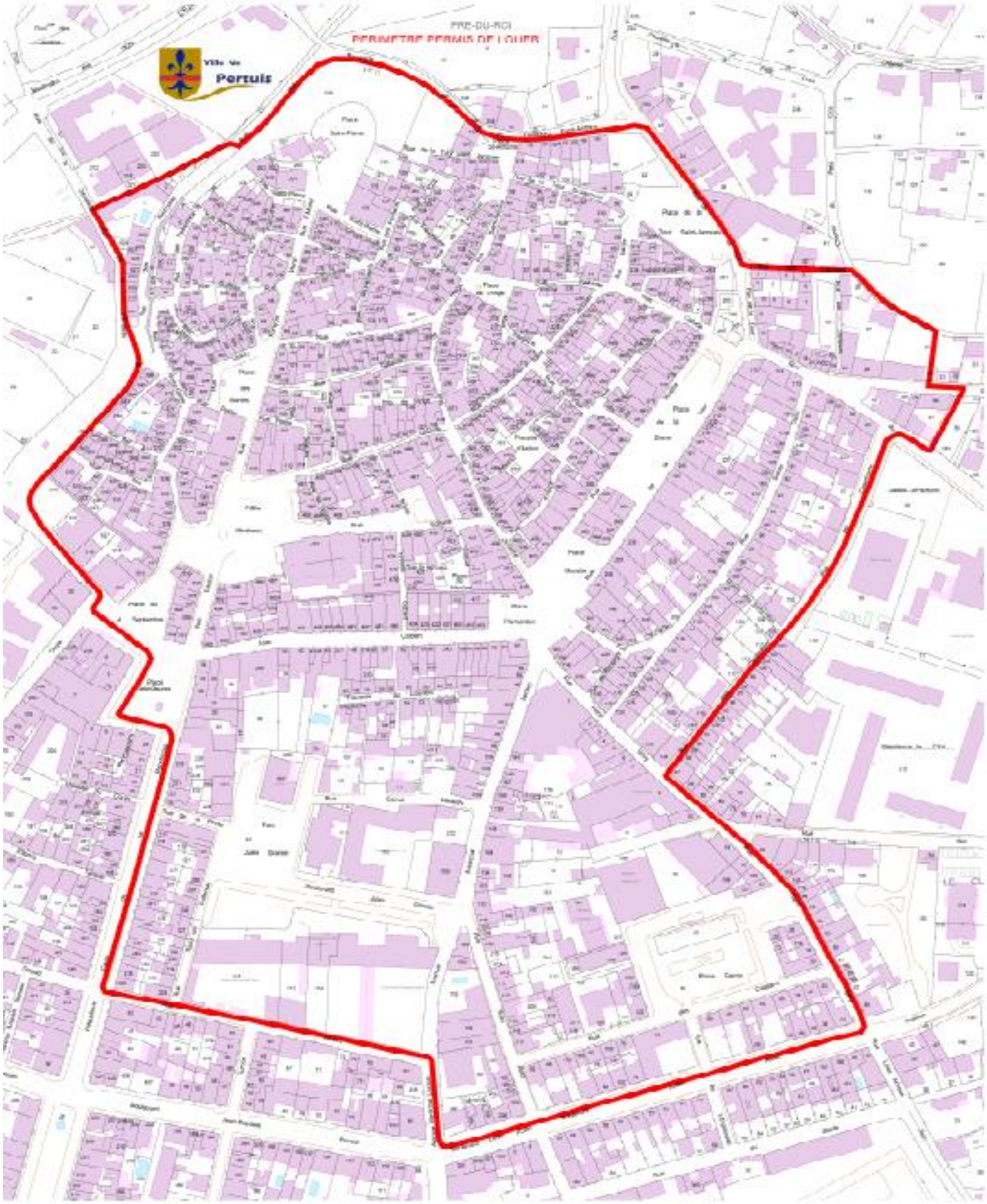
Annexe n°I : Périmètre



Reçu au Contrôle de légalité le 03 juillet 2024

Annexe n°II : Indicateurs quantitatifs et qualitatifs

Les données et informations quantitatives et qualitatives suivantes seront à renseigner sous réserve de la disponibilité de la donnée et des partenariats établis.

