

Annexe : clauses pour la sécurité du Système d'information (SI)

1. Objet de la clause de sécurité :

Cette clause a pour objet de définir les obligations du prestataire en matière de sécurité du système d'information (SI) dans le cadre de l'exécution du marché.

2. Obligations générales de sécurité :

Le prestataire s'engage à mettre en œuvre toutes les mesures techniques et organisationnelles appropriées pour garantir la sécurité du SI, y compris :

- La protection contre les accès non autorisés.
- La prévention des atteintes à la confidentialité, à l'intégrité et à la disponibilité des données.
- L'application de politiques de sécurité conformes aux normes en vigueur.

3. Gestion des accès

Le prestataire devra mettre en place un système de gestion des accès, garantissant que seules les personnes autorisées peuvent accéder aux données et aux systèmes.

Cette gestion devra inclure :

- L'attribution de droits d'accès basés sur le principe du moindre privilège.
- La mise en place d'authentifications fortes.
- L'enregistrement et la surveillance des accès aux systèmes et aux données.

4. Formation et sensibilisation du personnel

Le prestataire devra former et sensibiliser son personnel aux enjeux de la sécurité des systèmes d'information.

Cela inclut la formation sur :

- Les bonnes pratiques en matière de sécurité.
- Les procédures à suivre en cas de suspicion d'incident de sécurité.
- Les obligations de confidentialité liées au traitement des données. »

5. Surveillance et audits

Le prestataire s'engage à mettre en place des mécanismes de surveillance régulière de la sécurité du SI. Il devra permettre au responsable du traitement de réaliser des audits de sécurité sur demande, afin de vérifier la conformité aux obligations de sécurité prévues dans le contrat. Les résultats de ces audits devront être partagés avec le responsable du traitement.

6. Gestion des incidents de sécurité

En cas d'incident de sécurité affectant le SI, le prestataire devra :

- Informer le responsable du traitement dans les 24 heures suivant la détection de l'incident.
- Fournir un rapport détaillant la nature de l'incident, les données concernées, les conséquences potentielles et les mesures prises pour remédier à la situation.
- Collaborer avec le responsable du traitement pour évaluer l'incident et mettre en place des mesures correctives.

7. Sauvegarde et récupération des données

Le prestataire s'engage à mettre en œuvre des procédures de sauvegarde régulières des données et à garantir que des mesures de récupération soient en place en cas de perte de données ou de défaillance du système.

Les procédures de sauvegarde devront inclure :

- La fréquence des sauvegardes.

- Le stockage sécurisé des sauvegardes.
- Des tests réguliers de la restauration des données.

8. Transfert de données et sécurité

Toute transmission de données à caractère personnel ou d'informations sensibles devra être effectuée de manière sécurisée. Le prestataire doit s'assurer que les protocoles de transfert (par exemple, cryptage) sont en place pour protéger les données lors de leur transfert, que ce soit au sein du SI ou entre le SI et des tiers.

9. Responsabilité et indemnisation

En cas de manquement aux obligations de sécurité stipulées dans le contrat, le prestataire sera responsable des dommages directs causés au responsable du traitement et s'engage à indemniser ce dernier pour toute perte ou préjudice résultant de cette violation.