Cahier d'exigences techniques et fonctionnelles traitant de la Sécurité du SI et de la CNIL

Objet : Exigences Sécurité du SI et de la CNIL

Version : 1.3

Ce document et les documents joints en annexe, sont exclusivement réservés à usage interne à la Ville de Marseille et aux destinataires visés. Toute diffusion, divulgation ou transmission à toute autre personne ou organisme extérieur est strictement prohibée, sauf autorisation préalable expresse écrite.

Table des matières

1. Les Contraintes Réglementaires....3
1.1 Le RGS....3
1.2 La CNIL :....3
1.3 Le Code du Patrimoine....3
2. Les clauses générales de confidentialité....4
3. Les contraintes techniques de sécurité....4
3.1 Simplicité, traçabilité et gestion de version du code....4
3.2 Validation des données en entrées....5
3.3 Validation des données en sortie....5
3.4 Normalisation des messages d'erreurs....5
3.5 Authentification et autorisations....5
3.6 Gestion des sessions et des cookies....6
4. Les Livrables....6
5. Les Contrôles....6
6. phase de Réversibilité....6

Ce document et les documents joints en annexe, sont exclusivement réservés à usage interne à la Ville de Marseille et aux destinataires visés. Toute diffusion, divulgation ou transmission à toute autre personne ou organisme extérieur est strictement prohibée, sauf autorisation préalable expresse écrite.

1. LES CONTRAINTES RÉGLEMENTAIRES

1.1 Le RGS

Le décret **RGS** (*Référentiel Général de Sécurité*), pris en application de l'**ordonnance n° 2005-1516 du 8 Décembre 2005**, dite « ordonnance télé-services » et en vigueur depuis le 19 Mai 2013, s'impose à la totalité des systèmes d'information, et nous oblige à garantir la sécurité des échanges électroniques entre le citoyen et l'administration, entre deux administrations ou entre une administration et ses partenaires. Ces échanges électroniques sont également nommés **télé-services**.

Ainsi, tous les télé-services créés dans le cadre de ce marché, devront être **homologués** par la Ville de Marseille.
Cette homologation implique une évaluation du niveau de criticité du télé-service et d'une analyse de risque adaptée.

1.2 La CNIL :

Les dispositions de la **loi n°78-17 du 6 janvier 1978**, relative à l'informatique, aux fichiers et aux libertés modifiée par la loi n°2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel sont applicables dans le cadre de ce marché.

Il est notamment nécessaire de confirmer le respect de l'article 68 de la Loi Informatique et Libertés, qui précise que **les transferts en dehors de l'Union européenne sont interdits,** sauf exceptions, prévues par l'article 69 de la loi.

1.3 Le Code du Patrimoine

Les documents et données produits ou reçus par la Ville de Marseille constituent des archives publiques.
Or, la **loi n°2015-195** promulguée le 20 février 2015 et modifiant l'**article L.111-1 du code du patrimoine**, qualifie les archives publiques de "trésors nationaux"et ne peuvent donc sortir du territoire douanier qu'après autorisation du Service inter-ministériel des Archives de France (SIAF) et seulement dans certains cas précis.

Ce document et les documents joints en annexe, sont exclusivement réservés à usage interne à la Ville de Marseille et aux destinataires visés. Toute diffusion, divulgation ou transmission à toute autre personne ou organisme extérieur est strictement prohibée, sauf autorisation préalable expresse écrite.

2. LES CLAUSES GÉNÉRALES DE CONFIDENTIALITÉ

Les supports informatiques physiques et documents fournis par la **Ville de Marseille** à la société prestataire restent la propriété de la **Ville de Marseille**.

Les données contenues dans ces supports et documents sont **strictement couvertes par le secret professionnel** (article 226-13 du code pénal), il en va de même pour toutes les données dont la société prestataire prendra connaissance à l'occasion de l'exécution de ce marché.

La société prestataire s'engage donc 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 prestation prévue dans ce marché, l'accord préalable du responsable du fichier est nécessaire ;
- ne pas utiliser les documents et informations traités à des fins autres que celles spécifiées dans ce marché ;
- 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 marché ;
- prendre toutes mesures de sécurité, notamment matérielle, pour assurer la conservation et l'intégrité des documents et informations traités pendant la durée du marché ;
- échanger des informations personnelles, sensibles ou des authentifications/identifications uniquement de manière chiffrée ;
- en fin de marché à procéder à la mise à disposition de toutes les données appartenant à la Ville de Marseille ;
- et en fin de marché à procéder à la destruction de tous fichiers manuels ou informatisés stockant les informations saisies.

3. LES CONTRAINTES TECHNIQUES DE SÉCURITÉ

Les bonnes pratiques édictées par l'OWASP (Open Web Application Security Projet https://www.owasp.org/) sont la référence à respecter, selon laquelle la **Ville de Marseille** se réserve le droit d'auditer les solutions déployées sur son système d'information.

La **Ville de Marseille** exige, à minima, la mise en place des mesures techniques de sécurité suivantes :

3.1 Simplicité, traçabilité et gestion de version du code

Un code simple est toujours plus facile à maintenir et à sécuriser qu'un code complexe. La complexité est l'ennemie de la sécurité et de la capacité à évoluer.
Par exemple, il est inutile de ré-inventer des algorithmes de chiffrement alors que des standards, tels

Ce document et les documents joints en annexe, sont exclusivement réservés à usage interne à la Ville de Marseille et aux destinataires visés. Toute diffusion, divulgation ou transmission à toute autre personne ou organisme extérieur est strictement prohibée, sauf autorisation préalable expresse écrite.

que AES, existent, de même pour l'échange de clefs avec Diffie-Hellman.