Indicateurs de suivi :

Pour évaluer le respect des dispositions réglementaires par les propriétaires et la typologie des logements pour lesquels il est demandé :

- Nombre de demandes d'autorisation de mise en location par mois,

- Typologie des logements pour lesquels l'autorisation est demandée (maison / immeuble, copropriété / mono-propriété / nombre de pièces).

Pour évaluer le caractère préventif du dispositif :

- Nombre de permis de louer ayant entraîné une procédure administrative,

- Nombre d'autorisations / refus / accords sous réserve donnés,

- Si refus, nombre de dossiers transférés à la CAF pour suivi des adresses,

- Nombre de logements dans lesquels des travaux ont été réalisés,

- Nombre de locations constatées sans APML,

- Nombre de demandes hors périmètres,

- Nombre de refus de visite par les propriétaires,

- Description de la manière dont on contrôle l'effectivité des travaux,

- Type de travaux prescrits.

-**Pour évaluer la dimension coercitive du dispositif :**

- Articulation du dispositif avec les arrêtés de péril et de salubrité,

- Nombre de sanctions

- Montant des amendes.

Pour évaluer les moyens du service dans la mise en œuvre du « permis de louer » :

- Nombre d'agents voire de services mobilisés (préciser lesquels),

- Nombre de visites effectuées,

- Temps moyen par dossier,

- Description d'autres moyens employés.

Reçu au Contrôle de légalité le 03 juillet 2024

Indicateurs optionnels :

Pour évaluer la qualité des partenariats dans le cadre de la mise en œuvre du « permis de louer » :

- Fréquence des temps d'échange avec les partenaires,

- Communication mise en place autour du dispositif envers les propriétaires et autres acteurs,

· (Agences immobilières, notaires...),

- Supports de communication utilisés,

- Points forts/ faibles / axes d'amélioration,

- Indication des éventuelles modalités d'amélioration des relations avec l'ensemble des partenaires.

Reçu au Contrôle de légalité le 03 juillet 2024

Annexe n°III : « Sécurité et Traitement des données » & « Plan d'Assurance Sécurité

ANNEXE SÉCURITÉ ET PROTECTION DES DONNÉES

Adresse(s) mail de contact pour les notifications relatives à la protection des données (articles 5.3 à 5.5) :

- **.....@ampmetropole.fr**
- **.....@ampmetropole.fr**

Reçu au Contrôle de légalité le 03 juillet 2024

Contenu

1. Objet 6
2. Organisation de la sécurité 6
3. Cycle de vie des mesures de sécurité 6
4. Auditabilité 7
5. Obligations de la commune 7
   5.1. Obligations générales 7
   5.2. Sous-traitance 8
   5.3. Droit d'information des personnes concernées 8
   5.4. Exercice des droits des personnes 8
   5.5. Notification des violations de données à caractère personnel 9
   5.6. Aide de la commune dans le cadre du respect par la Métropole de ses obligations 10
   5.7. Mesures de sécurité 10
   5.8. Sort des données 10
   5.9. Délégué à la protection des données 10
   5.10. Registre des catégories d'activités de traitement 10
6. Management de la SSI de la commune 11
   6.1. Sécurité des ressources humaines 11
   6.2. Sécurité des infrastructures 11
      6.2.1. Cartographie du service 11
      6.2.2. Accès logiques 12
      6.2.3. Cloisonnement 12
      6.2.4. Sécurité des serveurs 12
      6.2.5. Sécurité des postes 12
      6.2.6. Supervision de la sécurité 12

Reçu au Contrôle de légalité le 03 juillet 2024

1. Objet

Dans le cadre de leurs relations contractuelles, les parties s'engagent à respecter la réglementation en vigueur applicable au traitement en matière de sécurité des systèmes d'information et de protection des données à caractère personnel et, en particulier, le règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 applicable à compter du 25 mai 2018 (ci-après, « le règlement européen sur la protection des données »).

Le présent document décrit les dispositions que la commune doit mettre en œuvre pour répondre aux exigences de sécurité de la Métropole Aix-Marseille-Provence.

Il est complété par le document PAS – Plan d'assurance sécurité et qui précise l'organisation qui sera mise en place, la méthodologie à suivre pour gérer la sécurité du projet et les mesures techniques et organisationnelles qui seront mises en œuvre par la commune.

