LARNAY Sagesse

ACCUEIL DE PERSONNES EN SITUATION DE HANDICAPS SENSORIELS

Politique de sécurité du système d'information

F.A.M
Foyer d'Accueil Médicalisé

F.V
Foyer de Vie

E.H.P.H.S.A.D
Etablissement d'Hébergement pour Personnes Handicapées Sensorielles, Agées Dépendantes

Mesures spécifiques à la protection des données à caractère personnel

En référence au RÈGLEMENT (UE) 2016/679 DU PARLEMENT EUROPÉEN ET DU CONSEIL du 27 avril 2016

Nom du chef d'établissement : Olivier Besseron

Commenté [BB1]: Modif nom

Nom du référent sécurité : B Blondeau

Date d'entrée en vigueur : 01/01/2020

ASSOCIATION LARNAY SAGESSE – 5 rue Charles Chaubier de Larnay – 86580 BIARD
☎ 05 49 58 46 99 /// 🖷 05 49 53 26 07
direction.generale@larnay-sagesse.fr /// www.larnay-sagesse.fr

Table des matières

Page 3

1. Objet

Le RÈGLEMENT (UE) 2016/679 DU PARLEMENT EUROPÉEN ET DU CONSEIL du 27 avril 2016 impose que les organismes mettant en œuvre des traitements ou disposant de fichiers de données en garantissent la sécurité. Par sécurité des données, on entend l'ensemble des « précautions utiles, au regard de la nature des données et des risques présentés par le traitement », pour notamment, « empêcher que les données soient déformées, endommagées, ou que des tiers non autorisés y aient accès. »

2. Contexte de l'entreprise

Association gérant des établissements médico-sociaux, les DCP traitées sont utilisées pour son activité de soin, d'accompagnement des résidents et des données RH du personnel.
L'association est localisée sur un seul site.

3. Base documentaire

Les documents et procédures, mentionnées dans les chapitres suivants, sont stockées sous :

- Dossier « Boite à outils » : 10- RGPD
- Dans la GED : dossier « RGPD »

Commenté [BB2]: Mise à jour des liens

4. DCP - Politiques de sécurité de l'information

4.1. Politique de sécurité

La direction de l'établissement s'engage à fournir les ressources pour faire appliquer la présente politique.

4.2. Révision des politiques de sécurité de l'information

La politique de sécurité est révisée, à minima, une fois par an, lors du bilan annuel DCP.

5. DCP - Organisation de la sécurité et mobilité

5.1. Fonctions et responsabilités liées à la sécurité de l'information

La mise en place de la sécurité relève de la fonction du responsable IT sous la responsabilité de la direction générale.

5.2. Politique en matière d'appareils mobiles

Les personnes accédant au Système d'Information en situation de mobilité sont sensibilisées aux bonnes pratiques pour éviter le vol de matériel, et aux bonnes pratiques de discrétion dans les lieux publics et les transports.
Formation : Mobilité
Support : Les bonnes pratiques en déplacement

6. DCP - La sécurité des données des ressources humaines

6.1. Responsabilités associées au contrat de travail

Les DCP du personnel sont à usage contractuelles. Elles sont accessibles seulement par le service RH et les cadres hiérarchiques. Tous salariés peuvent consulter son dossier sur simple demande.
Formulaire : Demande d'accès à ses DP

Commenté [BB3]: Changement du terme "direction"

7. DCP - Gestion du matériel

7.1. Mise au rebut des supports

Tous les supports de stockage des ordinateurs, portables ou serveurs mis au rebus, sont détruits avant envoi au recyclage ou réutilisés en interne après effacement.
Document : Procédures IT

8. DCP - Contrôle d'accès logique

8.1. Maîtrise de la gestion des accès utilisateur

Les droits d'accès aux différentes ressources sont gérés par le service informatique selon le profil métier et les missions de la personne.
Un annuaire type LDAP gère les comptes utilisateurs et leurs droits.
Les logiciels RH et de soins ont leur propre base d'utilisateurs avec une gestion des habilitations.

