Axes de la Politique de Sécurité des Systèmes d'Information

Synasens
Avancer ensemble

OBJECTIF

Assurer la confidentialité, l'intégrité, la disponibilité et la traçabilité des informations de chaque établissement, notre priorité absolue est la sécurité et la continuité de prise en charge des patients

CHAMP D'APPLICATION

Cette politique s'applique à :

- Tous les personnels, stagiaires, bénévoles et visiteurs
- Tous les prestataires externes et sous-traitants ayant accès au système d'information (SI).
- Toutes les données (santé, administrative, RH...)
- Tous les équipements informatiques

GOUVERNANCE ET RESPONSABILITE

La Direction valide la PSSI, alloue les ressources .
Le Délégué à la Protection des Données (DPO) garantit la conformité au RGPD et est point de contact avec la CNIL.
Le Responsable de la sécurité du Système d'information : Met en œuvre la PSSI, supervise la sécurité opérationnelle et cogère les incidents
Chaque utilisateur est responsable du respect de cette politique et doit signaler toute anomalie

PROTECTION DES DONNEES

Hébergement : Toutes les données de santé en mode SAAS doivent être hébergées chez un Hébergeur de Données de Santé (HDS) certifié. Le stockage sur le poste de travail est à proscrire
Classification : Le dossier du résident est au niveau le plus élevé.
Anonymisation : Anonymisation en cas de données pour la statistiques ou la recherche,
Transferts : Tout partage de données de santé se fait via des canaux sécurisés
Archivage : Respect des durées légales d'archivages

SECURITE DES ACCES ET DES POSTES

Authentification : Identifiant nominatif unique pour les acces. Renforcement avec Outil MFA (e-cps) pour les données de soins et l'acces à distance
Habilitation : Matrice des habilitations selon le principe du moindre privilège;
Revue régulière des droits avec révocation partielle ou totale selon absence ou départ
Poste de travail : Verrouillage des sessions, chiffrage des postes de travail, mise à jour des antivirus et système d'exploitation en temps maitrisé, interdiction d'installation de nouveaux outils sans validation de la direction

SENSIBILISATION ET FORMATION

Sensibilisation et formation obligatoire : Lors de la période d'intégration avec validation de Modules MOOC ANS
Rappel annuel : Session de sensibilisation annuelle pour l'ensemble des salariés
Outils sensibilisation flash : Diffusion des communication (affiches) de l'Etat

LES 6 AXES DE LA PSSI

INCIDENTS ET CONTINUITE

Segmentation en 3 Réseaux : Critique/ Interne/ Invités
Sauvegardes en 3 copies chiffrées, sur 2 supports différents, dont 1 hors site/déconnectée avec tests (restauration) au minimum trimestriellement.
Télétravail : L'accès à distance au SI doit exclusivement se faire via un VPN (Réseau Privé Virtuel) sécurisé avec MFA.

GESTION DES RISQUES NOUVEAUX

Maitrise de l'IA : Utilisation d'outil d'IA Souveraines après validation de la direction, du RSSI et du DPO
Protection de l'IA : Politique de la contre-vérification renforcée (Hameçonnage, Fraude vocale..)
Interdiction d'intégration de données nominatives dans les outils d'IA
I**ntegration des DMN :** Validation RSSI

SECURITE DES INFRASTRUCTURES ET RESEAUX

- **Incident ou suspicion :** Signalement immédiat via AGEVAL et application de la fiche réflexe
- **Plan de Continuité d'Activité :** Formalisé et testé annuellement
- **Notifications :** En cas de violation de données avérée, le DPO doit notifier la CNIL (sous 72h) et l'ARS.
- **Suivi :** L'infogérance fait un bilan annuel avec plan d'actions