

CAHIER DES CLAUSES TECHNIQUES PARTICULIERES (CCTP)

TECHNIQUES DE L'INFORMATION ET DE LA COMMUNICATION

MISE EN PLACE D'UNE ARMURERIE POUR LA POLICE MUNICIPALE DE LA VILLE D'ANGERS

SOMMAIRE

I. PRESENTATION GENERALE	4
A. Objet et durée du marché	4
B. Objectif principal.....	4
C. Contexte du projet.....	4
D. Les services impactés par ce marché	4
1. La Police Municipale d'Angers.....	4
2. La Direction du Système d'Information et du Numérique (DSIN).....	5
II. DESCRIPTION DES PRESTATIONS ATTENDUES.....	6
A. La fourniture, la pose et l'intégration d'une solution pour entreposer les armes de la police municipale d'Angers et en tracer les accès.....	6
1. Description des attendues	6
2. Dimensions de la future armurerie.....	6
3. Détail des armes à stocker	7
4. Administration fonctionnelle de la solution	8
5. Principales fonctionnalités	8
a) L'armoire à clé et la solution numérique liée	8
b) Les coffres individuels.....	9
c) Les coffres collectifs.....	9
B. Le référencement des armes	9
C. La traçabilité des entrées et sortie d'armes	9
1. Equipements à mettre en place	9
a) Pour ajouter, supprimer ou modifier des armes	9
b) Pour gérer les entrées / sorties d'armes et de munitions par les agents PM en intervention	10

2. Solution numérique	10
D. Accès en mobilité aux équipements	10
E. La gestion des dates de validité des équipements et des formations obligatoires.....	10
1. Date de validité des équipements.....	10
2. Formations obligatoires des agents.....	11
F. La gestion des stocks des équipements de la police Municipale	11
G. La formation des agents aux outils	11
H. Assistance annuelle autour du fonctionnement des outils.....	11
I. Garanties.....	12
J. Licences et maintenance	12
III. DESCRIPTION DES BESOINS TECHNIQUES	13
A. Hébergement de la solution	13
B. Modalités d'accès au service	13
C. Matériel fourni	13
D. Poste de travail	13
E. Authentification.....	13
F. Sauvegardes	13
G. Conservation et purge des données applicatives	14
H. Mode dégradé	14
I. Mises à jour	14
J. Journalisation	14
K. Envoi de mail.....	14
L. Référentiel de temps	15
M. Mise en place de la supervision applicative.....	15
N. Performances.....	15
O. Transfert de compétence à la DSIN.....	15
P. Documentation d'installation et d'exploitation	17
1. Rapport d'Installation	17
a) Description technique.....	17
b) Installation serveur	17
c) Installation client.....	17
d) Matrice des flux	17
e) Interfaces	18
f) Dépendances	18
g) Equipements Spécifiques.....	18
2. Schéma d'architecture applicative	18
3. Procédures d'exploitation	19
a) Exploitation.....	19
b) Certificats	20
c) Interfaces	20

IV. DESCRIPTION DES BESOINS DE SECURITE.....	21
A. Plan d'Assurance Sécurité (PAS)	21
B. Respect des exigences de sécurité de l'acheteur	21
C. Obligations pour les titulaires manipulant des informations de l'acheteur sur leur SI	21
1. Politique, organisation, gouvernance	21
2. Gestion des biens	22
3. Sécurité physique	23
4. Sécurité des réseaux et de l'exploitation	24
5. Sécurité du poste de travail	25
6. Traitement des incidents.....	25
7. Continuité des services.....	26
8. Conformité, audit, inspection, contrôle	26
D. Sécurité des développements applicatifs	26
1. Règles de développement	26
2. Gestion des évolutions	27
V. MISE EN ŒUVRE	28
A. Calendrier et organisation projet.....	28
B. Les intervenants du prestataire.....	28
C. Récapitulatif de la documentation projet à fournir	28
1. Dans le cadre de la réponse :	28
2. A l'issu du déploiement :	28
a) Documentation technique :	28
b) Documentation fonctionnelle :	29
VI. ANNEXES 30	
A. Liste des sigles.....	30

I. PRESENTATION GENERALE

A. Objet et durée du marché

Ce marché a pour objet les prestations suivantes :

- La fourniture et l'installation d'un coffre à clés numérique
- La fourniture et l'installation de coffres à clé individuels et collectifs dans lesquels les agents de la Police Municipale d'Angers entreposeront leurs armes
- La fourniture et la pose de tags RFID sur les armes de la Police Municipale d'Angers
- Une solution permettant de tracer les entrées / sorties d'armes via une lecture des tags RFID positionnés
- La formation des agents de la ville aux solutions déployées
- Les licences et la maintenance des solutions déployées
- Des jours d'assistances annuelles post déploiement des équipements objets de ce marché
- La possibilité d'étendre le nombre de casiers individuels compte tenu des évolutions d'effectifs de police municipale

B. Objectif principal

L'objectif principal est l'aménagement d'une armurerie dans les futurs locaux de la Police Municipale d'Angers, permettant de tracer toutes les entrées et sorties d'armes et ainsi répondre à la réglementation en vigueur.

C. Contexte du projet

En mars 2025, Angers Loire Métropole a acquis les anciens locaux de la Banque de France pour y installer trois directions de la ville d'Angers et de la communauté urbaine :

- La direction Sécurité Prévention, incluant les policiers municipaux de la ville d'Angers
- Le centre de pilotage d'Angers Loire Métropole (nouveau service, mis en place dans le cadre du projet Territoire Intelligent, qui a pour vocation de centraliser l'ensemble des données collectées par les milliers de capteurs installés sur le territoire de la collectivité, pour une vision du territoire à 360° en temps réel)
- Le service commerce de la ville d'Angers

En juin 2025, les élus ont voté pour la dotation en arme létale des policiers municipaux de la ville d'Angers.

Actuellement, les armes des agents sont stockées dans des armoires fortes, avec tenue manuelle d'un registre d'entrée/sortie d'armes. Ce procédé est relativement chronophage et faillible. Ces armoires actuelles ne répondent pas aux futurs besoins, ni en termes de sécurité, ni en termes d'espace pour le stockage des armes.

La future armurerie devra contenir des armoires fortes récentes, intégrant une solution de traçabilité des armes et des clés.

D. Les services impactés par ce marché

1. La Police Municipale d'Angers

La police municipale dépend de la direction de la Sécurité et de la Prévention

Composé de 75 agents, le service se décline en quatre secteurs :

- Le secteur "contact-proximité", composé d'une brigade proximité et d'une brigade équestre (trois chevaux). Les agents interviennent sur tous les quartiers de la ville. Cette mission met en valeur l'essence même du métier du policier municipal dans son rôle de prévention, d'anticipation et de lien avec les usagers. Les agents se déplacent à pied, à vélo, en véhicule motorisé et à cheval.
- Le secteur "surveillance générale", composé d'une brigade de surveillance générale et d'une brigade cynophile (trois chiens). La mission de ces agents est davantage axée sur les interventions sur l'ensemble de la commune.
- Le secteur "Centre de commandement opérationnel et de supervision" (CCOS), composé de la Salle de Commandement Opérationnel (la SCO) et du Centre de Supervision Urbain (CSU). La SCO est chargée du traitement des appels et d'orienter en conséquence les équipes sur le terrain. Le CSU exploite, de jour comme de nuit, les images des caméras de vidéoprotection positionnées sur l'ensemble de la ville.
- Le secteur "nuit", composé de deux brigades et d'un maître-chien. Présents de 19h à 4h du mardi au samedi, en lien direct avec la police nationale, les agents exercent toutes les missions du policier municipal avec une priorité accordée à la tranquillité publique et à la lutte contre les nuisances, sonores principalement.

2. La Direction du Système d'Information et du Numérique (DSIN)

La Direction du Système d'Information et du Numérique (**DSIN**), rattachée à la collectivité Angers Loire Métropole, est un service mutualisé entre la Ville d'Angers et Angers Loire Métropole.

L'organigramme de la DSIN est fourni en annexe.