8.2. Revue des droits d'accès utilisateur

Une revue complète est réalisée une fois par an, en plus des changements ponctuels lors d'un départ ou d'un changement de poste.
Document : Procédures entrée/sortie d'un salarié

9. DCP – Chiffrement

9.1. Politique d'utilisation des mesures de chiffrement

Les documents médicaux sont chiffrés et échangés (dans la mesure du possible) par la messagerie sécurisée MSSANTE avec les différents acteurs de santé extérieurs à l'association (CHU, spécialistes, Labo). Cette messagerie est accessible et utilisée seulement par le médecin et les infirmeries.

Tous les autres échanges se font par messagerie classique (Microsoft365) où les communications sont chiffrées (TLS).

Commenté [BB4]: Modif : De local à MS365

10. DCP - Sécurité physique et environnementale

10.1. Périmètre de sécurité physique

La salle serveur a un accès sécurisé par code (seul le personnel habilité en a connaissance).
La baie disque est également équipé d'un antivol (câble acier).

11. DCP - Sécurité liée à l'exploitation

11.1. Mesures contre les logiciels malveillants

Tous les ordinateurs et serveurs sont équipées d'un antivirus professionnel avec une console centralisée. Les mises à jour sont automatiques même pour les ordinateurs en mobilité.

11.2. Sauvegarde des informations

Les données sont sauvegardées tous les jours sur un support déporté (+de 300m) de la salle serveur.
Les sauvegardes sont glissantes avec une durée de conservation entre 15 et 60 jours selon leur nature.
Les tests de sauvegarde sont réalisés tous les 6 mois.
Document : Procédures IT

Commenté [BB5]: A mettre en place

Les dossiers du personnel sont archivés dans une GED et sur demande, au-delà des délais légaux, le dossier du salarié pourra être effacés.

11.3. Journalisation des événements

Tous les événements (détection de virus, sauvegarde non conforme, disque HS…) sont notifiés automatiquement au service informatique.
Le pare-feu enregistre les connexions à internet sur une période de 6 mois glissants.

11.4. Gestion des vulnérabilités techniques

Tous les équipements et logiciels sont mis à jour régulièrement par le service informatique.
Pour les ordinateurs et serveurs, une console d'administration (WSUS) permet de suivre le niveau de mise à jour des postes.

12. DCP - Sécurité des Communications

12.1. Contrôle des réseaux

Tous les éléments actifs du réseau sont sécurisés par mot de passe.
L'accès Wifi sur le réseau professionnel est en WAP2 entreprise avec une authentification par un serveur RADIUS.
L'accès WIFI pour le public est sécurisé en WAP2 avec mot de passe, fourni par le service informatique selon les besoins.
Les accès extérieurs (VPN) sont gérés par un pare-feu depuis un point unique.
Toutes les connexions à ce pare-feu se voient appliquées un filtrage de sécurité (IPS, antivirus) et de contenu (Filtrage url).

13. DCP - Relation avec les fournisseurs

13.1. Chaine d'approvisionnement informatique.

Concernant les serveurs, le prestataire fourni et prépare le matériel dans son atelier, les logiciels et les données sont installés dans nos locaux.

14. DCP - Gestion des incidents liés à la sécurité de l'information

14.1. Recueil de preuves

Lors d'un incident de sécurité, une analyse est réalisée avec le prestataire informatique pour connaitre les données impactées, si cela concerne des DCP, la CNIL en sera avertie sous 48h.

15. DCP - Gestion de la continuité de l'activité

15.1. Organisation de la continuité de la sécurité de l'information

Les procédures de PRA (plan de reprise d'activité) ont été établies selon un certain nombre de scénaris.

Elles sont disponibles dans un classeur dans le bureau IT, sur un site web interne (https://it.larnay-sagesse.fr) et également chez le prestataire VIENNEDOC.