Rédigé le 1er mai 2018 (révisé le 29/11/2022)

Charte d'utilisation des ressources informatiques de l'Association de Développement Sanitaire de la Côte d'Emeraude (ADSCE)

INTRODUCTION

La présente charte définit les conditions d'accès et les règles d'utilisation des moyens informatiques et des ressources extérieures via les outils de communication au sein de l'ADSCE.
Elle a également pour objet de sensibiliser les utilisateurs aux risques liés à l'utilisation de ces ressources en termes d'intégrité et de confidentialité des informations traitées.
Ces risques imposent le respect de certaines règles de sécurité et de bonne conduite. L'imprudence, la négligence ou la malveillance d'un utilisateur peuvent en effet avoir des conséquences graves de nature à engager sa responsabilité civile et/ou pénale ainsi que celle de l'association.

PROTECTION DES DONNÉES À CARACTÈRE PERSONNEL

La **loi n°78-17 du 6 janvier 1978** modifiée en 2004 relative à l'informatique, aux fichiers et aux libertés définit les conditions dans lesquelles des traitements de données à caractère personnel peuvent être effectués. Elle ouvre aux personnes concernées par les traitements un droit d'accès et de rectification des données enregistrées sur leur compte.
L'ADSCE a désigné le Directeur Général, Christophe HERVÉ, comme correspondant à la protection des données à caractère personnel. Ce dernier a pour mission de veiller au respect des dispositions de la loi n°78-17 du 6 janvier 1978 modifiée.
Il est obligatoirement consulté par le responsable des traitements préalablement à leur création.
Il recense dans un registre la liste de l'ensemble des traitements de données à caractère personnel de l'ADSCE de la Côte d'Emeraude au fur et à mesure de leur mise en œuvre. Cette liste est tenue à disposition de toute personne en faisant la demande.
Le correspondant veille au respect des droits des personnes (droit : d'accès, de rectification, d'opposition, d'oubli, de portabilité, au refus du profilage, à la limitation du traitement des données*). En cas de difficultés rencontrées lors de l'exercice de ces droits, les personnes concernées peuvent saisir leur responsable hiérarchique qui fera le lien avec le correspondant représenté par Christophe Hervé, Directeur Général.

Le Délégué à la Protection des Données (DPO) désigné par le correspondant est Aurélie DELESTRE. Elle est en charge de la conformité à la loi informatique et libertés ainsi qu'aux futures dispositions du règlement général sur la protection des données (RGPD). Vous pouvez contacter votre DPO par email (aurelie.delestre@adsce.fr) ou par téléphone (06.27.33.87.20).

* https://rgpd.orson.io/11/rgpd-et-droits-des-personnes

LE CHAMP D'APPLICATION DE LA CHARTE

La présente charte s'applique à tout utilisateur du Système d'Information et de communication de l'ADSCE pour l'exercice de ses activités professionnelles. **L'utilisation à titre privé de ces outils est tolérée, mais doit être raisonnable et ne pas perturber le bon fonctionnement du service.**

La charte est diffusée à l'ensemble des utilisateurs par note de service et, à ce titre, mise à disposition sur l'intranet de l'ADSCE de la Côte d'Emeraude. Elle est systématiquement remise à tout nouvel arrivant.

Des actions de communication internes sont organisées régulièrement afin d'informer les utilisateurs des pratiques recommandées.

Quelques définitions :

On désignera sous le terme « **utilisateur** » toute personne autorisée à accéder aux outils informatiques et aux moyens de communication de l'ADSCE de la Côte d'Emeraude et à les utiliser : employés, stagiaires, intérimaires, personnels de sociétés prestataires, visiteurs occasionnels....

Les termes "**outils informatiques et de communication**" recouvrent tous les équipements informatiques, de télécommunications et de reprographie de l'ADSCE.

LES RÈGLES D'UTILISATION DU SYSTÈME D'INFORMATION DE l'ADSCE

Chaque utilisateur accède aux outils informatiques nécessaires à l'exercice de son activité professionnelle dans les conditions définies par l'ADSCE.

1. Les modalités d'intervention du correspondant

Le correspondant veille au bon fonctionnement et la sécurité des réseaux, des moyens informatiques et de communication de l'ADSCE.