2. Organisation de la sécurité

La Métropole désigne un interlocuteur responsable de la sécurité du projet. Cet interlocuteur unique sera rattaché directement au directeur de projet. Cet interlocuteur sera responsable de l'ensemble de la sécurité du projet pour la Métropole, tant sur les aspects sécurité du système d'information cible que sur les aspects sécurité des interfaces avec la commune.

Le responsable de la sécurité désigné par la Métropole a pour mission de faciliter les relations entre les différents intervenants, et de mettre à disposition de la maîtrise d'œuvre l'ensemble des documents nécessaires au bon déroulement du projet sécurité lié à l'opération d'externalisation : politique de sécurité interne de la Métropole, documentation technique du système (documents d'architecture, documents d'exploitation, etc.), spécifications, etc.

Il a également pour mission de s'assurer de la prise en compte globale de la sécurité, par la maîtrise d'ouvrage et la maîtrise d'œuvre.

Il décide de la conduite à tenir selon le résultat des audits, des incidents ou des conseils remontés par la commune d'externalisation.

Il valide l'ensemble des actions réalisées au titre de la gestion de la sécurité du projet.

En tant que maître d'œuvre, la commune désigne un interlocuteur responsable de la sécurité, pilotant l'ensemble de la sécurité du projet : sécurité des développements, sécurité du système d'information cible et intégration des composants sécurité.

Elle conseille la Métropole dans son approche de la sécurité du projet, selon les audits, les incidents perçus sur le système ou les évolutions du contexte opérationnel.

3. Cycle de vie des mesures de sécurité

La commune est responsable de l'organisation de sa sécurité pour répondre aux exigences de la Métropole pendant toute la durée de la convention.

Voici une liste (non exhaustive) des situations susceptibles d'entraîner une modification de l'organisation de la sécurité de la commune :

- évolution du système d'information (configuration logicielle ou matérielle) ;
- évolution de l'environnement du système d'information (locaux, personnels, procédures, etc.) ;
- évolution législative ou réglementaire ;

Reçu au Contrôle de légalité le 03 juillet 2024

- évolution du périmètre de l'opération.

En cas d'évolution, la commune vérifie si l'organisation de sa sécurité doit être modifiée. Si tel est le cas, elle propose une modification à la Métropole. Le cas échéant, cette modification est approuvée par avenant.

4. Auditabilité

La commune met à la disposition de la Métropole la documentation nécessaire pour démontrer le respect de toutes ses obligations et pour permettre la réalisation d'audits, y compris des inspections, par la Métropole ou un autre auditeur qu'elle a mandaté, et contribuer à ces audits.

Cet audit est réalisé sur l'ensemble du périmètre la convention et sur les services de la commune en lien avec ce contrat. Il peut prendre la forme d'audits documentaires, d'interviews et/ou de tests d'intrusion.

La commune doit se rendre disponible lors de ces audits et donner aux auditeurs l'accès à l'ensemble des éléments nécessaires.

Le rapport d'audit sera transmis à la commune par la Métropole.

La commune devra fournir dans le mois suivant la transmission du rapport d'audit un plan d'actions détaillé pour couvrir les non-conformités identifiées dans cet audit ou justifier de leur acceptation.

5. Obligations de la commune

5.1. Obligations générales

La commune est tenue à une obligation de conseil, de mise en garde et de recommandations en termes de sécurité et de mise à l'état de l'art. En particulier elle s'engage à informer la Métropole des risques d'une opération envisagée, des incidents éventuels ou potentiels, et de la mise en œuvre éventuelle d'actions correctives ou de prévention.

Outre le respect de ses obligations au titre de la convention, la commune informera préalablement la Métropole de toute opération susceptible de provoquer l'indisponibilité (ou une dégradation des performances) du système.

La commune est responsable du maintien en condition de sécurité du système pendant toute la durée des prestations.

Les mécanismes de sécurité mis en œuvre doivent évoluer conformément à l'état de l'art : la découverte de failles dans un algorithme, un protocole, une implémentation logicielle ou matérielle, ou encore l'évolution des techniques de cryptanalyse et des capacités d'attaque par force brute doivent être pris en compte.

