Charte Informatique

Bonnes pratiques d'utilisation des ressources informatiques, des services Intranet et Internet ainsi que des moyens de communication.

Version 2024

Préambule

La présente Charte a pour objet de décrire les règles d'accès et d'utilisation des ressources informatiques, des services Intranet et Internet ainsi que des moyens de communications de l'association avens.

Elle pose des règles permettant d'assurer la sécurité et la performance du système d'information du groupe, de préserver la confidentialité des données dans le respect de la réglementation en vigueur et des droits et libertés reconnus aux utilisateurs, conformément à la politique de sécurité du système d'information définie par l'association avens et en respect de la Règlementation Générale à la Protection des Données (RGPD)

Elle est disponible sur simple demande et fait l'objet d'une diffusion sur l'Intranet du groupe.

Chaque utilisateur doit en prendre connaissance, un **acte d'engagement** signé de l'utilisateur en atteste dont un exemplaire lui sera remis et un autre remis aux Ressources Humaines.

Ce document est strictement confidentiel et ne s'applique qu'au périmètre informatique de l'association avens.

Le cadre réglementaire

Le cadre réglementaire de la sécurité de l'information est complexe. Il porte notamment sur les grands thèmes suivants :

- Le traitement de données à caractère personnel et le respect de la vie privée *
- Le droit d'accès des salariés, intérimaires à leurs données personnelles
- L'hébergement de données
- Le secret professionnel
- La signature électronique des documents
- Le secret des correspondances
- La lutte contre la cybercriminalité
- La protection des logiciels et des bases de données et le droit d'auteur.

L'utilisateur s'engage à ne pas utiliser les ressources mises à sa disposition à des fins de harcèlement, menaces, injures ou de manière générale violer les droits en vigueur.

* Le règlement général de protection des données (RGPD) est un texte réglementaire européen qui encadre le traitement des données de manière égalitaire sur tout le territoire de l'Union européenne (UE). Il est entré en application le 25 mai 2018.
Le RGPD s'inscrit dans la continuité de la loi française « Informatique et Libertés » de 1978, modifiée par la loi du 20 juin 2018 relative à la protection des données personnelles, établissant des règles sur la collecte et l'utilisation des données sur le territoire français. Il a été conçu autour de trois objectifs :

- renforcer les droits des personnes
- responsabiliser les acteurs traitant des données
- crédibiliser la régulation grâce à une coopération renforcée entre les autorités de protection des données.

En cas de difficultés liées à la gestion de vos données ou de l'exercice de vos droits, vous pouvez contacter notre délégué à la protection des données (DPO) à l'adresse dpo@avens83.fr vous avez également la possibilité de vous renseigner auprès de la CNIL : www.cnil.fr.

Champ d'application et définitions

La charte s'applique à tous les utilisateurs autorisés à exploiter les ressources informatiques, services Intranet, Internet et moyens de communications mis à disposition par l'association avens. Dans la présente Charte, sont désignés sous les termes suivants :

Ressources informatiques : Ensemble des moyens informatiques mis à disposition par l'association (ordinateurs, smartphones, logiciels, ⋯)

Service Intranet/internet : Services web d'échange d'information et de collaboration interne ou externe à l'association avens (logiciels métiers en mode Saas).

Utilisateurs : Toutes personnes (Salariés à titre permanent, en contrat de courte durée, intérimaires, stagiaires, personnels de sociétés, prestataires, visiteurs occasionnels...) ayant accès ou utilisant les ressources informatiques mis à disposition par l'association avens dans le cadre de leur activité professionnelle.

Administrateur : Direction du groupe, Direction des Systèmes d'Information et toute personne de son service ou prestataire qu'ils désigneront en tant que tel et autorisés à gérer les droits d'accès, d'assurer le bon fonctionnement et garantir l'intégrité du système d'information dans la limite de leurs attributions.

L'utilisateur et les outils informatiques

avens confie à l'utilisateur des outils adaptés aux besoins de sa fonction.

Il est important que l'utilisateur respecte les outils et les procédures définies. Pour réduire au maximum les risques de pannes, il est essentiel de ne pas modifier son environnement (appareils, branchements, installation de logiciels⋯). Tout comme il est essentiel de respecter les procédures d'utilisation communiquées.

Il est **strictement interdit** à l'utilisateur d'installer des logiciels, progiciels autres que ceux expressément autorisés par la Direction, d'enregistrer des fichiers personnels susceptibles de créer des risques de sécurité. Il ne doit jamais sauvegarder les données sur des périphériques externes (clés USB, disques externes⋯) et ne jamais emporter les données en dehors du lieu de travail.