Les agents/personnels de ce service disposent d'outils techniques afin de procéder aux investigations et au contrôle de l'utilisation des systèmes informatiques mis en place.

Ils ont accès à l'ensemble des données techniques mais s'engagent à respecter les règles de confidentialité applicables aux contenus des documents.

Ils sont assujettis au devoir de réserve et sont tenus de préserver la confidentialité des données qu'ils sont amenés à connaître dans le cadre de leurs fonctions.

Les informations directement ou indirectement liées à l'ADSCE ne peuvent ni ne doivent apparaitre sur les réseaux sociaux privés (Facebook, twitter...).

2. Le rôle et mission de l'administrateur

Le Directeur général, sa Directrice adjointe sont les administrateurs de la structure, ils gèrent les accès informatique et en porte la responsabilité. Ils sont les seuls à présenter le profil superviseur permettant de gérer les habilitations de chacun et les droits d'accès. L'assistante de Direction quant à elle a la possibilité de créer et modifier les adresses mails professionnels, ainsi que les mots de passe de messagerie via l'hébergement de données sécurisées (HDS via OVH).

3. L'authentification

L'accès aux ressources informatiques repose sur l'utilisation d'un nom de compte ("login" ou identifiant) fourni à l'utilisateur lors de son intégration. Un mot de passe est associé à cet identifiant de connexion.
Les moyens d'authentification sont personnels et confidentiels.

Actuellement, le mot de passe doit être composé de 5 caractères minimum combinant chiffres, lettres et/ou caractères spéciaux. Il ne doit comporter ni le nom, prénom ni l'identifiant d'ouverture de la session de travail.

4. Les règles de sécurité

Tout utilisateur s'engage à respecter les règles de sécurité suivantes :

- Signaler à la direction de site ou direction générale de l'ADSCE de la Côte d'Emeraude toute violation ou tentative de violation suspectée de son compte réseau et de manière générale tout dysfonctionnement.
- Ne jamais confier son identifiant/mot de passe.
- Ne jamais demander son identifiant/mot de passe à un collègue ou à un collaborateur.
- Ne pas masquer sa véritable identité.
- Ne pas usurper l'identité d'autrui.
- Ne pas modifier les paramétrages du poste de travail.
- Ne pas installer de logiciels sans autorisation.
- Ne pas copier, modifier, détruire les logiciels propriétés de l'ADSCE.
- Verrouiller son ordinateur dès qu'il quitte son poste de travail.
- Utiliser, échanger, ou discuter des informations utilisées par l'ADSCE à l'extérieur ou à des fins privées.
- Ne pas accéder, tenter d'accéder, supprimer ou modifier des informations qui ne lui appartiennent pas.
- Toute copie de données sur un support externe est soumise à l'accord du supérieur hiérarchique et doit respecter les règles définies par l'ADSCE de la Côte d'Emeraude.

En outre, il convient de rappeler que les visiteurs ne peuvent avoir accès au Système d'Information de l'ADSCE sans l'accord préalable du directeur général.
Les intervenants extérieurs doivent s'engager à faire respecter la présente charte par leurs propres salariés et éventuelles entreprises sous-traitantes. Dès lors, les contrats signés entre l'ADSCE et tout tiers ayant accès aux données, aux programmes informatiques ou autres moyens, doivent comporter une clause rappelant cette obligation.

LES MOYENS INFORMATIQUES

1. Configuration du poste de travail

L'ADSCE met à disposition de chaque utilisateur un poste de travail doté des outils informatiques nécessaires à l'accomplissement de ses fonctions.

L''utilisateur ne doit pas :

- Modifier ces équipements et leur fonctionnement, leur paramétrage, ainsi que leur configuration physique ou logicielle.
- Connecter ou déconnecter du réseau les outils informatiques et de communications sans y avoir été autorisé par l'équipe informatique interne.
- Déplacer l'équipement informatique (sauf s'il s'agit d'un « équipement nomade »)
- Nuire au fonctionnement des outils informatiques et de communications.

Toute installation de logiciels supplémentaires (logiciels de consultation de fichiers multimédia) est subordonnée à l'accord de la direction générale

2. Equipements nomades et procédures spécifiques aux matériels de prêt.

- **Equipements nomades**

On entend par « **équipements nomades** » tous les moyens techniques mobiles (ordinateur portable, imprimante portable, téléphones mobiles ou smartphones, CD ROM, clé USB, cloud etc.. ..).