La commune s'engage à :

- traiter les données uniquement pour la ou les seule(s) finalité(s) qui fait/font l'objet de la convention ;

- traiter les données conformément aux instructions de la Métropole ;

  Si la commune considère qu'une instruction constitue une violation du règlement européen sur la protection des données ou de toute autre disposition du droit de l'Union ou du droit des Etats membres relative à la protection des données, il en informe immédiatement la Métropole.

  En outre, si la commune est tenu de procéder à un transfert de données vers un pays tiers ou à une organisation internationale, en vertu du droit de l'Union ou du droit de l'Etat membre auquel il est soumis, il doit informer la Métropole de cette obligation juridique avant le traitement, sauf si le droit concerné interdit une telle information pour des motifs importants d'intérêt public ;

- garantir la confidentialité des données à caractère personnel traitées dans le cadre du présent marché ;

Reçu au Contrôle de légalité le 03 juillet 2024

- veiller à ce que les personnes autorisées à traiter les données à caractère personnel en vertu du présent marché :

  - s'engagent à respecter la confidentialité ou soient soumises à une obligation légale appropriée de confidentialité,

  - reçoivent la formation nécessaire en matière de protection des données à caractère personnel ;

- prendre en compte, s'agissant de ses outils, produits, applications ou services, les principes de protection des données dès la conception et de protection des données par défaut.

5.2. Sous-traitance

Le sous-traitant de la commune est tenu de respecter les obligations du présent contrat pour le compte et selon les instructions de la Métropole. Il appartient à la commune de s'assurer que le sous-traitant présente les mêmes garanties suffisantes quant à la mise en œuvre de mesures techniques et organisationnelles appropriées de manière à ce que le traitement réponde aux exigences du règlement européen sur la protection des données. Si le sous-traitant ne remplit pas ses obligations en matière de protection des données, la commune demeure pleinement responsable devant la Métropole de l'exécution par le sous-traitant de ses obligations.

La commune veille à la bonne prise en compte des principes et exigences de sécurité de la Métropole pour ses sous-traitants et notamment :

- Du respect des réglementation nationales et internationales :
  - Le RGPD
  - Le RGS
- De la mise en œuvre chez le sous-traitant d'une démarche SSI cohérente avec les exigences de la PSSIE
- De la présence chez son sous-traitant d'un responsable de la sécurité
- De l'existence d'un processus de gestion des alertes et incidents de sécurité informatique
- De l'existence d'un processus de gestion de la continuité d'activité

5.3. Droit d'information des personnes concernées

Dans le cas où la commune procède à la collecte des données pour le compte du responsable de traitement, la commune, au moment de la collecte des données, doit fournir aux personnes concernées par les opérations de traitement l'information relative aux traitements de données qu'elle réalise. La formulation et le format de l'information doit être convenue avec le responsable de traitement avant la collecte de données.

Dans les autres cas, il appartient au responsable de traitement de fournir l'information aux personnes concernées par les opérations de traitement au moment de la collecte des données.

5.4. Exercice des droits des personnes

Dans la mesure du possible, la commune doit aider la Métropole à s'acquitter de son obligation de donner suite aux demandes d'exercice des droits des personnes concernées : droit d'accès, de rectification, d'effacement et d'opposition, droit à la limitation du traitement, droit à la portabilité des données, droit de ne pas faire l'objet d'une décision individuelle automatisée (y compris le profilage).

Reçu au Contrôle de légalité le 03 juillet 2024

Dans le cas où la commune est désignée comme point de contact pour l'exercice des droits dans l'information prévue à l'article précédent, la commune doit répondre, au nom et pour le compte du responsable de traitement et dans les délais prévus par le règlement européen sur la protection des données aux demandes des personnes concernées en cas d'exercice de leurs droits, s'agissant des données faisant l'objet du présent marché.

Dans les autres cas, lorsque les personnes concernées exercent auprès de la commune des demandes d'exercice de leurs droits, la commune doit adresser ces demandes dès réception par courrier électronique à l'adresse mail (ou aux adresses mail) mentionnée(s) en page de garde du présent document, et copie à dpo@ampmetropole.fr.

