spécifiques à des affaires ou projets sensibles (Diffusion Restreinte, Confidentiel Défense, …). Ces mesures spécifiques ne sont pas détaillées dans la présente charte. Elles lui sont transmises au lancement du projet ou de l'affaire. L'usage d'outils de chiffrement, à identifier avec le

référent informatique de sa société, est ainsi à privilégier pour le stockage et la diffusion de données sensibles.

42. L'utilisateur doit être particulièrement vigilant sur le risque de divulgation de ces informations dans le cadre d'utilisation d'outils informatiques, dans des lieux autres que ceux de l'entreprise (hôtels, lieux publics…).
43. L'attention de l'utilisateur est attirée sur les risques liés à la diffusion de contenus d'information sur Internet, en particulier au sein des réseaux sociaux et sur les blogs. Il est donc strictement interdit de diffuser la moindre information à caractère professionnel, qu'elle soit ou non protégée par une obligation légale de secret ou une obligation contractuelle de confidentialité sur internet.

1.8 Sécurité

44. L'entreprise, via les actions de la DSIG et de setec sécurité, met en œuvre les moyens appropriés pour assurer la sécurité matérielle et logicielle du système d'information et de communication. A ce titre, il lui appartient de limiter les accès aux ressources sensibles et d'acquérir les droits de propriété intellectuelle ou d'obtenir les autorisations nécessaires à l'utilisation des ressources mises à disposition des utilisateurs.
45. A titre préventif, des systèmes automatiques de filtrage permettant de diminuer les flux d'information et d'assurer la sécurité et la confidentialité des données sont mis en œuvre. Il s'agit notamment du filtrage des sites Internet, de l'élimination des courriels non sollicités, du blocage de certains protocoles.
46. L'utilisateur se doit d'accepter et de faciliter l'exécution de toutes les mises à jour de son ordinateur qui sont configurées par le service informatique de sa société ou par l'équipe informatique de la DSIG.
47. Le caractère « non professionnel/personnel » du répertoire ou des courriers électroniques échangés, ne fait pas obstacle à ce qu'un administrateur ou toute personne « habilitée », accède à ces contenus dans le respect des conditions de confidentialités et dans le cadre de sa mission consistant à assurer le fonctionnement normal et la sécurité des moyens informatiques et de communication électronique, ce notamment dans le cadre d'opération de maintenance, ou en cas de détection ou de suspicion de la présence d'un code malveillant à la mise en quarantaine ou le cas échéant, à la suppression de l'élément quelconque qui comporte ou comporterait un code malveillant.
48. L'utilisateur s'engage à signaler au référent informatique de sa société toute violation ou tentative de violation suspectée de son compte informatique et de manière générale tout dysfonctionnement.
49. La mise en place d'outils de sécurité ne doit pas, toutefois, dispenser les utilisateurs d'une obligation de vigilance à cet égard.
50. En effet, l'utilisateur a la charge, à son niveau, de contribuer à la sécurité des moyens informatiques et de communication électronique mis à sa disposition, principalement en

évitant l'introduction de codes malveillants susceptibles d'endommager le système d'information.

51. Cette vigilance passe notamment par le respect des règles de conduite suivantes :
    a. ne pas ouvrir les pièces jointes ou cliquer sur un lien suspect dans un message reçu de l'extérieur quand l'émetteur est inconnu ou douteux ;
    b. détruire les messages du type « chaîne de solidarité » ;
    c. ne pas renseigner le mot de passe de son compte informatique sur un portail dont il n'est pas certain qu'il est géré et maitrisé par la société, le groupe setec ou par un client/partenaire connu ;
    d. ne pas désactiver ou altérer les fonctionnalités d'authentification multi-facteurs sur son compte informatique ;
    e. ne pas stocker ou transférer des gadgets (logiciel sans licence) reçus ou trouvés sur internet ;
    f. ne pas faire suivre les messages d'alerte de l'arrivée d'un virus mais prévenir son référent informatique ;
    g. Faire preuve de rigueur dans la gestion sécurisée de ses mots de passe
        - Ne pas utiliser le même mot de passe pour des usages différents ;
        - S'efforcer de définir des mots de passe suffisamment complexes. En particulier ne pas utiliser le nom de sa société, « setec », une année, etc. ;
        - Ne pas conserver en clair ses mots de passe. Privilégier l'utilisation d'un outil de type « coffre-fort de mots de passe » qui pourra vous être présenter par le service informatique ;
        - Ne pas transmettre à des tiers les moyens d'authentification qui sont fournis par l'entité, lesquels doivent rester personnels et confidentiels.