Les prestations demandées devront être réalisées en coordination avec la DSIN, et notamment avec les intervenants suivants :

- Le **chef de projet numérique** chargé d'accompagner la maîtrise d'ouvrage dans ce projet,
- L'**administrateur / intégrateur** référent technique sur le projet,
- Le **Responsable Sécurité du Système d'Information (RSSI)** de la collectivité,
- Les **agents de l'équipe Relation à l'utilisateur**, en charge notamment du déploiement des matériels sur site.

II. DESCRIPTION DES PRESTATIONS ATTENDUES

A. La fourniture, la pose et l'intégration d'une solution pour entreposer les armes de la police municipale d'Angers et en tracer les accès

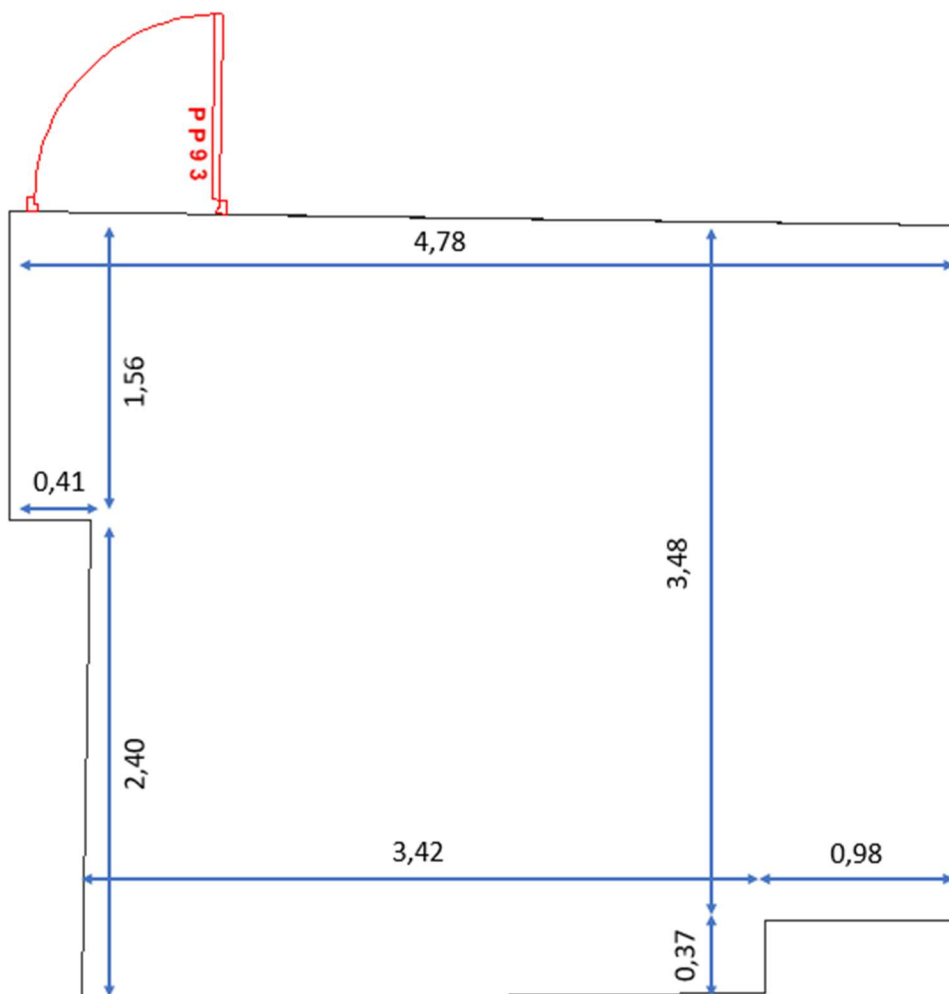
1. Description des attendues

La ville d'Angers souhaite s'équiper de nouveaux équipements pour y stocker son armement. Cela se présente sous la forme :

- D'une nouvelle armoire à clé
- D'armoires composées de casiers individuels pour y stocker les armes à dotation individuelle des agents de police (armement décrit plus loin)
- D'armoires collectives pour y stocker les armes non nominatives des agents de police (armement décrit plus loin)
- D'un poste d'administration fonctionnelle de la (ou des) solution numérique

2. Dimensions de la future armurerie

Les dimensions de la future salle d'armes sont présentées dans le schéma ci-dessous :



Cette salle accueillera l'ensemble des équipements décrits en point 3.

3. Détail des armes à stocker

Le tableau ci-dessous présente l'ensemble des équipements qu'il y aura à stocker dans les nouveaux coffres individuels et collectifs (prendre les projections à 2027) :

	Dotation	Nombre en 07/2025	Nombre en 2027 (projection)	Lieu de stockage	Typologie de coffre
Bâton télescopique	Individuelle	77	100	Armurerie	Individuel
Tonfa	Collective	11	0	Armurerie	Collectif
Pistolet à Impulsion Electrique (PIE)	Collective	26	26	Armurerie	Collectif
Lanceur de Balle de Défense (LBD)	Collective	4	6	Armurerie	Collectif
GAIL (gazeuses) + de 100ml (aujourd'hui individuel mais collectif avec l'arrivée de l'armurerie)	Collective	77	20	Armurerie	Collectif
GAIL (gazeuses) - de 100ml (aujourd'hui individuel mais collectif avec l'arrivée de l'armurerie)	Individuelle	0	100	Armurerie	Individuel
Arme létale	Individuelle	0	100	Armurerie	Individuel
Chargeur individuel (2)	Individuelle	0	200	Armurerie	Individuel
PVE/PDA (Procès-Verbal Electronique / Personal Digital Assistant) pour les agents PM	Stockage collectif mais avec attribution individuelle	75	100	Armurerie	Individuel (prise électrique à prévoir)

Les équipements suivants **ne sont pas à prendre en compte dans le cadre du marché** car stockés dans les coffres actuellement utilisés qui seront déménagés dans les futurs locaux de la DSP.

ATTENTION : les deux premières lignes seront à prendre en compte dans l'étude d'aménagement de la salle d'arme par les candidats.

	Dotation	Nombre en 07/2025	Nombre en 2027 (projection)	Lieu de stockage	Coffre
Cartouches PIE et LBD	Collective			Armurerie	Autre coffre : utilisation d'un des coffres actuels (profondeur 50 x largeur 100 x hauteur 195 cm)

Caméra piéton	Collective	25	50	Armurerie	Etagères positionnées au centre de l'armurerie (Environ 1m de largeur et 0.8 de profondeur)
Stock de Munitions (entraînement et réelles)	Collective			Local équipement	Autre coffre : utilisation d'un des coffres actuels
PVE/PDA (Procès Verbal Electronique / Personal Digital Assitant) pour les ASVP	Stockage collectif mais avec attribution individuelle	20	20	Local équipement	Individuel

4. Administration fonctionnelle de la solution

Un poste permettant l'administration fonctionnelle de la solution sera positionné dans une salle sécurisée attenante à l'armurerie. Ce poste n'est donc pas à prendre en compte dans l'aménagement de la future salle d'armes. Ce poste sera fourni par la collectivité pour qu'elle en garde la maîtrise (mise à jour, antivirus, EDR, etc.). Les caractéristiques techniques de ce poste sont décrites en chapitre III.

5. Principales fonctionnalités

a) L'armoire à clé et la solution numérique liée

La future armoire à clé contiendra l'ensemble des clés suivantes :

- Les 100 clés des coffres individuels
- Les clés des coffres collectifs
- Les 20 clés des véhicules légers dédiés aux agents PM

Les droits d'accès à chacune de ces clés seront administrés depuis le poste d'administration fonctionnelle de la solution.