5.5. Notification des violations de sécurité et/ou de données à caractère personnel

La commune notifie à la Métropole toute violation de sécurité et/ou de données à caractère personnel dans un délai maximum de 48 heures calendaires après en avoir pris connaissance et par courrier électronique à l'adresse mail (ou aux adresses mail) mentionnée(s) en page de garde du présent document, avec copie à dpo@ampmetropole.fr et rssi@ampmetropole.fr. Cette notification est accompagnée de toute documentation utile afin de permettre à la Métropole, si nécessaire, de notifier cette violation à l'autorité de contrôle compétente.

Après accord de la Métropole, la commune notifie à l'autorité de contrôle compétente (la CNIL), au nom et pour le compte de la Métropole, les violations de données à caractère personnel dans les meilleurs délais et, si possible, 72 heures calendaires au plus tard après en avoir pris connaissance, à moins que la violation en question ne soit pas susceptible d'engendrer un risque pour les droits et libertés des personnes physiques.

La notification contient au moins :

- la description de la nature de la violation de données à caractère personnel y compris, si possible, les catégories et le nombre approximatif de personnes concernées par la violation et les catégories et le nombre approximatif d'enregistrements de données à caractère personnel concernés ;
- le nom et les coordonnées du délégué à la protection des données ou d'un autre point de contact auprès duquel des informations supplémentaires peuvent être obtenues ;
- la description des conséquences probables de la violation de données à caractère personnel ;
- la description des mesures prises ou que La Métropole propose de prendre pour remédier à la violation de données à caractère personnel, y compris, le cas échéant, les mesures pour en atténuer les éventuelles conséquences négatives.

Si, et dans la mesure où il n'est pas possible de fournir toutes ces informations en même temps, les informations peuvent être communiquées de manière échelonnée sans retard indu.

Après accord de la Métropole, la commune communique, au nom et pour le compte de la Métropole, la violation de données à caractère personnel à la personne concernée dans les meilleurs délais, lorsque cette violation est susceptible d'engendrer un risque élevé pour les droits et libertés d'une personne physique.

La communication à la personne concernée décrit, en des termes clairs et simples, la nature de la violation de données à caractère personnel et contient au moins :

- la description de la nature de la violation de données à caractère personnel y compris, si possible, les catégories et le nombre approximatif de personnes concernées par la violation et les catégories et le nombre approximatif d'enregistrements de données à caractère personnel concernés ;
- le nom et les coordonnées du délégué à la protection des données ou d'un autre point de contact auprès duquel des informations supplémentaires peuvent être obtenues ;

Reçu au Contrôle de légalité le 03 juillet 2024

- la description des conséquences probables de la violation de données à caractère personnel ;
- la description des mesures prises ou que la Métropole propose de prendre pour remédier à la violation de données à caractère personnel, y compris, le cas échéant, les mesures pour en atténuer les éventuelles conséquences négatives.

5.6. Aide de la commune dans le cadre du respect par la Métropole de ses obligations

La commune aide la Métropole pour la réalisation éventuelle d'analyses d'impact relative à la protection des données. Lorsqu'elles sont requises, les analyses d'impact relatives à la protection des données sont incluses dans les prestations de la convention.

La commune aide la Métropole pour la réalisation de la consultation préalable de l'autorité de contrôle.

5.7. Mesures de sécurité

La commune s'engage à mettre en œuvre les mesures de sécurité techniques et organisationnelles garantissant un niveau de sécurité adapté au risque, y compris, entre autres :

- la pseudonymisation et le chiffrement des données à caractère personnel,
- les moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et des services de traitement,
- les moyens permettant de rétablir la disponibilité des données à caractère personnel et l'accès à celles-ci dans des délais appropriés en cas d'incident physique ou technique,
- une procédure visant à tester, à analyser et à évaluer régulièrement l'efficacité des mesures techniques et organisationnelles pour assurer la sécurité du traitement.

Le détail des mesures de sécurité est précisé dans le PAS.

5.8. Sort des données

Au terme de la prestation de services relatifs au traitement de ces données, la commune s'engage à renvoyer toutes les données à caractère personnel à la Métropole.

Le renvoi doit s'accompagner de la destruction de toutes les copies existantes dans les systèmes d'information de la commune. Une fois détruites, la commune doit justifier par écrit de la destruction.

5.9. Délégué à la protection des données

La commune communique à la Métropole le nom et les coordonnées de son délégué à la protection des données, si elle en a désigné un conformément à l'article 37 du règlement européen sur la protection des données.