52. L'utilisateur a l'interdiction de :
    a. modifier les moyens mis à sa disposition notamment par l'ajout de logiciels, progiciels, même gratuits, ou de matériels pour quelque raison que ce soit ; si ces logiciels ou matériels lui semblent nécessaires pour l'exercice de sa mission, il en fait part à son référent informatique ;
    b. modifier ou détruire, ou tenter de modifier ou détruire, des fichiers sur lesquels il ne dispose d'aucun droit dans le cadre de ses fonctions ;
    c. mettre à la disposition d'utilisateurs non autorisés un accès aux systèmes ou aux réseaux à travers les matériels dont il a usage.
53. L'utilisateur est tenu d'informer le référent informatique de sa société de tout dysfonctionnement, altération, perte, vol, destruction et autre événement pouvant affecter les ressources informatiques. Il doit, en particulier, signaler toute tentative d'intrusion extérieure, de falsification ou la présence de virus.
54. L'utilisateur a la responsabilité de traiter avec la plus grande vigilance les données à caractère personnel et dans le respect du Règlement Général pour la Protection des Données (RGPD). Il doit se rapprocher du référent RGPD de sa société pour identifier quelles précautions prendre et doit lui signaler sans délai toute violation constatée ou suspectée (se référer à l'annexe RGPD accessible sur le site intranet du groupe setec).

1.9 Traçabilité

55. Afin de répondre aux obligations légales qui lui incombent, tenant à sa capacité à apporter des preuves du bon usage des ressources informatiques mis à la disposition des utilisateurs, l'entreprise se réserve le droit de mettre en œuvre des outils de traçabilité tels que des journaux de connexions de l'ensemble des moyens informatiques et de communication électronique.

1.10 Filtrage

56. Afin de répondre aux obligations légales qui lui incombent, tenant à sa capacité de tenter de prévenir tout usage illicite de ces moyens, l'entreprise procède à la mise en place des outils de filtrage (filtrage des contenus, des URL, protocolaire, etc.) permettant d'analyser les conditions d'utilisation de ces moyens, d'interdire des protocoles, ou encore de restreindre certaines catégories de sites internet.
57. Ces outils permettent un contrôle des connexions des utilisateurs.
58. Tout détournement, altération ou modification de ces outils ou des données recueillies grâce à ces outils est strictement interdit.

1.11 Maintenance

59. La mise à disposition des ressources informatiques implique nécessairement des opérations de maintenance technique, qu'il s'agisse de maintenance corrective, de maintenance préventive ou de maintenance évolutive.
60. Ces opérations peuvent nécessiter l'intervention d'une « personne habilitée » soit sur site, soit à distance, conduisant alors cette personne à ce qui est couramment appelé « prendre la main à distance ».
61. Il est rappelé que, dans ce cadre, la « personne habilitée » peut être amenée à prendre connaissance de l'ensemble des éléments présent sur le poste de l'utilisateur, ainsi que des données de connexion, qu'il s'agisse d'un usage professionnel ou privé.
62. Lorsque la « prise de main à distance » est effectuée à la demande de l'utilisateur par une personne extérieure à l'entreprise, par exemple lors d'une webconférence, l'utilisateur est responsable des actions qui sont réalisées Il est tenu de les superviser.

1.12 Contrôle et audit

Les opérations de contrôle et d'audit se distinguent des opérations de maintenance en ce qu'elles portent sur la régularité de l'utilisation des moyens informatiques et de communication électronique.

63. L'utilisation des ressources informatiques pourra faire l'objet d'une surveillance afin de détecter toute utilisation non conforme, ou même d'optimiser cette utilisation et de mener des analyses statistiques.
64. Ces opérations de contrôle et d'audit relèvent des fonctions des services informatiques de chaque société et des équipes DSIG et setec sécurité de l'entreprise, qui ont la charge de la qualité, de la protection et de la sécurité des moyens informatiques et de communication électronique fournis aux utilisateurs.
65. Les utilisateurs sont informés que les administrateurs informatiques sont conduits, de par leurs fonctions, à avoir accès à l'ensemble des informations relatives aux utilisateurs (messages, connexions à internet, etc.), y compris à celles qui sont enregistrées sur le disque dur des postes de travail.

66. En cas de non-respect avéré de la présente charte par un utilisateur, et suivant la gravité des faits, les droits d'accès de l'utilisateur concerné pourront être suspendus temporairement ou définitivement
67. En accord avec la Direction Générale de l'entreprise, des campagnes d'évaluation et de suivi du niveau de sensibilisation des collaborateurs aux bonnes pratiques d'utilisation des ressources informatiques pourront être organisées régulièrement par la DSIG et setec sécurité.