Ne pas utiliser comme outil de sauvegarde ou de synchronisation les services « *cloud* » (exemple OneDrive, ou google drive⋯)

Il est recommandé d'éteindre « proprement » son ordinateur par arrêt logiciel et non par interrupteur(on/off) pour terminer correctement sa session de travail (hors cas de blocages techniques), et de verrouiller sa session informatique lorsqu'il quitte son poste de travail.

Ne pas laisser trainer les documents sensibles utilisés pour l'activité professionnelle (documents confiés, envoyés, imprimés ou photocopiés (penser à les récupérer sur les fax, copieurs ou imprimantes).

Les utilisateurs de postes portables s'engagent, quel que soit l'endroit où ils se trouvent, à sécuriser leur matériel et l'accès aux données qu'il contient. De ne jamais transporter l'intégralité des fichiers qui auraient une valeur stratégique pour avens. Les données et

informations sensibles stockées sur le disque dur du portable devront être protégées conformément aux directives fournies par la direction dont relève l'utilisateur.

Un compte utilisateur unique est confié à chaque utilisateur (login + mot de passe), il est personnellement responsable de l'utilisation qui peut être faite de son compte**.**

Un mot de passe temporaire est fourni à la création du compte que l'utilisateur devra changer à sa première connexion.

Règle de gestion du mot de passe

Votre mot de passe doit rester secret car il constitue votre principale garantie contre toute intrusion ou malversation.

Il doit être suffisamment **long et complexe** : Minimum 12 caractères alphanumériques/spéciaux.
Il doit être impossible à deviner : par exemple ne doit pas être attaché à l'utilisateur d'une quelconque façon que ce soit (identique au login même en inversant les caractères, comporter le nom et/ou prénom de l'utilisateur ou de membres de sa famille, de numéro de téléphone personnel ou professionnel, de marque de la voiture ou toute autre référence à quelque chose appartenant à l'utilisateur...
Le mot de passe **ne doit pas être enregistré dans les navigateurs internet**

Assurer la sécurité de ses mots de passe
Optez plutôt pour un gestionnaire de mots de passe. Cet outil chiffre vos données privées et personne n'a accès à vos informations. Un gestionnaire de mots de passe est comme un coffre-fort, vos données sont enregistrées et protégées par un mot de passe maître. Exemples de coffres forts numériques validés par la DSI avens et l'ANSSI : Keepass, Bitwarden⋯

Pour éviter les virus, n'ouvrez jamais les messages - ou les pièces jointes - aux intitulés suspects. Détruisez-les. En cas de doute, informez-en votre responsable ou le service informatique.
En cas d'anomalie ou de doute constaté, l'utilisateur **doit stopper toute activité** et prévenir immédiatement le service informatique ou la Direction.

Engagements Utilisateur

Chaque utilisateur prend conscience que d'une part l'usage de ces ressources obéit à des règles qui s'inscrivent dans le respect de la loi et de la sécurité du groupe et que d'autre part sa négligence ou sa mauvaise utilisation des ressources fait encourir des risques à l'ensemble de l'association avens, et donc à lui-même.

Chaque utilisateur s'engage en sa qualité à connaître et appliquer l'ensemble des dispositions de la présente charte de bon usage de l'informatique.

Chaque utilisateur est responsable de la pérennité de ses fichiers, données, informations... ainsi que des accès en lecture et modification qu'il peut donner à d'autres personnes ou utilisateurs. Il doit donc concourir à la protection des dites ressources, en faisant preuve de prudence, dans le respect de la législation, qui protège notamment les droits de propriété intellectuelle, le secret des correspondances, les données personnelles, les systèmes de traitement

automatisé de données, le droit à l'image des personnes, l'exposition des mineurs aux contenus préjudiciables.
Il ne doit en aucun cas se livrer à une activité concurrente à celle du groupe ou susceptible de lui causer un quelconque préjudice en utilisant le système d'information et de communication.

L'utilisateur s'engage à utiliser les chartes de communication fournies par l'association avens (logo, trames, polices de caractères...) et entre-autre à respecter les chartes de signature des documents professionnels.

L'utilisateur s'engage à prendre connaissance et respecter les **annexes spécifiques** liées à l'utilisation des outils métiers spécifiques tels que « Teams », « Messagerie 365 », ⋯ L'ensemble de ces documents étant fournis en annexe de la présente charte.

Les moyens de contrôle et de protection de l'intégrité de avens.

La direction de l'association avens fournit un système d'information qui s'appuie sur une infrastructure informatique. Elle doit assurer la mise en sécurité de l'ensemble, c'est-à-dire protéger ces ressources contre des pannes, des erreurs ou des malveillances.

Les enjeux majeurs de la sécurité du système d'information sont la qualité et la continuité de service des outils métiers nécessaire au traitement et à l'accompagnement des usagers du groupe tout en garantissant le respect du cadre juridique sur l'usage de leurs données personnelles, de celle des utilisateurs ainsi que des partenaires de l'association avens.