Ci-dessous les principales fonctionnalités attendues (liste non exhaustive) :

- L'authentification se fera avec nos badges actuels (badges TIL Desfire avec clé de chiffrement usine TIL)
- Un second moyen contrôle d'accès (via code par exemple) peut être envisagé si préconisé par le candidat
- Une alarme envoyée par mail sera émise si une clé n'est pas remise en place dans un laps de temps défini
- L'armoire à clé devra présenter un accès mécanique aux clés en cas de panne réseau ou électrique. La traçabilité des accès se fera dans ce cas manuellement
- L'accès aux différentes clés sera tracé automatiquement (si la connexion au réseau est opérationnelle)

L'accès administrateur de la solution permettra (liste non exhaustive) :

- Le référencement des différentes clés : positionnement dans l'armoire et utilité
- La gestion des droits d'accès des agents aux différentes clés
- La génération d'un rapport présentant tous les accès aux différentes clés et présentant à minima les informations suivantes :
 - Nom ou matricule de l'agent PM
 - Date et heure de récupération de la clé
 - Nom de la clé
 - Utilité de la clé
- La saisie manuelle d'entrée/sortie de clés suite à une panne réseau ou électrique
- Cet accès ne sera octroyé qu'à une liste très restreinte d'utilisateurs et géré depuis une pièce attenante (en dehors de l'armurerie, dont l'accès est géré via notre solution de contrôle d'accès)

b) Les coffres individuels

Les coffres individuels ne seront pas liés à la solution numérique et ne pourront s'ouvrir qu'avec une clé. Un pass permettant d'ouvrir l'ensemble des casiers individuels devra être prévu par le candidat.

Chaque coffre individuel devra être doté d'une prise électrique permettant à l'agent PM d'y brancher son PVE

Chaque coffre individuel devra être en capacité de stocker l'ensemble des armements décrits en point 3 de ce chapitre.

Une fenêtre de visibilité de présence de l'arme depuis le coffre peut être proposé par le candidat mais n'est pas obligatoire.

c) Les coffres collectifs

Les coffres collectifs ne seront pas liés à la solution numérique et ne pourront s'ouvrir qu'avec une clé. Un pass. permettant d'ouvrir l'ensemble des casiers collectifs devra être prévu par le candidat. Ce dernier sera différent ou non de celui des coffres individuels, selon les préconisations du candidat.

L'ensemble des coffres collectifs devra être en capacité de stocker l'ensemble des armements décrits en point 3 de ce chapitre.

B. Le référencement des armes

Le référencement des armes s'appuiera sur l'enregistrement de tags RFID positionnés sur ces dernières.

Ci-dessous la liste exhaustive des équipements qu'il faudra référencer :

	Nombre à référencer
Bâton télescopique	100
Pistolet à Impulsion Electrique (PIE)	26
Lanceur de Balle de Défense (LBD)	6
GAIL (gazeuses) + de 100ml (aujourd'hui individuel mais collectif avec l'arrivée de l'armurerie)	20
GAIL (gazeuses) - de 100ml (aujourd'hui individuel mais collectif avec l'arrivée de l'armurerie)	100
Arme létale	100
Chargeur individuel	200
Caméra piéton	50

S'il ne s'appuie pas sur l'utilisation de tags RFID, le candidat devra décrire la solution qu'il compte mettre en place pour gérer le référencement des armes de la police municipale d'Angers.

Le stock de cartouche d'armes létale et des cartouches PIE et LBD devront également être référencés dans l'outil (sans tag RFID mais avec référencement dans l'outil du numéro de cartouche pour les PIE).

C. La traçabilité des entrées et sortie d'armes

1. Equipements à mettre en place

a) Pour ajouter, supprimer ou modifier des armes

L'ajout, la suppression ou la modification d'armes se fera depuis une salle attenante à la future salle d'armes. Le candidat devra décrire le système à mettre en place pour le permettre :

- Utilisation d'un poste de la collectivité obligatoire (voir caractéristiques techniques en chapitre III)

- Utilisation d'un lecteur de tag RFID ? Décrire le mode de communication entre le lecteur et le poste (USB, bluetooth, wifi sécurisé, autre)
- Schéma d'installation physique du système

b) Pour gérer les entrées / sorties d'armes et de munitions par les agents PM en intervention

Les entrées et sorties d'équipements et d'armes lors des interventions des agents de la Police Municipale se fera par le passage sous un portique. D'autres solutions sont possibles néanmoins c'est vers cette option que souhaite s'orienter la collectivité.

Il n'est pas attendu du candidat de présenter une solution de zone froide pour le chargement/déchargement des armes. La PM d'Angers se sera en effet équipée de puits balistiques qui seront installés dans l'armurerie (leur positionnement sera à définir avec le candidat retenu).

2. Solution numérique

Ci-dessous les principales fonctionnalités attendues :

- L'authentification se fera avec nos badges actuels (badges TIL Desfire avec clé de chiffrement usine TIL)
- Un second mode de contrôle d'accès (via code par exemple) peut être envisagé si préconisé par le candidat
- Une alarme envoyée par mail sera émise si une arme n'est pas remise en place dans un laps de temps défini
- Une alarme visuelle et/ou sonore sera émise si :
 - Un agent ne redépose pas l'ensemble de son armement à son retour de mission
 - Un agent sort avec un PIE mais sans caméras piéton (obligation légale de filmer lors de l'utilisation du PIE)
- La traçabilité automatique des entrées et sorties d'armes
- La gestion du stock de munitions (saisie manuelle du nombre de cartouches prises puis ramenées)

L'administration fonctionnelle de la solution se fera depuis le même poste que celui utilisé pour l'administration fonctionnelle de l'armoire à clé :

- Ajout, suppression, modification d'armes
- Attribution d'armes à 1 ou plusieurs agents
- Génération d'un rapport
- Réalisation d'inventaires
- Etc.

Aucune reprise de données n'est à prévoir. Le référencement total des armes se fera dans le cadre de la mise en place du système.

Le poste d'administration sera fourni par la collectivité, avec un Win11 à jour. L'application devra donc être compatible avec ce système.

IMPORTANT : le profil administrateur devra être distinct du profil utilisateur. Un utilisateur agent PM ne devra pas pouvoir réaliser ces opérations d'administration.

D. Accès en mobilité aux équipements

Il n'est pas attendu du candidat de proposer un accès aux solutions décrites plus haut en mobilité. Les accès se feront exclusivement depuis l'armurerie et depuis la salle attenante accueillant le poste d'administration des solutions.

E. La gestion des dates de validité des équipements et des formations obligatoires

1. Date de validité des équipements

Certains équipements, nécessitant ou non d'être tracés, présentent des dates de fin de validité :

- Gilets pare-balles
- Ethylo-tests
- Radars
- Gazeuses
- Etc.

Même sans tag RFID la solution qui sera déployée devra être en capacité de référencer ces équipements et d'en indiquer une date de fin d'utilisation possible.

Des alertes devront être générées :

- Par mail, régulièrement (fréquence à déterminer), listant les équipements arrivant en fin de validité (échéance paramétrable dans l'outil)
- Visuellement (ou sonore) lors de récupération d'un des équipements par un agent s'il possède un tag RFID et que la date de validité est dépassée

2. Formations obligatoires des agents

Les policiers municipaux ont l'obligation de suivre des formations tout au long de leur carrière (FIA, FCO, FPA, FE). La solution déployée devra permettre de renseigner, pour chacun des policiers référencés, sa date de dernière formation et de validité de cette dernière.

Des alertes devront être générées :

- Par mail, régulièrement (fréquence à déterminer), listant les agents n'ayant pas suivi leur formation ou pour lesquels la formation arriverait à échéance (délais à déterminer)
- Visuellement (ou sonore) lors de récupération d'un équipement si l'agent n'a pas suivi sa formation et n'est donc pas en droit de porter son arme

F. La gestion des stocks des équipements de la police Municipale

En sus des équipements référencés avec un tag RFID, la ville d'Angers souhaite pouvoir suivre son stock d'autres équipements utilisés par les policiers municipaux (équipements sans attribution individuelle) :

- Ethylo-tests,
- Radars,
- LEI (Laser Eblouissant d'Interdiction),
- Boucliers,
- Casques,
- Etc.

La gestion de ce stock sera réalisée par les mêmes agents qui seront en charge de l'administration fonctionnelle de la solution déployée.

La saisie des entrées / sorties de ces équipements par les agents PM lors de leurs interventions n'est pas attendue.

G. La formation des agents aux outils

Il est attendu du candidat retenu des formations pour :

- Les administrateurs fonctionnels du ou des solutions déployées : ajout/suppression/modification d'un nouvel agent, d'une nouvelle arme, génération d'un rapport, etc.
- L'ajout ou la modification de tags sur des armes
- Les agents de police : utilisation de l'armoire à clé, procédure d'entrée et de sortie des armes
- Les process d'utilisation des solutions en mode dégradé, en cas de coupure de courant ou de coupure réseau

Pour chacune de ces formations, un manuel utilisateur (ou procédure d'utilisation) devra être produit par le prestataire.