1.13 Contrôles de volume d'activité et de bon fonctionnement

68. En cas de dysfonctionnement constaté par le service informatique de la société ou par la DSIG de l'entreprise et en accord avec la Direction Générale de cette-dernière, il peut être procédé à un contrôle manuel et à une vérification de toute opération effectuée par un ou plusieurs utilisateurs.
    Le service informatique de la société ou la DSIG, en accord avec la Direction Générale de l'entreprise, pourra rétrograder les droits d'accès si des utilisations malveillantes ou non autorisées sont constatées. L'utilisateur sera bien entendu informé au préalable.

1.14 Mobilité

69. Les utilisateurs doivent garder avec eux leurs appareils, supports et fichiers, pendant leurs voyages comme pendant leurs séjours.
70. En cas d'inspection ou de saisie de matériel par des autorités étrangères, l'utilisateur doit informer son responsable hiérarchique au sein de la société ainsi que le référent informatique de cette-dernière.
71. En cas de vol ou de perte d'appareil mobile hébergeant des données de l'entreprise l'utilisateur doit informer immédiatement son référent informatique. Celui-ci pourra, dans la mesure du possible, procéder à des mesures spécifiques (ex : suppression à distance des données, renouvellement des mots de passe, …).
72. L'utilisation des smartphones ou tablette pour relever automatiquement la messagerie électronique comporte des risques particuliers pour la confidentialité des messages, notamment en cas de perte ou de vol de ces équipements. L'accès depuis ces appareils à des messageries électroniques professionnelles peut être soumis à des prérequis de sécurité imposés par la DSIG (verrouillage automatique, mot de passe obligatoire, …).
73. Lors de déplacements professionnels, les utilisateurs doivent éviter, dans la mesure du possible, de connecter une ressource professionnelle (poste de travail ou téléphone mobile) sur un réseau non protégé, et en particulier sur des points d'accès WIFI publics (aéroports, trains, hôtels, etc.). L'utilisation d'une connexion partagée par le téléphone mobile doit être privilégiée.

1.15 Gestion des départs et des absences

74. En cas d'absence ou de départ de l'utilisateur, l'administrateur informatique de sa société se réserve le droit de mettre en place une solution de transfert des messages électroniques ou toute autre solution technologique permettant d'assurer la continuité de l'activité du service.
75. Lors de son départ, l'utilisateur doit remettre en bon état général de fonctionnement, l'ensemble des moyens informatiques et de communication électronique qui lui ont été remis.
76. Il doit préalablement effacer ses fichiers et données privées.

77. Toute copie de documents professionnels doit être autorisée par le responsable hiérarchique.
78. Les comptes informatiques et les données de l'utilisateur sont, en tout état de cause, supprimés dans un délai maximum d'un mois après son départ sauf procédure judiciaire ou enquête administrative.

1.16 Gestion de connaissances et de l'espace collaboratif

79. L'entreprise privilégie le partage et la capitalisation des connaissances, et peut être amenée à mettre en place des espaces collaboratifs de travail.
80. Les utilisateurs des espaces collaboratifs s'engagent à être attentifs à la pertinence des informations diffusées au sein de ces espaces et au travers des outils mis à disposition et à appliquer en particulier les recommandations décrites dans le guide des bonnes pratiques pour l'usage des outils collaboratifs, accessible sur le site intranet du groupe setec.
81. Par souci de qualité, de responsabilité et de protection du patrimoine de l'entreprise, l'utilisation de ces espaces et outils peut faire l'objet d'opérations de contrôle, d'audit, de modération et de traçabilité renforcées.

1.17 Information et sanctions

82. La présente charte est communiquée et rendue accessible à tout utilisateur par sa société. Elle est de plus accessible sur le site intranet du groupe setec.
83. Chaque utilisateur doit se conformer aux procédures et règles de sécurité édictées par la DSIG dans le cadre de la présente charte.
84. Le manquement aux règles et mesures de sécurité de la présente charte est susceptible d'engager la responsabilité de l'utilisateur et d'entraîner à son encontre des avertissements, des limitations ou suspensions d'utiliser tout ou partie du système d'information et de communication, voire des sanctions disciplinaires, proportionnées à la gravité des faits concernés.
85. Dans ce dernier cas, les procédures prévues dans le règlement intérieur et dans le Code du travail seront appliquées.

Entrée en vigueur

Le présent règlement a été soumis pour avis aux représentants du personnel et communiqué en double exemplaire à l'inspecteur du travail dont dépend la société, le 16 juin 2022 .

Il a par ailleurs été déposé en deux exemplaires au secrétariat-greffe du conseil des prud'hommes dont dépend la société, le 16 juin 2022 .

Il sera affiché dans les lieux prévus à cet effet et entrera en vigueur le 16 juillet 2022, soit un mois plus tard.

A Arles, le 16 juin 2022