Modèle annexe Sécurité au contrat informatique

**Sommaire**

[**1. Confidentialité des données 3**](#_8xtwp8odgfs6)

[**2. Intégrité des données 3**](#_wvht4zz1l68j)

[**3. Disponibilité des services 4**](#_7s7pxhu6rsn0)

[**4. Sécurité des accès 4**](#_sdqpvjuj2mfo)

[**5. Sécurité du matériel et des logiciels 4**](#_q8xeifyg9nec)

[**6. Gestion des incidents de sécurité 4**](#_gor249jkznot)

[**7. Audit et contrôle 4**](#_x1q8vczhno4w)

[**8. Responsabilités 5**](#_dd8gp9niaeje)

[**9. Références 5**](#_62l5ocawkknw)

[**10. Entrée en vigueur 5**](#_2p2ijmsqmw8p)

# 

Annexe de sécurité au contrat informatique

Préambule

La présente annexe a pour objectif de définir les exigences de sécurité minimales que le prestataire informatique doit respecter dans le cadre du contrat [Nom du contrat] conclu avec l'établissement [Nom de l'établissement].

# 1. Confidentialité des données

* **Protection des données personnelles et de santé** : le prestataire s'engage à respecter les dispositions du Règlement Général sur la Protection des Données (RGPD) et les obligations relatives au secret professionnel concernant les données de santé.
* **Accès restreint** : seules les personnes habilitées par l'établissement et ayant besoin d'en connaître auront accès aux données. Le prestataire mettra en place un système de gestion des accès basé sur le principe du moindre privilège.
* **Chiffrement des données** : les données sensibles seront chiffrées au repos et en transit, conformément aux recommandations de l'ANSSI.
* **Gestion des mots de passe** : le prestataire mettra en place une politique de gestion des mots de passe robuste, conformément aux recommandations présentes dans le guide “Recommandations relatives à l'authentification multifacteur et aux mots de passe” de l’ANSSI.

# 2. Intégrité des données

* **Mesures de prévention** : le prestataire mettra en place des mesures de prévention contre les modifications non autorisées des données, telles que des contrôles d'intégrité et des signatures électroniques.
* **Sauvegardes et restauration** : le prestataire réalisera des sauvegardes régulières des données selon le principe de sauvegarde 3-2-1 a minima et mettra en place une procédure de restauration en cas d'incident.
* **Tests de restauration de sauvegardes :** le prestataire réalisera des tests de restauration de sauvegardes régulièrement et au minimum de façon annuelle.
* **Plan de continuité et de reprise d'activité (PCRA)** : le prestataire élaborera et maintiendra un PCRA pour assurer la continuité des services en cas de sinistre ainsi que la reprise d’activité.

# 3. Disponibilité des services

* **Maintien du service** : le prestataire s'engage à maintenir le service informatique en conditions normales d'exploitation et à intervenir rapidement en cas d'incident.
* **Niveaux de service (SLA)** : le contrat précisera les niveaux de services appliqués pour garantir un certain niveau de disponibilité des services.

# 4. Sécurité des accès

* **Gestion des identités et des accès** : le prestataire mettra en place un système de gestion des identités et des accès pour contrôler l'accès aux ressources informatiques.
* **Authentification forte** : l'authentification forte sera exigée pour l'accès aux données sensibles et aux fonctions critiques.

# 5. Sécurité du matériel et des logiciels

* **Mises à jour** : le prestataire s'engage à maintenir les logiciels et les systèmes d'exploitation à jour avec les derniers correctifs de sécurité.
* **Protection contre les menaces** : le prestataire mettra en place des mesures de protection contre les virus, les logiciels malveillants et les intrusions.
* **Sécurité physique** : le prestataire assurera la sécurité physique des locaux techniques et du matériel informatique.

# 6. Gestion des incidents de sécurité

* **Procédure de signalement** : le prestataire mettra en place une procédure de signalement des incidents de sécurité et s'engage à informer l'établissement dans les plus brefs délais en cas de violation de données.
* **Collaboration** : le prestataire collaborera avec l'établissement pour résoudre les incidents de sécurité et mettre en place les mesures correctives nécessaires.

# 7. Audit et contrôle

* **Droit d'audit** : l'établissement se réserve le droit de réaliser des audits de sécurité pour vérifier le respect des exigences de la présente annexe.
* **Correction des écarts :** les écarts constatés lors d'un audit doivent faire l'objet de mesures correctives planifiées par le prestataire en accord avec l’établissement. Le prestataire fournira un plan d'action.
* **Communication des résultats** : le prestataire communiquera à l'établissement les résultats des audits et les actions correctives mises en place.

# 8. Responsabilités

* **Répartition des responsabilités** : le contrat précisera la répartition des responsabilités en matière de sécurité entre l'établissement et le prestataire.
* **Clauses de responsabilité** : le contrat inclura des clauses de responsabilité en cas de manquement aux obligations de sécurité.

# 9. Références

Le prestataire s'engage à respecter les référentiels et guides de bonnes pratiques en matière de sécurité des systèmes d'information, notamment le RGPD, la PGSSI-S et les recommandations spécifiques au secteur médico-social.

# 10. Entrée en vigueur

La présente annexe entre en vigueur à la date de signature du contrat [Nom du contrat].

**Signature :**

|  |  |
| --- | --- |
| [Nom et signature du représentant de l'établissement] | [Nom et signature du représentant du prestataire] |
|  |  |