H. Assistance annuelle autour du fonctionnement des outils

A l'issue du déploiement des équipements et des solutions numériques, la ville d'Angers souhaite pouvoir bénéficier annuellement et sur la durée totale du marché de jours supplémentaires d'accompagnement notamment pour :

- S'assurer que les outils et équipements sont correctement utilisés

- Faire une revue des paramétrages réalisés post déploiements pour valider que les bonnes pratiques sont toujours respectées
- Faire une revue des droits et privilèges accordés
- Faire une passe des éventuelles nouvelles fonctionnalités proposées par l'éditeur

L'objectif de ces jours supplémentaire est de s'assurer qu'il n'y a pas de dérive dans l'utilisation des solutions déployées et que les agents restent en maîtrise de leurs outils.

Si ce genre d'accompagnement n'est pas déjà prévu au titre de la maintenance, le candidat devra l'intégrer à sa réponse.

I. Garanties

Le candidat indiquera les durées de garantie des équipements et des solutions déployées (période durant laquelle le candidat s'engage à corriger des dysfonctionnements, avant le démarrage de la maintenance)

J. Licences et maintenance

L'offre du candidat retenu devra inclure les licences et la maintenance des solutions numériques et des coffres sur toute la durée du marché.

Le candidat détaillera les moyens mis en œuvre pour assurer cette maintenance et les délais d'intervention en cas de dysfonctionnement du système.

Le niveau de disponibilité de l'application étant faible (l'application peut être indisponible pour 5 jours), la collectivité n'attend pas d'intervention en HNO et uniquement la semaine.

Les conditions d'accès au SI déployés sont détaillées dans le chapitre III (Description des besoins techniques)

III. DESCRIPTION DES BESOINS TECHNIQUES

A. Hébergement de la solution

La solution sera hébergée sur une VM fournie par la collectivité (solution On premise). Le prestataire devra détailler dans son offre les caractéristiques attendues pour pouvoir y installer sa solution.

B. Modalités d'accès au service

Pour limiter l'exposition du système qui sera mis en place, la collectivité souhaite privilégier des interventions sur place et non à distance, pour la phase de déploiement mais également lors de la maintenance. Le prestataire devra prendre en compte ce souhait dans sa réponse et y détailler ce que cela implique.

Si toutefois un accès distant devait être mis en place, il s'appuiera sur la solution fournie par la collectivité : accès VPN sur un bastion gérant les accès à privilège (et enregistrant toute l'activité), avec approbation systématique de la DSIN avant l'ouverture de l'accès. La prestataire devra dans ce cas préciser ses éventuels horaires d'intervention (HO/HNO).

C. Matériel fourni

Dans le cas où un matériel fourni par le prestataire serait à déployer, le prestataire précisera dans son offre les communications nécessaires entre ce matériel et les autres composants de la solution (ordinateurs, lecteur de badge ou de tag RFID, etc.). Les mesures détaillées dans le paragraphe « *Respect des exigences de sécurité de l'acheteur* » s'appliquent au matériel fourni.

D. Poste de travail

L'administration fonctionnelle des solutions déployées se fera depuis un poste fixe fourni par la collectivité sous **Windows 11**. **Aucun plug-in** ne devra être installé sur les postes de travail.

Le prestataire précisera (et fournira au moment de la prestation) dans son offre si des **pilotes** en lien avec les matériels utilisés (imprimantes, matériels mobiles...) sont à installer sur les postes de travail.

Les sources d'installation éventuelles seront également fournies par le prestataire (toutes les sources, ne pas prévoir de téléchargement internet au moment de l'installation). Leur installation sur les postes devra pouvoir être automatisable (pas d'exé nominatif, passage par un .msi).

Par défaut, ce poste sera isolé dans une bulle réseau étanche d'internet et ne pourra accéder qu'aux équipements et outils nécessaires au bon fonctionnement du système.

Le prestataire indiquera si des **ports** doivent être ouverts et si oui lesquels. Pour rappel, **il n'y aura aucune ouverture à internet de permise** pour le bon fonctionnement de la solution déployée

E. Authentification

Le prestataire précisera dans son offre les moyens d'authentification nécessaires à l'utilisation de sa solution.

Nous interdisons tout lien avec notre Active Directory, même si la solution le permet.

La politique de gestion des mots de passe est décrite dans le paragraphe « *Sécurité des réseaux et de l'exploitation* ». Le mot de passe sera stocké en utilisant un chiffrement irréversible en respectant les préconisations de la CNIL et de l'ANSSI.

F. Sauvegardes

Le prestataire précisera dans son offre le plan de sauvegarde (moyens, fréquence, durée de rétention...) ainsi que les informations relatives à un éventuel PRA (Plan de Reprise d'Activité) et PCA (Plan de Continuité d'Activité).

Le prestataire indiquera si le plan de sauvegarde est commun à l'ensemble de ses clients ou si un plan de sauvegarde spécifique peut être mis en œuvre. Il est souhaité que la périodicité de sauvegarde soit au minimum quotidienne.

Concernant la continuité d'activité, le prestataire devra détailler dans sa réponse la méthodologie détaillée pour sauvegarder le serveur dans sa totalité (OS, applis et données) via Veeam Backup (hébergement sur des VMs) et pouvoir repartir en cas de crash d'OS/appli d'un snapshot VMWare. La prestataire devra préciser s'il est nécessaire ou non de mettre en place une stratégie particulière (sauvegarde à froid, pré et post-traitements, ...) pour s'assurer de la consistance des données applicatives.

G. Conservation et purge des données applicatives

Les données applicatives devront être conservées 3 ans (conformément à l'article **R511-33 du CSI**).

La prestataire devra détailler le mécanisme de purge des données passé cette durée. Ce mécanisme devra être automatisé par le prestataire.

H. Mode dégradé

Le prestataire indiquera dans son offre les modes dégradés disponibles avec sa solution (par exemple en cas de coupure réseau ou électrique). Il précisera les mesures de sécurité proposées pour protéger les équipements et le SI de la collectivité dans ce cas. A noter que la collectivité évaluera les conditions de sécurité du mode dégradé proposé avant de décider de son implémentation.

I. Mises à jour

Le prestataire devra préciser les modalités de mise à jour des équipements et des solutions fournies : OS, mise à jour applicative, etc.

Les mises à jour d'OS (Windows ou Linux) pourront se faire via un passage en liste blanche par nos proxys. Les montées de version applicatives ne pourront se faire que manuellement. **Il n'y aura pas d'ouverture internet de permise.**

La solution déployée **devra toujours être compatible avec la dernière version de l'OS** du serveur l'hébergeant. Il en est de même pour la compatibilité du client lourd (si un client lourd est nécessaire) avec le poste de travail.

J. Journalisation

Le prestataire indiquera la nature des logs qui seront tracés par sa solution :

- Badgeage,
- Récupération d'une clé ou d'une arme,
- Restitution d'une clé ou d'une arme,
- Ouverture manuelle d'un coffre,
- Accès administrateur à la solution
- Ajout/modification/suppression d'une arme
- Etc.

Le prestataire devra préciser la volumétrie de ces événements et du stockage à prévoir. La prestataire devra également préciser la durée de conservation légale de ces logs et les moyens à mettre en œuvre pour en réaliser la purge.

K. Envoi de mail

L'envoi de mail depuis la solution numérique déployée par le prestataire s'appuiera sur le SMTP de la collectivité. Si cette utilisation n'est pas possible, le prestataire devra détailler comment il compte implémenter cette fonctionnalité autrement. Pour rappel, **il n'y aura aucune ouverture à internet de permise** pour le bon fonctionnement de la solution déployée.

La matrice des flux attendue dans les livrables contiendra cette information.

L. Référentiel de temps

Le prestataire pourra s'appuyer sur le serveur NTP de la collectivité pour l'horodatage des équipements et des données. Si cette utilisation n'est pas possible, le prestataire devra détailler comment il compte implémenter cette fonctionnalité autrement. Pour rappel, **il n'y aura aucune ouverture à internet de permise** pour le bon fonctionnement de la solution déployée.

La matrice des flux attendue dans les livrables contiendra cette information.