Pour cela, la direction déploie un ensemble de dispositifs informatiques techniques mais aussi organisationnels.

Au-delà des outils, la bonne utilisation des ressources informatiques est essentielle pour garantir à un bon niveau leur sécurité et leur sureté.

Certains comportements humains, par ignorance des risques, peuvent fragiliser le système d'information.

Pour des nécessités de maintenance et de gestion, l'utilisation des ressources matérielles ou logicielles, les échanges via le réseau, ainsi que les rapports des télécommunications peuvent être analysés et contrôlés dans le respect de la législation applicable,

L'inobservation des règles d'utilisation définies ci-dessus pourra entraîner le prononcé de sanctions disciplinaires en fonction de la gravité du manquement commis.
Afin de garantir l'effectivité des principes définis ci-dessus, avens pourra exercer des contrôles à posteriori sur l'utilisation de ces différents moyens d'information et de communication, dans le respect du droit à la vie privée de chacun.

Ces contrôles porteront notamment sur l'utilisation des différents outils d'information et de communication, le nombre d'utilisateurs, le coût et la durée des communications, les plages et l'amplitude horaire de connexion, les sites les plus visités en temps et en fréquence.
Ces contrôles porteront également sur les machines et périphériques de stockage qui pourraient avoir été connectés au réseau de l'entreprise ainsi que sur les CD, DVD, clé USB ou tout autre support qui auraient eu pour objet de copier des informations appartenant à avens.

avens assure une traçabilité sur l'ensemble des accès aux applications et aux ressources informatiques qu'elle met à disposition pour des raisons d'exigence réglementaire de

traçabilité, de prévention contre les attaques et de contrôle du bon usage des applications et des ressources.

avens respecte la confidentialité des données et des traces auxquelles ils sont amenés à accéder dans l'exercice de leur fonction, mais peuvent être amené à les utiliser pour mettre en évidence certaines infractions commises.

Pour des nécessités de sécurité, de maintenance et de gestion technique, et pour pouvoir réagir en cas d'attaque des systèmes informatiques, tous les événements et toutes les informations échangées par le biais du réseau Internet sont enregistrés.

Il peut être procédé à un contrôle manuel et à une vérification de toute opération effectuée par un ou plusieurs utilisateurs.

Les fichiers et messages contenus sur les outils informatiques de l'entreprise sont présumés être de nature professionnelle. Par conséquent l'employeur dispose d'un libre accès à ces derniers.

En revanche, sauf risque ou événement particulier, la Direction Générale avens ou la DSI, ne peuvent ouvrir les fichiers ou messageries identifiés par l'utilisateur comme « privé » ou « personnel » ou liés à la délégation de personnel (IRP).

Responsabilités et Sanctions

Le non-respect des règles et mesures de sécurité figurant dans la présente charte engage la responsabilité personnelle de l'utilisateur. Dès lors qu'il est prouvé que les faits fautifs lui sont personnellement imputables les sanctions disciplinaires définies par le règlement intérieur de l'association avens, seront appliquées, de manière appropriée et proportionnée aux manquements commis.

Les règles définies dans la présente Charte ont été fixées par la Direction Générale de l'association avens dans le respect des dispositions législatives et réglementaires applicables (CNIL, RGPD, Code du travail ...).

avens ne pourra être tenu pour responsable des détériorations d'informations ou des infractions commises par un utilisateur qui ne se sera pas conformé aux règles d'accès et d'usage des ressources informatiques et des services internet décrites dans la Charte.

Publicité – Dépôt – Entrée en Vigueur

La présente charte est annexée au règlement intérieur de l'association avens.
En application des dispositions de l'article L. 1321-4 du Code du travail, elle a été soumise à l'avis des IRP.

Conformément aux articles L. 1321-4, R. 1321-1 et R. 1321-2 du Code du Travail, la présente charte est également déposée au secrétariat du Greffe du Conseil de Prud'hommes de TOULON et transmise à l'inspecteur du travail, accompagnée de l'avis des délégués du personnel.

Dès à présent elle est affichée sur les lieux de travail et d'embauche de l'association avens pour valoir ce que de droit.

Elle entre en vigueur dès le

Par la suite, toutes les modifications et adjonctions apportées à la présente charte feront l'objet des mêmes procédures de consultation, de communication et de publicité.

Liste des annexes

annexe 1 : utilisation d'internet
annexe 2 : utilisation de la messagerie
annexe 3 : aparté sur les smartphones et sur la vidé protection
annexe 4 : utilisation de Teams

En cas de modification de la législation, de l'évolution des outils et de la stratégie de l'association avens, la présente charte et ses annexes pourront être amenées à évoluer, ainsi que la limite des responsabilités décrites.

Fait à **Toulon,** le **1er juillet 2024**

Le Directeur Général	Le Directeur des Systèmes d'Information