

## **Annexe 1 : Sécurité informatique**

Le Titulaire doit être en mesure de présenter un plan d'assurance sécurité (PAS) permettant d'évaluer la couverture des exigences de sécurité. Il est recommandé au Titulaire d'utiliser le modèle présent sur le site de l'ANSSI.

S'il choisit de ne pas l'utiliser, il doit fournir un document répondant à l'ensemble des exigences prévues dans ce modèle.

### **Mise à jour**

Le Titulaire doit se conformer aux recommandations de l'ANSSI pour être à jour sur son système d'information et être en conformité aux exigences du ministère de l'intérieur.

### **Gouvernance**

La politique de sécurité des systèmes d'information et de son évolution doit être fourni à la personne publique.

Le Titulaire s'engage à respecter les obligations suivantes et à les faire respecter par son personnel :

- Ne prendre aucune copie des documents et supports d'informations qui lui sont confiés, à l'exception de celles nécessaires à l'exécution de la présente prestation prévue au contrat avec l'accord préalable de l'administration ;
- Ne pas utiliser les documents et informations traités à des fins autres que celles spécifiées au présent contrat ;
- Ne pas divulguer ces documents ou informations à d'autres personnes, qu'il s'agisse de personnes privées ou publiques, physiques ou morales ;
- Prendre toutes mesures permettant d'éviter toute utilisation détournée ou frauduleuse des fichiers informatiques en cours d'exécution du contrat.

Le Titulaire s'engage à prendre les mesures nécessaires pour assurer la conservation et l'intégrité des documents et informations traités pendant la durée de l'accord-cadre.

Il s'engage à utiliser un système de sauvegarde des données et de continuité de service.

### **Intégrité des échanges**

Les flux entre le Titulaire et la personne publique doivent être cryptés selon les règles du Référentiel Général de Sécurité de l'ANSSI.

L'ensemble de la documentation expliquant l'algorithme retenu, les dispositifs de contrôle de l'intégrité des données, les restaurations de données ainsi que les procédures d'exploitation et de protection du système doit être fourni.

## **Données**

L'hébergement des données doit se faire de manière transparente en fournissant la liste des lieux de stockage, leur sécurisation, les sites de secours.

Ces informations doivent apparaître dans le plan d'assurance sécurité. La documentation des Procédures d'Exploitation Sécurité doit être fournie et disponible à la demande.

La personne publique peut mener dans un délai bref toute vérification sur site nécessaire de sécurité de stockage.

En cas d'hébergement cloud, celui-ci doit avoir le niveau de garanties correspondant à la certification SECNUMCLOUD.

## **Données sensibles**

S'il devait y avoir un échange de données sensibles, elles devront être protégées selon l'instruction interministérielle 901 relative à la protection des systèmes d'information sensibles.

## **Antivirus**

Une politique anti virale doit être mise en place, l'ensemble de la documentation doit être fournie.

## **Incidents**

L'ensemble des moyens doit être mis en œuvre pour journaliser, superviser et détecter les éventuels incidents de sécurité. Le cloisonnement entre les moyens (humains et techniques) de détection et ceux du fonctionnement commun doit être respecté. Les journaux doivent être compréhensibles et stockés sur une période de six mois.

Aucune donnée portant mention de l'affectation professionnelle ne pourra être demandée par le titulaire aux bénéficiaires.