3.2 Validation des données en entrées

Toutes les données venant de l'extérieur d'une application et plus généralement d'une fonction doivent être normalisées, analysées et épurées. C'est à dire qu'aucune confiance ne doit être faite par la couche présentation et applicative sur le contenu et la bonne validité des données lui étant envoyées.

Par exemple :

- un champ recevant un mail ne devra que contenir des caractères valides et respecter la RFC 53221 (taille, casse …),
- un nombre ne peut être constitué que des caractères 0 à 9 et du signe ',' et peut être précédé du signe + ou -. Il sera en plus borné (longueur et valeur).

Toute donnée non conforme à l'attendu, devra être rejetée avec un message d'erreur conforme et explicite ou simplement non pris en compte. Il ne doit pas faire l'objet d'une évaluation et/ou consommation par l'application.

3.3 Validation des données en sortie

De même que précédemment, les données envoyées à l'utilisateur doivent être analysées et encodées pour quelles ne puissent pas être interprétées par le navigateur comme du code HTML, javascript ou autre lorsque cela n'est pas nécessaire.

3.4 Normalisation des messages d'erreurs

Les messages d'erreurs ne doivent pas donner d'information autre que le fait qu'il y a eu une erreur. En particulier les messages d'erreur de débogage ne doivent jamais être visibles et accessibles par les utilisateurs. Ils doivent respecter la règle : « toute information qui n'est pas utile pour le quidam, ne doit pas être donnée ». Les messages de débogage sont envoyés vers un fichier et non vers l'utilisateur.

3.5 Authentification et autorisations

Si des mécanismes d'authentification forte n'ont pas été mis en œuvre dans une application, un attaquant peut accéder à ses contenus sensibles sans avoir à s'authentifier.
Il faut instaurer des règles simples telles que :

- appliquer la politique de mot de passe définie par la Ville de Marseille :Le mot de passe doit contenir au moins 10 caractères (12 caractères maxima) avec au moins un chiffre, au moins une minuscule et au moins une majuscule.
- mettre en œuvre un délai après un échec d'authentification, afin d'éviter les attaques par force brute,
- ne pas utiliser des CAPTCHA trop simples,
- protéger les accréditations lors du transit :
- chiffrer les données entre le client et le serveur,

Ce document et les documents joints en annexe, sont exclusivement réservés à usage interne à la Ville de Marseille et aux destinataires visés. Toute diffusion, divulgation ou transmission à toute autre personne ou organisme extérieur est strictement prohibée, sauf autorisation préalable expresse écrite.

- ne pas envoyer le mot de passe au serveur mais une empreinte du mot de passe (MD5, SHA1 …),
- définir des rôles et des niveau d'accréditations dans les applications.
- Désactiver la possibilité de stocker le mot de passe dans la base locale du navigateur.

3.6 Gestion des sessions et des cookies

Les sessions et le contenu des cookies, ont des identifiants non prédictibles et doivent intégrer au minimum l'adresse IP du client, un aléa, un secret et un paramètre dépendant de la date et de l'heure. Ceci afin de permettre une impossibilité de rejeux de l'identification tout en gardant une validité dans le temps. La base de temps ne sera pas celle du client, mais uniquement celle du serveur.

4. LES LIVRABLES

Tous les livrables demandés ci-dessous, dans le cadre de ce marché, doivent répondre aux contraintes de sécurité exigées par la **Ville de Marseille :**

- La prise en compte des besoins et enjeux de sécurité ;
- Les modalités d'hébergement ainsi que la politique de sauvegarde ;
- Les résultats des tests d'intrusion sur le système d'information s'ils ont été faits ;
- Le PAS (Plan d'Assurance Sécurité) s'il existe, sinon, tout document (PSSI, charte, étude, ...) prouvant la capacité à assurer à la Ville de Marseille un niveau de sécurité suffisant.

5. LES CONTRÔLES

La Ville de Marseille se réserve le droit de procéder à toute vérification qui lui paraîtrait utile pour constater le respect des obligations réglementaires et techniques de sécurité par la société prestataire, notamment par la réalisation d'audits ponctuels.

En cas de non-respect des dispositions précitées, la responsabilité du titulaire peut également être engagée sur la base des dispositions des articles 226-5 et 226-17 du nouveau code pénal.

La Ville de Marseille pourra prononcer la résiliation du marché, sans indemnisation du titulaire, en cas de violation du secret professionnel ou de non-respect des dispositions précitées.

6. PHASE DE RÉVERSIBILITÉ

Au terme du marché, le prestataire s'engage à faciliter la réversibilité selon les modalités choisies par la **Ville de Marseille** et à fournir toutes les informations et prestations utiles à sa mise en œuvre.

La fourniture de toutes les **informations relatives à l'exécution du marché**, la **documentation** constituée durant la prestation, sous forme électronique mise à jour, ainsi que le **transfert de connaissance** sont inclus dans le présent marché.

Ce document et les documents joints en annexe, sont exclusivement réservés à usage interne à la Ville de Marseille et aux destinataires visés. Toute diffusion, divulgation ou transmission à toute autre personne ou organisme extérieur est strictement prohibée, sauf autorisation préalable expresse écrite.

Ce transfert se fera directement aux équipes de la Ville de Marseille.

Ce document et les documents joints en annexe, sont exclusivement réservés à usage interne à la Ville de Marseille et aux destinataires visés. Toute diffusion, divulgation ou transmission à toute autre personne ou organisme extérieur est strictement prohibée, sauf autorisation préalable expresse écrite.