ANNEXE N°7

CLAUSES DE SECURITE VILLE DE MARSEILLE

Sécurité

Le TITULAIRE s'engage à prendre toutes précautions utiles afin de préserver la sécurité des informations et notamment d'empêcher qu'elles ne soient déformées, endommagées ou communiquées à des personnes non autorisées.

Le TITULAIRE s'engage à respecter les instructions données par la COLLECTIVITE en matière de sécurité et de confidentialité des données transmises et des traitements réalisés dès lors que ces instructions sont de nature à apporter des garanties effectives et proportionnées.

Sécurisation des Serveurs

Les serveurs de développement et d'intégration mis en œuvre

- sont virtualisés
- ont des mots de passe complexes connus seulement de l'équipe projet
- sont sauvegardés régulièrement
- n'hébergent que les versions anonymisées des bases de données le nécessitant
- ont des antivirus à jour
- ont les mises à jour de sécurité activées

Les environnements de validation d'aptitude et de production sont soumis aux mêmes règles, excepté le fait que ce sont les seuls environnements aptes à héberger des données non anonymisées.

Le TITULAIRE, lorsque les données sont hébergées sous sa responsabilité, devra veiller à ce que seules des données anonymisées soient utilisées dans les environnements de tests et de développements.

Sécurisation des postes de travail

Les postes de travail du TITULAIRE au sein de la collectivité sont installés et gérés par la DGANSI. Ils sont sécurisés suivant les règles internes de sécurité des postes clients. Chaque poste est équipé d'une solution antivirale et les mises à jour des patchs correctifs sont faites de façon automatique.

Le TITULAIRE devra s'assurer que ses postes de travail sont protégés et ne permettent pas une compromission du SI de la COLLECTIVITE par son intermédiaire.

Sécurisation des réseaux

Les flux internes et à destination d'Internet sont gérés au travers d'équipements et de solutions habituels (firewalls, proxys, sondes réseau, …).

Tout flux considéré comme sensible doit être sécurisé en utilisant un protocole adéquat (https, ...).

Sécurisation des données

Les documents considérés comme sensibles seront stockés sur l'espace de gestion électronique des documents de la COLLECTIVITE.

Aucune donnée numérique à caractère personnel ne sera stocké dans les locaux du TITULAIRE.

Échanges de données et bases de données

Les bases de données sensibles sont installées et utilisés chez le TITULAIRE uniquement dans leur version anonymisée.

Les mots de passe permettant d'accéder à ces bases sont connues uniquement des équipes projet et sont d'un niveau de complexité suffisant (10 caractères minimum contenant une combinaison d'au moins 3 de ces critères : majuscules, minuscules, numériques et caractères spéciaux) et ne pas être vulnérables aux attaques par dictionnaire

Sécurité des développements applicatifs

Le TITULAIRE est tenu d'assurer la sécurité des développements conformément à l'état de l'art dans chacune des technologies mises en œuvre. Les règles applicables sont les suivantes (liste non exhaustive) :

- environnement applicatif maintenu en tenant compte des recommandations d'application de correctifs par les éditeurs ;
- contrôle rigoureux des entrées utilisateurs ;
- sécurisation des accès aux fonctions d'administration ;
- installation du minimum de fonctions nécessaires lors de l'installation ;
- principe du moindre privilège ;
- utilisation de mots de passe fixés dans le code interdite ;
- mise en œuvre d'une gestion efficace des erreurs.