Quand cela est techniquement possible, ils doivent faire l'objet d'une sécurisation particulière, au regard de la sensibilité des documents qu'ils peuvent stocker, notamment par chiffrement.

L'utilisation d'un téléphone mobile professionnel 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. Quand ces appareils ne sont pas utilisés pendant quelques minutes, ils doivent donc être verrouillés par un moyen adapté de manière à prévenir tout accès non autorisé aux données qu'ils contiennent.

- **Procédures spécifiques aux matériels de prêt**

L'utilisateur doit renseigner et signer un registre, tenu par la direction générale, actant la remise de l'équipement nomade ou encore la mise à disposition d'un matériel spécifique pour la tenue d'une réunion (vidéoprojecteur). Il en assure la garde et la responsabilité et doit informer la direction générale en cas d'incident (perte, vol, dégradation) afin qu'il soit procédé aux démarches telles que la déclaration de vol ou de plainte. Il est garant de la sécurité des équipements qui lui sont remis et ne doit pas contourner la politique de sécurité mise en place sur ces mêmes équipements. Le retour du matériel est consigné dans le registre.

3. Internet

Les utilisateurs peuvent consulter les sites internet présentant un lien direct et nécessaire avec l'activité professionnelle, de quelque nature qu'ils soient.

Toutefois, une utilisation ponctuelle et raisonnable, pour un motif personnel, des sites internet dont le contenu n'est pas contraire à la loi, l'ordre public, et ne met pas en cause l'intérêt et la réputation de l'institution, est admise uniquement entre 12h et 14h.

4. Messagerie électronique

- **Conditions d'utilisation**

La messagerie mise à disposition des utilisateurs est destinée à un usage professionnel. L'utilisation de la messagerie à des fins personnelles est tolérée si elle n'affecte pas le travail de l'agent ni la sécurité du réseau informatique de l'ADSCE.

Tout message qui comportera la mention expresse ou manifeste de son caractère personnel bénéficiera du droit au respect de la vie privée et du secret des correspondances. A défaut, le message est présumé professionnel.

L'ADSCE s'interdit d'accéder aux dossiers et aux messages identifiés comme « personnel » dans l'objet de la messagerie du salarié.

L'utilisation de la messagerie électronique doit se conformer aux règles d'usage définies et validées par le directeur de site:

- volumétrie de la messagerie,
- taille maximale de l'envoi et de la réception d'un message,
- nombre limité de destinataires simultanés lors de l'envoi d'un message,
- gestion de l'archivage de la messagerie.

- **Consultation de la messagerie**

En cas d'absence d'un salarié et afin de ne pas interrompre le fonctionnement du service, la direction du site ou générale de L'ADSCE peut ponctuellement transmettre au supérieur hiérarchique un message électronique à caractère exclusivement professionnel et identifié comme tel par son objet et/ou son expéditeur (cf. conditions d'utilisation).

Le supérieur hiérarchique n'a pas accès aux autres messages de l'agent. L'agent concerné est informé dès que possible de la liste des messages qui ont été transférés.

En cas d'absence prolongée d'un agent (longue maladie), le chef de service peut demander à la direction générale, le transfert des messages reçus.

- **Courriel non sollicité**

L'ADSCE dispose d'un outil permettant de lutter contre la propagation des messages non désirés (spam). Aussi, afin de ne pas accentuer davantage l'encombrement du réseau lié à ce phénomène, les utilisateurs sont invités à limiter leur consentement explicite préalable à recevoir un message de type commercial, newsletter, abonnements ou autres, et de ne s'abonner qu'à un nombre limité de listes de diffusion notamment si elles ne relèvent pas du cadre strictement professionnel.

5. Téléphone

L'ADSCE met à disposition des utilisateurs, pour l'exercice de leur activité professionnelle, des téléphones fixes et mobiles.

L'utilisation du téléphone à titre privé est admise à condition qu'elle demeure raisonnable.

Des restrictions d'utilisation par les agents des téléphones fixes sont mises en place en tenant compte de leurs missions. A titre d'exemple, certains postes sont limités aux appels nationaux, d'autres peuvent passer des appels internationaux.