5.10. Registre des catégories d'activités de traitement

La commune déclare tenir par écrit un registre de toutes les catégories d'activités de traitement effectuées pour le compte de la Métropole comprenant :

- le nom et les coordonnées de la Métropole pour le compte de laquelle il agit, des éventuels sous-traitants et, le cas échéant, du délégué à la protection des données ;

Reçu au Contrôle de légalité le 03 juillet 2024

- les catégories de traitements effectués pour le compte de la Métropole ;
- le cas échéant, les transferts de données à caractère personnel vers un pays tiers ou à une organisation internationale, y compris l'identification de ce pays tiers ou de cette organisation internationale et, dans le cas des transferts visés à l'article 49, paragraphe 1, deuxième alinéa du règlement européen sur la protection des données, les documents attestant de l'existence de garanties appropriées ;
- dans la mesure du possible, une description générale des mesures de sécurité techniques et organisationnelles, y compris entre autres, selon les besoins :
    - la pseudonymisation et le chiffrement des données à caractère personnel ;
    - des moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et des services de traitement ;
    - des moyens permettant de rétablir la disponibilité des données à caractère personnel et l'accès à celles-ci dans des délais appropriés en cas d'incident physique ou technique ;
    - une procédure visant à tester, à analyser et à évaluer régulièrement l'efficacité des mesures techniques et organisationnelles pour assurer la sécurité du traitement.

6. Management de la SSI de la commune

La commune dispose d'un corpus documentaire SSI composé de :

- une PSSI : celle est revue à minima tous les 3 ans. Elle respecte les principes de la PSSIE.
- une analyse de risque : elle s'appuie sur une méthode d'analyse de risques en cohérences avec les principes de l'ISO27005, est revue régulièrement et définit des actions de suppression ou limitation des risques.
- une démarche d'audit : elle définit les principes de contrôle internes permettant à la commune de vérifier le maintien en condition de sécurité de son système.

6.1. Sécurité des ressources humaines

Lors du processus de recrutement des contrôles de vérification de fond sur tous les candidats sont effectués par la commune en conformité avec les lois, les règlements pertinents et l'éthique. Ces contrôles doivent être proportionnées aux exigences métier, à la classification des informations accessibles et aux risques identifiés.

L'ensemble du processus d'arrivée et départ d'un collaborateur est piloté par les Ressources Humaines de la commune.

Des plans de formation et des plans de sensibilisation aux mesures de sécurité sont mis en place à l'attention du personnel de la commune et, quand cela est pertinent, des sous-traitants. De plus, le personnel et les sous-traitants reçoivent régulièrement les mises à jour des politiques et procédures de l'organisation s'appliquant à leurs fonctions.

6.2. Sécurité des infrastructures

6.2.1. Cartographie du service

La commune dispose d'une cartographie des principaux composants entrant dans le cadre des prestations de la convention.

Cette cartographie est tenue à jour.

Reçu au Contrôle de légalité le 03 juillet 2024

6.2.2. Accès logiques

Les systèmes d'exploitation, applications et équipements réseaux utilisés doivent exiger que chaque utilisateur soit authentifié avec succès avant d'autoriser toute autre action pour le compte de cet utilisateur. Les droits sont configurés afin que :

- chaque profil d'utilisateurs n'ait accès qu'aux fonctions nécessaires pour remplir sa mission
- chaque utilisateur n'ait accès qu'au profil qui lui est attribué

Aucun authentifiant ne doit être stocké en clair (sans chiffrement ou condensat) quelle que soit la méthode de stockage (fichier, base de données, scripts …).

Des droits doivent être positionnés afin qu'aucun authentifiant ne soit accessible en lecture, même sous forme chiffrée, aux utilisateurs.

Les procédures de création, modification et suppression de compte doivent être décrites dans un document.

L'ajout d'utilisateur ou les modifications entrainant l'attribution de privilèges supplémentaires, doivent être officiellement validés et tracées dans l'outil.

Tous les comptes (système et applicatif) doivent être configurés de manière sécurisée (complexité de mots de passe, blocage au bout 5 tentatives, changement de mot de passe régulier, etc.)

Toute utilisation ou modification d'un compte doit être tracée.