M. Mise en place de la supervision applicative

La collectivité supervise le bon fonctionnement de son SI avec l'outil Centréon. Afin de pouvoir superviser de manière exhaustive l'environnement applicatif de la solution, elle souhaite être accompagnée par le prestataire pour la mise en place cette supervision.

Cet accompagnement doit avoir lieu après l'installation des environnements applicatifs et le transfert de compétence à l'intégrateur de la DSIN. La collectivité estime à deux jours/Homme d'un ingénieur système cette prestation d'accompagnement.

La DSIN se chargera de la mise en place technique de cette supervision dans Centréon grâce à l'accompagnement du prestataire. Celui-ci devra décrire de manière exhaustive et grâce à ses connaissances de l'applicatif, toutes les briques techniques qu'il est nécessaire de superviser pour s'assurer du bon fonctionnement applicatif.

Pour l'exemple, les services, processus, ports, espaces disques, charge CPU, utilisation mémoire, validité des certificats, partages, tablespace des bases de données, webservices, temps de réponse des serveurs web, erreurs dans les fichiers journaux, interfaces ... sont supervisés dans Nagios par la Collectivité.

La mise en place de la Supervision applicative fera l'objet d'un PV de réception.

N. Performances

La collectivité entend maintenir un niveau de performance pour la solution logicielle. A cet effet, elle entend travailler avec le prestataire à l'établissement de plusieurs scripts ou méthodes de test de performance (métriques à superviser, outil de benchmark, ...) permettant de juger de celle-ci et le cas échéant de pouvoir corriger des soucis de performance.

La collectivité utilise Centreon/Nagios/rrdtools/nagvis/nsclient/Munin pour assurer la supervision de son SI, elle souhaite donc que ces outils de test de performance puissent être mis en place au travers de ses outils de supervision.

La définition et la mise en place de ces quelques outils se fera en collaboration avec la Collectivité.

Le prestataire devra donc fournir dans son offre les éléments de test de performance les plus pertinents, ainsi qu'un plan pour la mise en place de ces outils de test de performance en collaboration avec la DSIN et la direction utilisatrice de l'application.

Le plan de mise en place devra reprendre les éléments suivants :

- Script ou méthode à mettre en place
- Objet du script ou de la méthode (qu'est-ce qui est mesuré ?)
- Métriques de référence (indices de référence)
- Méthodologie d'implémentation
- Planification
- Coût
- Besoin d'accompagnement au sein de la DSIN (acteurs, compétences nécessaires)

La réception des éléments permettant de mesurer les performances applicatives fera l'objet d'un PV.

O. Transfert de compétence à la DSIN

Un transfert de compétence et une présentation de la nouvelle solution seront dispensés par le titulaire à l'équipe technique d'Angers Loire Métropole. Ces prestations auront lieu sur le site d'Angers Loire Métropole.

Ce transfert de compétences techniques de l'architecture déployée concernera un groupe de 3 à 8 personnes maximum. Une évaluation préalable des exploitants à former doit être réalisée par le soumissionnaire afin d'adapter le contenu des sessions de transfert de compétence.

Cette prestation permettra de valider l'architecture technique mise en place à Angers Loire Métropole et les documentations

Le contenu et les modalités du transfert de compétences techniques seront définis par le Titulaire en accord avec l'équipe d'Angers Loire Métropole, sur la base de la proposition remise par le Titulaire.

La documentation fournie dans ce cadre comprendra la documentation technique et fonctionnelle pour les administrateurs et le support de premier niveau.

A l'issue de ce transfert de compétence, les personnels concernés devront être capables de manager la solution et mettre en œuvre la reprise d'activité si nécessaire.

L'objectif est de :

- Présenter la nouvelle architecture mise en œuvre
- Décliner son fonctionnement
- Présenter l'organisation du service de supervision et/ou d'administration
- Présenter la documentation fonctionnelle et technique afférente au projet
- Présenter le fonctionnement interne des composants
- Présenter l'architecture de supervision et les composants supervisés
- Présenter l'architecture d'administration
- Décrire les fonctionnalités et le maniement du (ou des) outil(s) de configuration / administration
- Prendre en main les équipements et/ou plateforme de gestion/supervision
- Décrire précisément la configuration effective et les fichiers de configuration
- Décrire et tester les sauvegardes/restaurations
- Décrire les méthodes et l'aide au diagnostic
- Prévenir les dysfonctionnements courants
- Présenter le plan d'exploitation et les travaux courants
- Présenter l'organisation mise en place afin d'assurer la communication entre l'équipe des techniciens de Angers Loire Métropole et celle du Titulaire
- Fournir les procédures
- Fournir la documentation technique et fonctionnelle adaptée au SI d'Angers Loire Métropole et commentée lors de ce transfert de compétence
- Apporter les réponses aux questions qui seront posées

Modalité du transfert de compétences :

Le transfert de compétences est à distinguer de la formation sur plusieurs points :

- Le Titulaire a une obligation de résultats
- L'intervenant est un spécialiste du domaine couvert par le transfert de compétences
- Ce transfert de compétences correspond au contexte organisationnel, fonctionnel et technique d'Angers Loire Métropole
- Le transfert de compétences doit permettre de formaliser une méthode de travail.

La fourniture des documentations spécifiques à Angers Loire Métropole, amendées lors du transfert de compétence, sera soumise à un PV de validation.

P. Documentation d'installation et d'exploitation

Le prestataire devra fournir une documentation détaillée, dans un format permettant sa modification ultérieure par la DSIN, contextualisée à l'environnement de la Collectivité concernant l'installation et l'exploitation de la solution logicielle.

La Collectivité souhaite bénéficier de logigrammes ou schémas au format soit Microsoft Visio ou <https://app.diagrams.net/> (draw IO), pour les documentations de type textuel, des formats Microsoft Word ou ODT.

Les éléments attendus par la collectivité sont décrits dans les sous chapitres qui suivent.

1. Rapport d'Installation

Le prestataire s'engage à fournir à la Collectivité au moment de la MOM, un rapport d'installation détaillé (avec captures d'écran) contextualisé à l'environnement de la collectivité.

Ce rapport doit décrire toutes les briques techniques déployées, toutes les dépendances systèmes, les comptes utilisés, les ports, les tâches planifiées (Cron), ... Toutes les personnalisations produites dans le contexte de la collectivité devront être listées dans le document, soit regroupées dans un chapitre, soit par une couleur de texte spécifique suivie au fil du document.

Ce rapport doit permettre à la Collectivité d'assurer le Maintien en Condition Opérationnelle de la solution applicative, les tâches d'exploitation et la supervision.

Ce rapport d'Installation ne doit comporter aucun mot de passe mais seulement les comptes utilisés. Les identifiants seront fournis de manière sécurisée à la DSIN qui les stockera ensuite dans sa solution de gestion de mot de passe.

Voici les éléments attendus à minima dans ce livrable :

a) Description technique

Le prestataire devra fournir une description détaillée des briques techniques mises en œuvre, de leurs versions et de leurs dépendances en regard de leur destination fonctionnelle.

b) Installation serveur

- Procédure d'installation des applications (contextualisée à notre environnement)
- Description, préemption, mot de passe des comptes utilisés pour faire tourner les services/daemons
- Droits nécessaires au fonctionnement applicatif (administrateur local, utilisateur)
- Description et chemin des paramètres de configuration (fichiers de configuration, base de registre etc....)
- Section des fichiers de configuration liées à des personnalisations
- Description et chemin des données
- Description et chemin des sauvegardes
- Description et chemins des logs
- Description et paramètres des tâches planifiées, des règles firewall, des exclusions antivirus... toute modification de configuration de l'OS liée à l'applicatif
- Description et chemin des partages utilisés par la solution logicielle (NFS, CIFS ...) et des groupes et comptes utilisés pour accéder aux partages
- Description de la base de données (technologie, comptes utilisés)

c) Installation client

- Procédure d'installation d'un poste client
- Description et chemin des paramètres de configuration
- Description et chemin des paramètres en lien avec le profil utilisateur
- Description et chemin des paramètres liés à des périphériques
- Méthodologie d'installation des périphériques
- Prérequis techniques ou modules nécessaires au bon fonctionnement du client (version de navigateur, modules complémentaires, OS client, ...)
- Droits de l'utilisateur nécessaires au fonctionnement (administrateur local, utilisateur avec pouvoirs, utilisateur)

d) Matrice des flux

Le trafic réseau en provenance et à destination du système doit faire l'objet d'un contrôle permanent afin de n'autoriser que les flux légitimes. Une matrice de flux (inventaire des flux légitimes) sera fournie par le prestataire et maintenue à jour durant la durée du marché par le prestataire. (cf article 4 CCSC).

e) Interfaces

Descriptions des interfaces : Types, fonction de l'interface, ports, comptes, Entrées/Sorties, ...)

f) Dépendances

Préciser les services réseaux et logiciels dont la solution est dépendante (Smtip, composants système, java, framework, middleware...)