L'ADSCE s'interdit de mettre en œuvre un suivi individuel de l'utilisation des services de télécommunications. Seules des statistiques globales sont réalisées sur l'ensemble des appels entrants et sortants. Elle vérifie que les consommations n'excèdent pas les limites des contrats passés avec les opérateurs.

L'ADSCE s'interdit d'accéder à l'intégralité des numéros appelés via l'autocommutateur mis en place et via les téléphones mobiles. Toutefois, en cas d'utilisation manifestement anormale, sur demande du directeur de site, l'ADSCE se réserve le droit d'accéder aux numéros complets des relevés individuels. L'association peut à tout moment suspendre la fonctionnalité de la ligne via la plateforme, ceci est systématiquement validé par le CIL.

6. L'utilisation des outils informatiques par les représentants du personnel

Les représentants du personnel au Comité Social et Economique (CSE) utilisent, dans le cadre de leur mandat, les outils informatiques qui leur sont attribués pour l'exercice de leur activité professionnelle. Ils disposent d'une adresse électronique dédiée (cse@adsce.fr).

7.Consultation du Dossier de l'Usager Informatisé (DUI)

Le dossier Informatisé de l' Usager permet un suivi simple et agile des usagers des établissements sociaux et médico-sociaux.

Il respecte les spécifications du RGPD, du projet « Ma santé 2022 », ainsi que celles des programmes de financement ESMS numérique et SONS.

Il facilite la prise en charge et la gestion du parcours des usagers des établissements sociaux et médico-sociaux (ESMS) depuis l'admission de l'usager jusqu'à la gestion de la relation usager en passant par la gestion administrative, les soins de l'usager, son accompagnement et la coordination des acteurs internes et externes.

Le dossier de l'usager informatisé (DUI) est conçu pour suivre les usagers dans le respect de leurs droits fondamentaux décrits dans la loi 2002-2 du 2 janvier 2002 rénovant le Code de l'action sociale et des familles et le règlement 2016-679, dit RGPD (Règlement général sur la protection des données). Il garantit la diffusion d'une information adaptée et nécessaire, aux professionnels, aux usagers et aux familles.

Les échanges entre les collaborateurs sont facilités, via une messagerie sécurisée et des écrits professionnels comme le cahier de liaison ou les comptes rendus des réunions d'équipes.

La mise en place d'un DUI interopérable implique de sensibiliser les professionnels aux enjeux d'échange et de partage des données de santé.

C'est l'occasion de rappeler les obligations légales, le secret professionnel, les droits des personnes et la définition d'une donnée de santé à caractère personnel mais aussi de revenir sur la distinction entre l'échange et le partage de données, et ce qu'implique l'accès au DMP ou à MSSanté pour les professionnels.
Nous avons pour devoir de former les professionnels identifiés et mener des actions de sensibilisation auprès de l'ensemble de nos professionnels sur chaque structure, par le biais d'un référent en identitovigilance, désigné.
Ce référent s' assure de la connaissance partagée des notions essentielles et des bonnes pratiques relatives à l'identitovigilance et au fonctionnement de l'INS.

DROITS DES PERSONNES EN MATIERE DE RGPD

Il existe différents droits des personnes en matière de Réglementation dur la Protection des Données.

- Droits absolus non opposables tels que : *(cf. FO 119)*
  - Droit à l'information
  - Droit d'accès pour les personnes aux données le concernant
  - Droit de rectification de ces données
- Droits sous conditions donc opposables, auxquels nos structures répondent uniquement s'ils n'entravent pas l'accompagnement des personnes ou si leurs satisfactions ne nous empêche pas de répondre à des obligations réglementaires :
  - Droit d'opposition
  - Droit à la limitation
  - Droit à l'effacement, à l'oubli, à la mort numérique
  - Droit à la portabilité

L'ADMINISTRATION DU SYSTEME D'INFORMATION

Afin de surveiller le fonctionnement et de garantir la sécurité du système d'information de la Commission, différents dispositifs sont mis en place.

1. Les systèmes automatiques de filtrage

A titre préventif, des systèmes automatiques de filtrage permettant de diminuer les flux d'information pour L'ADSCE 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 (Peer to Peer, messagerie instantanée....).