Règles spécifiques pour les administrateurs :

Les comptes à privilèges (comptes administrateurs) doivent être nominatifs et distincts des comptes utilisateurs standards.

Les comptes à très hauts privilèges (administrateurs de domaines par exemple) doivent être sécurisés (mots de passes très complexes), nominatifs et distincts des comptes administrateurs standards.

6.2.3. Cloisonnement

Les infrastructures en charge du projet sont positionnées dans des zones réseau en cohérence avec leur criticité et leurs fonctions, et dans le respect des principes de cloisonnement.

La commune dispose d'une matrice des flux à jour pour l'ensemble des équipements du projet.

6.2.4. Sécurité des serveurs

Tous les serveurs respectent les bonnes pratiques de sécurisation (recommandations constructeurs, guides de l'ANSSI, etc.). Ces pratiques sont listées et maintenues dans un document.

Une solution contre les codes malveillants est déployée sur tous les serveurs du périmètre projet de la commune.

6.2.5. Sécurité des postes

L'installation des postes utilisés dans le cadre du projet respecte les bonnes pratiques de sécurisation. Ces pratiques sont listées et maintenues dans un document.

Une solution contre les codes malveillants est déployée sur chaque poste du périmètre projet de la commune.

6.2.6. Supervision de la sécurité

La commune doit disposer de solutions de supervision de la sécurité (EDR, SIEM, puits de logs, etc.).

Reçu au Contrôle de légalité le 03 juillet 2024

Annexe n°**III** : Plan d'Assurance Sécurité

La commune doit prendre toutes les précautions utiles au regard des risques présentés par son traitement pour préserver la sécurité des données et, notamment au moment de leur collecte, durant leur transmission et leur conservation, empêcher qu'elles soient déformées, endommagées ou que des tiers non autorisés y aient accès, et mettre en oeuvre au moins les mesures suivantes :

Catégories	Code mesure	Mesure
Sensibiliser les utilisateurs	PAS-01	Informer et sensibiliser les personnes manipulant les données
	PAS-02	Rédiger une charte informatique et lui donner une force contraignante
Authentifier les utilisateurs	PAS-03	Définir un identifiant (login) unique à chaque utilisateur
	PAS-04	Adopter une politique de mots de passe utilisateur conforme aux recommandations de la CNIL
	PAS-05	Obliger l'utilisateur à changer son mot de passe après réinitialisation
	PAS-06	Limiter le nombre de tentatives d'accès à un compte
Gérer les habilitations	PAS-07	Définir des profils d'habilitation
	PAS-08	Supprimer les permissions d'accès obsolètes
	PAS-09	Réaliser une revue annuelle des habilitations
Tracer les accès et gérer les incidents	PAS-10	Prévoir un système de journalisation
	PAS-11	Informer les utilisateurs de la mise en place du système de journalisation
	PAS-12	Protéger les équipements de journalisation et les informations journalisées
	PAS-13	Prévoir les procédures pour les notifications de violation de données à caractère personnel
Sécuriser les postes de travail	PAS-14	Prévoir une procédure de verrouillage automatique de session
	PAS-15	Utiliser des antivirus régulièrement mis à jour
	PAS-16	Installer un «pare-feu» (firewall) logiciel
	PAS-17	Recueillir l'accord de l'utilisateur avant toute intervention sur son poste
Sécuriser l'informatique mobile	PAS-18	Prévoir des moyens de chiffrement des équipements mobiles
	PAS-19	Faire des sauvegardes ou des synchronisations régulières des données
	PAS-20	Exiger un secret pour le déverrouillage des ordiphones
Protéger le réseau informatique interne	PAS-21	Limiter les flux réseau au strict nécessaire
	PAS-22	Sécuriser les accès distants des appareils informatiques nomades par VPN
	PAS-23	Mettre en oeuvre le protocole WPA2 ou WPA2-PSK, ou supérieur, pour les réseaux Wi-Fi
Sécuriser les serveurs	PAS-24	Limiter l'accès aux outils et interfaces d'administration aux seules personnes habilitées
	PAS-25	Installer sans délai les mises à jour critiques
	PAS-26	Assurer une disponibilité des données
	PAS-27	Utiliser le protocole TLS et vérifier sa mise en oeuvre