En complément des briques systèmes externes dont la solution est dépendante, le prestataire fournira la liste des logiciels inclus dans la solution (SBOM). Les composants logiciels inclus peuvent provenir de :

- Tiers
- Logiciel existant non développé selon une norme de sécurité
- Logiciel développé en interne déjà utilisé

Indépendamment de la source ou de l'utilisation actuelle du logiciel, le SBOM doit décrire tous les logiciels inclus dans la version. Le prestataire présentera le calendrier et le plan d'actions (par exemple montées de versions planifiées) afin qu'aucun composant utilisé ne soit dans une version obsolète non maintenue par son éditeur ou développeur.

Pour répondre, le prestataire s'appuiera sur la nomenclature SBOM ci-dessous :

- **Nom du fournisseur** : Le fournisseur ou les personnes qui ont écrit le logiciel.
- **Nom du composant** : Le nom du composant.
- **Identifiant unique** : Un identifiant unique universel (UUID).
- **Chaîne de version** : Les détails de construction et de version du composant.
- **Hash de composant** : Un hachage cryptographique du composant. Cela permet à un destinataire de vérifier, s'il a des soupçons, si un binaire qui lui a été fourni a été modifié.
- **Relation** : La relation entre les composants logiciels décrit les dépendances entre les composants et les composants qui ont été compilés et liés à d'autres composants.
- **Licence** : Le type de licence sous lequel le composant logiciel est publié.
- **Nom de l'auteur** : L'auteur du SBOM. Ce n'est pas nécessairement le fournisseur du logiciel.

g) Equipements Spécifiques

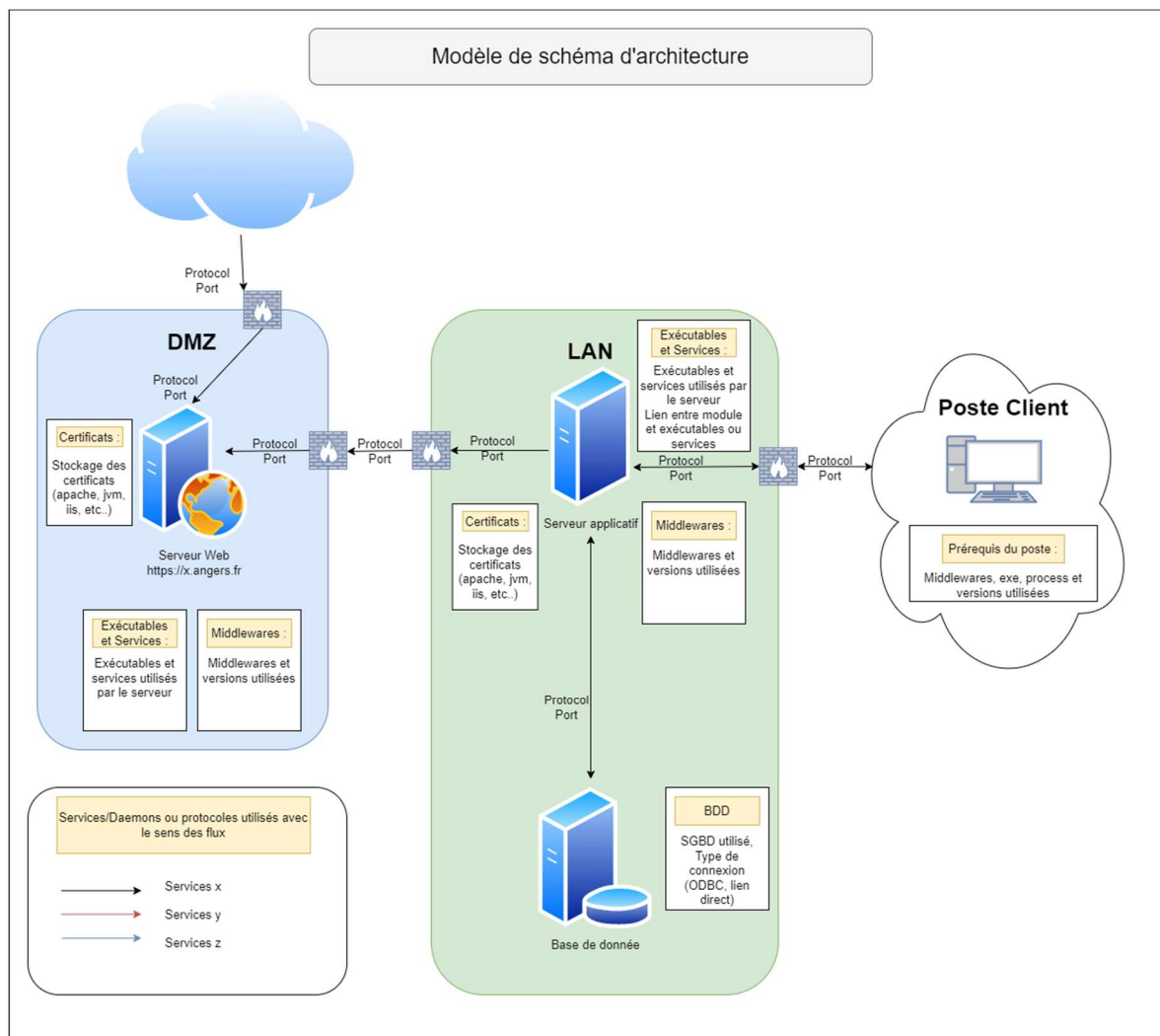
Descriptions du rôle et méthodologie d'installation des équipements spécifiques nécessaires au fonctionnement de la solution.

2. Schéma d'architecture applicative

Schéma reprenant l'ensemble des briques techniques et fonctionnelles de l'application et intégrant leur interdépendance fonctionnelle, ainsi que ses différentes interfaces avec des produits/modules internes/externes.

Le schéma doit être contextualisé à l'environnement mis en place dans la collectivité et être détaillé et reprendre à minima :

- Noms de serveurs
- Noms des services, processus
- Noms des bases de données
- Identification des flux (matrice des flux)
- Identification des ports et protocoles utilisés
- À compléter suivant les spécificités du logiciel pour la compréhension globale de l'application



3. Procédures d'exploitation

Pour maintenir en condition opérationnelle la solution applicative, le prestataire devra attacher un grand soin dans l'élaboration et la rédaction de la procédure d'exploitation.

a) Exploitation

Il s'agit ici de rédiger les procédures et méthodes nécessaires à l'exploitation de la solution et à son maintien en condition opérationnelle. Le prestataire devra à minima fournir les éléments documentaires listés ci-dessous, il devra en outre compléter ces éléments de toute particularité de son application portant sur la maintenance et la supervision.

Procédure d'arrêt/redémarrage de l'écosystème applicatif complet, en précisant l'ordre de redémarrage de chacun des services et leurs dépendances.

Description des travaux périodiques nécessaires au bon fonctionnement applicatif (purgas, ré-indexation, recyclage de serveurs web, ...)

Procédure détaillée de montée de version avec prise en compte des environnements interdépendants. Pour les sites web, prévoir et fournir les pages de maintenance et la méthodologie pour les mettre en place. Pour les webservices, fournir un plan de reprise après arrêt de la solution.

Méthodologie de copie de la base de production vers la base de test (si c'est possible).

Description et méthodologie de purgas, anonymisation, pseudonymisation, ... des données.