2. Les systèmes automatiques de traçabilité

Le correspondant de L'ADSCE opère sans avertissement les investigations nécessaires à la résolution de dysfonctionnements du système d'information ou de l'une de ses composantes, qui mettent en péril son fonctionnement ou son intégrité.
Il s'appuie pour ce faire, sur des fichiers de journalisation (fichiers « logs ») qui recensent toutes les connexions et tentatives de connexions au système d'information. Ces fichiers comportent les données suivantes : dates, postes de travail et objet de l'évènement.

Le correspondant est le seul utilisateur de ces informations qui sont effacées à l'expiration d'un délai de trois mois.

3. Gestion du poste de travail

A des fins de maintenance informatique, le correspondant interne de l'ADSCE peut accéder à distance à l'ensemble des postes de travail. Cette intervention s'effectue avec l'autorisation expresse de l'utilisateur.
Dans le cadre de mises à jour et évolutions du système d'information, et lorsqu'aucun utilisateur n'est connecté sur son poste de travail, le correspondant peut être amené à intervenir sur l'environnement technique des postes de travail. Il s'interdit d'accéder aux contenus.

4 – Système « Serveur » / Data center

L'ADSCE est en contrat avec la société Arche MC2, pour la sauvegarde des données et l'administration de son serveur. Cet hébergement est agréé « hébergement données de santé ».
Le répertoire général est divisé en deux répertoires « X et Y », ils donnent l'accès aux données de l'association.
Chaque session, donc chaque utilisateur a accès aux fichiers en fonction de ses droits.
Ces droits sont administrés par le CIL. Toutes modifications sont effectuées par l'administrateur (Arche MC2) à la demande du CIL.

PROCÉDURE APPLICABLE LORS DU DÉPART DE L'UTILISATEUR

Lors de son départ, l'utilisateur doit restituer les matériels mis à sa disposition par l'ADSCE.
Il doit préalablement effacer ses fichiers et données privées. L'ADSCE ne saurait être tenue responsable des fichiers personnels non effacés par l'utilisateur.
Toute copie de documents professionnels doit être autorisée par la Direction générale ou à défaut, la direction adjointe.
Les comptes et les données personnelles de l'utilisateur sont, en tout état de cause, supprimés dans un délai maximum d'un mois après son départ.

RESPONSABILITÉS- SANCTIONS

Le manquement aux règles et mesures de sécurité et de confidentialité définies par la présente charte est susceptible d'engager la responsabilité de l'utilisateur et d'entraîner des sanctions à son encontre.
Des sanctions en interne peuvent être prononcées, elles consistent :

- dans un premier temps, en un rappel à l'ordre émanant du directeur de site, après avis du directeur général, Christophe HERVE, en cas de non-respect des règles énoncées par la charte ;
- dans un second temps, et en cas de renouvellement du directeur général, Christophe HERVE, après avis, en des sanctions disciplinaires adoptées après saisine des institutions représentatives du personnel.

Le non-respect des lois et textes applicables en matière de sécurité des systèmes d'information (cf. liste des textes en annexe) est susceptible de sanctions pénales prévues par la loi.

ENTRÉE EN VIGUEUR DE LA CHARTE

La présente charte a été adoptée après information et consultation du comité consultatif paritaire.

Elle est applicable à compter du 1er Juin 2018.

_____, le _____20

La Direction

Le(a) salarié(e) *

Direction Générale
M. HERVE Christophe
6 rue de la ville biais LA RICHARDAIS
BP 30130 - 35801 DINARD Cedex
02.99.16.16.13 - christophe.herve@adsce.fr

(*) Signature précédée de la mention « lu et approuvé »

ANNEXE

DISPOSITIONS LÉGALES APPLICABLES

Directive 95/46/CE du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données.

Loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés modifiée par la loi n°2004-801 du 6 août 2004.
Dispositions Pénales :
- Code Pénal (partie législative) : art 226-16 à 226-24
- Code Pénal (partie réglementaire) : art R. 625-10 à R. 625-13

Loi n°88-19 du 5 janvier 1988 relative à la fraude informatique dite loi Godfrain. Dispositions pénales : art 323-1 à 323-3 du Code pénal.

Loi n°2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique (LCEN)

Loi n°94-361 du 10 mai 1994 sur la propriété intellectuelle des logiciels.
Disposition pénale : art L.335-2 du Code pénal.