Reçu au Contrôle de légalité le 03 juillet 2024

Sécuriser les sites web	PAS-28	Vérifier qu'aucun mot de passe ou identifiant n'est encapsulé dans les URL
	PAS-29	Contrôler que les entrées des utilisateurs correspondent à ce qui est attendu
	PAS-30	Mettre un bandeau de consentement pour les cookies et autres traceurs non nécessaires au service
Sauvegarder et prévoir la continuité d'activité	PAS-31	Effectuer des sauvegardes régulières
	PAS-32	Stocker les supports de sauvegarde dans un endroit sûr
	PAS-33	Prévoir des moyens de sécurité pour le convoyage des sauvegardes
	PAS-34	Prévoir et tester régulièrement la continuité d'activité
Archiver de manière sécurisée	PAS-35	Mettre en oeuvre des modalités d'accès spécifiques aux données archivées
	PAS-36	Détruire les archives obsolètes de manière sécurisée
Encadrer la maintenance et la destruction des données	PAS-37	Enregistrer les interventions de maintenance dans une main courante
	PAS-38	Encadrer par un responsable de l'organisme les interventions par des tiers
	PAS-39	Effacer les données de tout matériel avant sa mise au rebut
Gérer la sous-traitance	PAS-40	Les relations avec les prestataires qui traitent des données au nom et pour le compte du responsable de traitement (l'organisme employeur) doivent faire l'objet d'un accord écrit. Cet accord doit contenir une ou des clauses spécifiques relatives aux obligations respectives des parties résultant du traitement des données à caractère personnel. L'accord doit notamment prévoir les conditions de restitution et de destruction des données. Il incombe au responsable de traitement de s'assurer de l'effectivité des garanties prévues (audits de sécurité, visites, etc.). Pour plus de précisions, vous pouvez vous reporter au guide de la sous-traitance et aux exemples des clauses de sous- traitance.
Sécuriser les échanges avec d'autres organismes	PAS-41	Ne pas transmettre des fichiers contenant les données à caractère personnel des usagers en clair via des messageries grand public
	PAS-42	Privilégier des moyens de communication autres que les messageries grand public pour communiquer des informations relatives aux personnes accompagnées à d'autres travailleurs sociaux ou organismes (p. ex.: plateformes d'échanges sécurisées, messagerie interne, etc.)
	PAS-43	Chiffrer les pièces sensibles à transmettre, si cette transmission utilise la messagerie électronique
	PAS-44	S'assurer qu'il s'agit du bon destinataire
	PAS-45	Assurer la confidentialité des secrets (clé de chiffrement, mot de passe, etc.) en les transmettant via un canal distinct (par exemple, envoi du fichier chiffré par courriel et transmission du secret par téléphone ou par SMS
Protéger les locaux et les bureaux physiques	PAS-46	Restreindre les accès aux locaux au moyen de portes verrouillées
	PAS-47	Installer des alarmes anti-intrusion et les vérifier périodiquement
	PAS-48	Ranger tous les documents papiers relatifs aux usagers dans des armoires fermées à clé
	PAS-49	Verrouiller la porte d'accès au bureau en cas d'absence prolongée
Encadrer les développements informatiques	PAS-50	Proposer des paramètres respectueux de la vie privée aux utilisateurs finaux
	PAS-51	Encadrer de manière stricte les zones de commentaires libres
	PAS-52	Tester sur des données fictives ou anonymisées
	PAS-53	Utiliser des algorithmes, des logiciels et des bibliothèques reconnus

Reçu au Contrôle de légalité le 03 juillet 2024

Utiliser des fonctions cryptographiques	PAS-54	Conserver les secrets et les clés cryptographiques de manière sécurisée
Sécuriser les mots de passe des usagers	PAS-55	Utiliser un gestionnaire de mots de passe ou un carnet stocké dans un coffre-fort pour enregistrer les mots de passe des usagers accompagnés dans le cadre de l'accompagnement numérique
Sécuriser les données de santé	PAS-56	En cas d'hébergement des données de santé à caractère personnel réalisé pour le compte des organismes assurant le suivi social ou médico-social par un prestataire informatique, celui-ci doit être agréé ou certifié pour l'hébergement, le stockage, la conservation de données de santé, conformément aux dispositions de l'article L. 1111-8 du code de la santé publique.

Reçu au Contrôle de légalité le 03 juillet 2024