NB : La DSIN maintenant un script de redémarrage automatisé hebdomadaire de l'ensemble de ses solutions informatiques, elle s'appuiera sur ce document pour redémarrer les briques de la solution.

b) Certificats

Le prestataire fournira le cas échéant, et contextualisée à l'environnement de la Collectivité, une procédure d'installation et de renouvellement des certificats. Celle-ci doit faire mention des fichiers de configurations, chemin de stockage, magasins utilisés et services dépendants.

Si la solution s'appuie sur des certificats serveurs (pour des serveur web par exemple), ils seront générés et fournis par la collectivité. Le prestataire aura ensuite la charge de l'installer sur le serveur le nécessitant.

c) Interfaces

Le prestataire détaillera la méthodologie de diagnostic des différentes interfaces, de leurs entrées/sorties. Il s'attachera à fournir des informations sur les options de journalisation et chemin des fichiers journaux.

IV. DESCRIPTION DES BESOINS DE SECURITE

A. Plan d'Assurance Sécurité (PAS)

Le **Plan d'Assurance Sécurité (PAS)**, dont la trame est fournie en annexe, devra être complété par le prestataire et remis avec son offre. Le contenu de ce document pourra être discuté avec la collectivité. Une fois établi, ce document sera contractuel.

L'objet de ce document est de permettre au candidat de décrire ses pratiques en matière de sécurité (organisationnelles et techniques) permettant de couvrir les préconisations de la collectivité.

En complément du PAS, la matrice de couverture des préconisations de sécurité fournie dans le DCE permettra au candidat d'indiquer son niveau de prise en compte des différentes préconisations.

B. Respect des exigences de sécurité de l'acheteur

Au même titre que les agents de l'acheteur, le titulaire prend connaissance et applique les règlements internes de l'acheteur (PSSI, directive d'utilisation des systèmes d'information, directive d'utilisation de la messagerie, etc.).

Seuls les équipements fournis par ou explicitement autorisés par la DSIN peuvent être connectés au réseau de la collectivité. Ces matériels doivent donc être administrés par les équipes de la DSIN, pouvoir être gérés par les outils en place de gestion de parc et de configuration. Conformément au CCSC et au CCAG-TIC un MCS complet est en place, l'obsolescence et les corrections de vulnérabilités sont correctement gérées. Les éventuels accès à distance pour maintenance ne peuvent se faire qu'en respectant la politique d'accès à distance de la collectivité et en utilisant les solutions en place (solution d'accès à distance en place, authentification renforcée, cloisonnement et services de rebond, journalisation et traçabilité des actions). Tout équipement ne permettant pas un respect de la PSSI ne pourra pas être connecté, ou devra être mis en place au sein d'une zone entièrement cloisonnée du reste du SI.

La collectivité sera assujettie à la réglementation NIS 2 au niveau « entité essentielle ». Ainsi les 20 objectifs de sécurité amenés par NIS 2 devront être respectés à terme, notamment pour l'administration sécurisée.

C. Obligations pour les titulaires manipulant des informations de l'acheteur sur leur SI

1. Politique, organisation, gouvernance

Politique de sécurité du titulaire : le titulaire applique et fait appliquer à ses sous-traitants la politique de sécurité du présent marché. Cette politique de sécurité traite notamment des thèmes suivants :

- Organisation de la Sécurité des SI ;
- Application de la Politique de Sécurité des SI ;
- Évaluation de la sensibilité et protection des documents ;
- Gestion des ressources humaines ;
- Sécurité physique des locaux et des salles informatiques ;
- Architecture et exploitation des SI : réseaux, systèmes ;
- Sécurité des postes de travail ;
- Sécurité des supports numériques ;
- Gestion des autorisations et contrôle d'accès logique aux ressources ;
- Développement et maintenance des systèmes ;
- Gestion des incidents et des alertes ;
- Gestion de la continuité d'activité des SI ;
- Conformité et démarche de contrôle interne ;
- Localisation des données.

Organisation de la sécurité adéquate : le titulaire définit une organisation de la sécurité afin de respecter l'ensemble des contraintes émises par l'acheteur.

Existence d'un correspondant de sécurité : le titulaire désigne parmi son personnel un correspondant sécurité pour toute la durée de la prestation. Ce correspondant est notamment :

- L'interlocuteur privilégié de l'acheteur pour toutes les questions relatives à la sécurité de la prestation, notamment dans le cadre d'investigations initiées par l'acheteur ou le titulaire suite à des incidents de sécurité opérationnels ;
- Chargé du maintien et de la mise en application du PAS ;
- Ce correspondant est joignable aux horaires de bureau habituels. Tout remplacement de ce correspondant doit être notifié à l'acheteur.

Mise en œuvre d'une gestion de risques et son suivi : le titulaire met en place une gestion des risques et assure un suivi permanent de son niveau de maîtrise de risques ainsi que du respect des politiques et règles de sécurité applicables sur le périmètre des prestations, y compris auprès de ses propres sous-traitants.

Gestion de crise sécurité : sur son domaine de responsabilité SI, le titulaire applique le **processus formalisé et opérationnel de gestion de crise**, apte à assurer le traitement d'événements remettant en cause de façon inacceptable pour l'acheteur le respect des engagements de service et de sécurité SI contractualisés. Ce plan précise au minimum :

- Les principes d'escalade (critères de déclenchement, synoptique d'escalade) ;
- La composition de la cellule de crise : fonctions et responsabilités des membres (acheteur et titulaire) ;
- La liste nominative des membres et de leurs suppléants est référencée dans un annuaire ;
- Les moyens dédiés à la gestion de crise (salle(s) de crise, procédures opérationnelles, moyens de communication).

Exercices de gestion de crise : les exercices de gestion de crise prendront en compte les principales menaces, notamment le risque de corruption du SI à l'aide de rançongiciels.

2. Gestion des biens

Séparation des données de l'acheteur et des données d'autres clients : le titulaire conserve et traite les données de l'acheteur de manière séparée de ses propres données ou de données d'autres clients du titulaire. Le titulaire doit restreindre l'accès aux données de l'acheteur suivant le principe de restriction au besoin d'en connaître.

Protection de la documentation de l'acheteur sur support papier : le titulaire assure la protection de la documentation de l'acheteur sur support papier au sein des locaux, en la stockant dans des armoires ou des coffres fermés à clé/code par exemple, et sa destruction à la fin de la prestation.

Modalités d'échanges d'informations : le titulaire garantit que les modalités de stockage et d'échanges d'informations par mail permettent d'en assurer la confidentialité et l'intégrité.

Échange de supports : le titulaire garantit que les supports échangés ou à connecter sur un SI de l'acheteur n'intègrent aucun code malveillant et ont fait l'objet d'un test d'innocuité positif au moyen d'une attestation à fournir à l'acheteur.

Transmission de fichiers sur un support physique : toute transmission de fichiers sur un support physique (DAT, CDROM, etc.), par courrier externe ou par porteur, donne lieu à un accusé de réception. Il doit respecter les règles de protection des informations et documents existant en vigueur au sein de l'acheteur.

De plus, l'ensemble des opérations de transferts de disques durs, de supports d'archives ou de sauvegarde doit être inscrit dans un registre des opérations précisant :

- L'émetteur et le destinataire ;

- Le détail des opérations de transferts et notamment le nombre, la date.

Sur simple demande, ce registre est mis à la disposition de l'acheteur par le titulaire.

Marquage des ressources techniques : le titulaire applique des règles de marquage sur les ressources techniques (matériels et logiciels informatiques, supports de stockage) et les supports papier pour faire savoir au personnel autorisé que ces éléments contiennent des informations sensibles ou classifiées.

Les données les plus sensibles à protéger sont identifiées.

Supports de stockage hébergeant des données de l'acheteur : le titulaire conserve en lieu sûr les supports de stockage de données en fin de vie hébergeant des données de l'acheteur, en attendant de procéder à leur effacement ou à leur destruction avec des moyens adaptés visant à s'assurer qu'aucune donnée ne puisse être récupérée.

Le cas échéant, le titulaire ne met pas au rebut ou ne fait pas emporter par une société de maintenance, ou encore réutilise ces supports de sauvegarde à d'autres fins que celles prévues initialement sans l'autorisation expresse de l'acheteur.

Maintien à jour et mise à disposition des données relatives à la prestation : le titulaire maintient à jour et est en mesure de mettre à disposition de l'acheteur toutes les données relatives à la prestation. Le titulaire fournit systématiquement toute la documentation générée dans le cadre de la prestation à l'acheteur pour archive.

3. Sécurité physique

Contrôle d'accès physique aux bâtiments du titulaire : les bâtiments du titulaire hébergeant son personnel dans le cadre de la prestation doivent être équipés d'un dispositif de contrôle d'accès individuel. Les accès physiques aux bâtiments en question doivent être restreints aux stricts besoins opérationnels des différentes populations présentes dans les locaux du titulaire.

Le titulaire dispose d'une procédure de gestion des accès physiques aux bâtiments du titulaire. Celle-ci précise au minimum les modalités de gestion des demandes et de suppressions d'accès.

Le titulaire dispose d'une organisation relative à la gestion et au suivi des autorisations d'accès pour les bâtiments du titulaire.

Contrôle des accès aux ressources techniques du titulaire : le titulaire garantit que les accès physiques aux salles informatiques sont strictement restreints aux besoins opérationnels des différentes populations présentes sur les sites utilisés dans le cadre de la prestation. Les accès sont équipés d'un dispositif de contrôle d'accès individuel.

Le titulaire dispose d'une procédure de gestion des accès physiques aux locaux techniques du titulaire. Celle-ci précise au minimum les modalités de gestion des demandes et suppressions d'accès.

Le titulaire dispose d'une organisation relative à la gestion et au suivi des autorisations d'accès pour les locaux hébergeant des ressources de l'acheteur et les équipements de sûreté.

Protection intrusion physique des locaux techniques du titulaire : les locaux du titulaire qui hébergent ses ressources techniques (serveurs, équipements informatiques, équipements réseaux / télécoms, etc.) sont équipés de moyens de :

- Protection contre l'intrusion et les effractions ;
- Détection d'intrusion et d'effraction reliés à un système de surveillance centralisé ;
- Réaction en cas d'intrusion ou d'effraction.

Ces équipements sont opérationnels 24h/24h et 7j/7j.

Les moyens de protection sont adaptés aux moyens de détection et de réaction.

En particulier, toutes les portes donnant sur l'extérieur du bâtiment ont une méthode automatique de détection d'ouverture. De plus, toute fenêtre raisonnablement accessible est protégée contre les intrusions.

Accompagnement des visiteurs : le titulaire dispose d'une procédure spécifique à l'accueil des personnes étrangères à l'organisme. Il dispose également d'une procédure pour l'accès des véhicules au site.

En particulier, les personnes extérieures nécessitant un accès aux salles hébergeant des ressources informatiques (techniciens, visiteurs, maintenance, etc.) sont accompagnées par une personne habilitée.

Protection des plateaux mutualisés : en cas de mutualisation de ses plateaux, le titulaire met en place les mesures pour protéger les espaces attribués pour la prestation effectuée pour l'acheteur (accès au poste par badge, blocage session automatique après un certain temps d'inutilisation, câble de sécurité pour le matériel fourni par l'acheteur, etc.).

Étanchéité physique des ressources informatiques : les salles hébergeant les ressources informatiques utilisées dans le cadre de la prestation ne partagent pas le même bâtiment avec d'autres fonctions, particulièrement des bureaux n'appartenant pas à l'organisation. Si l'espace doit être mutualisé pour des raisons économiques, alors la salle hébergeant des ressources informatiques utilisées dans le cadre de la Prestation de l'acheteur n'a pas de murs adjacents à d'autres bureaux.

Le titulaire met en place des moyens garantissant une étanchéité physique entre les infrastructures physiques dédiées à l'acheteur de celles des autres clients au sein des salles informatiques : la salle hébergeant des matériels de l'acheteur doit si possible lui être dédiée ; dans le cas où la séparation physique des salles n'est pas possible, le titulaire fournit à l'acheteur une solution de « suite privative » au sein de la salle multi-clients, isolée physiquement du reste de la salle par un grillage descendant plus bas que le faux plancher et montant plus haut que le faux plafond.

4. Sécurité des réseaux et de l'exploitation

Cloisonnement des environnements informatiques : le titulaire est garant du bon cloisonnement (physique ou logique) des environnements utilisés dans le cadre de la prestation.

Sécurisation des flux d'administration : le titulaire chiffre tous les flux d'administration (système et fonctionnelle) par des procédés fiables garantissant la confidentialité et l'intégrité des données. Par ailleurs, les postes d'administration utilisés pour la prestation doivent être dédiés et n'avoir accès ni à Internet, ni aux infrastructures bureautiques du titulaire.

Règles de sécurité et d'exploitation : l'installation, l'exploitation et l'administration des moyens mis en œuvre dans le cadre des prestations sont conformes aux bonnes pratiques et aux règles de sécurité et d'exploitation établies par l'acheteur. Toute exception fera l'objet d'un accord préalable écrit des équipes de l'acheteur.

Anti-virus opérationnel et à jour : le titulaire s'assure de la bonne installation et mise à jour d'un logiciel anti-virus sur tous les postes de travail et serveurs dont il est responsable dans le cadre de la prestation.

La désactivation, même temporaire, d'un antivirus sur un serveur utilisé dans le cadre de la prestation devra avoir été préalablement notifiée à l'acheteur.

Gestion des mises à jour : le titulaire gère les mises à jour et l'application des correctifs de sécurité et des mises à jour antivirales, pour assurer le maintien en condition opérationnelle de l'ensemble de ses équipements pour les services fournis à l'acheteur.

Sauvegarde des données : le titulaire met en place un système de sauvegarde permettant la sauvegarde des données de la prestation hébergées sur les serveurs du titulaire conformément aux besoins de sauvegarde exprimés par le chef de projet de l'acheteur dans le cadre de la prestation.

Des tests périodiques (a minima semestriels) de restauration des sauvegardes effectuées sur les données contenues dans les serveurs du titulaire sont formalisés et effectués.

Stockage des sauvegardes informatiques : le titulaire protège les sauvegardes informatiques en les stockant dans un coffre étanche et ignifuge pour les supports magnétiques, ou sur un site de back up sécurisé.

Politique d'habilitation : une politique d'habilitation doit être formalisée. Elle doit inclure à minima l'accès aux actifs et aux informations (notamment les données métiers sensibles). En fonction des profils et des missions du personnel, la Politique d'Habilitation doit spécifier qui peut avoir accès à quoi.

Comptes individuels : le titulaire s'assure que son personnel devant accéder à des ressources informatiques ou réseau dans le cadre de la prestation (qu'elles soient hébergées chez le titulaire ou chez l'acheteur) dispose d'un compte individuel nominatif qui lui est personnel et qui ne sera utilisé uniquement par cette personne tout au cours de la vie du compte.

Comptes obsolètes ou par défaut : le titulaire s'assure de la suppression de tous les comptes inutiles ou obsolètes. De même, les mots de passe par défaut d'usine devront être systématiquement modifiés.

Comptes techniques : le titulaire doit disposer d'un inventaire justifié des comptes techniques (le compte propriétaire du fichier de la base de données, des données du serveur WEB, ...) nécessaires au fonctionnement du système.

Comptes d'administration : Les comptes et les privilèges du personnel à la fois utilisateurs et administrateurs sont dissociés. Le nombre d'administrateur du service est limité au strict nécessaire.

Une **authentification multifacteur** est prévue pour tous les administrateurs.

L'administration métier et de l'administration technique sont séparées

Politique du moindre privilège : le titulaire s'assure que tous les comptes (accès Windows et autres...) des intervenants dans le cadre de la prestation sont habilités selon le principe du moindre privilège.

Recensement des comptes d'accès : le titulaire tient à jour la liste exhaustive des comptes d'accès au SI de l'acheteur existants ainsi que des rôles et privilèges qui y sont associés.

Il fournit cette liste à l'acheteur sur demande.

Le titulaire effectue et formalise une revue périodique des comptes d'accès aux serveurs et autres ressources du titulaire utilisées dans le cadre de la prestation.

Attaques en essai et erreurs sur secrets d'authentification : les moyens d'authentification mis en place par le titulaire (sur ses serveurs, applications et postes de travail) incluent une protection contre les attaques en essai et erreur sur les secrets d'authentification.

Journalisation des actions : le titulaire conserve de manière exploitable, sur une durée d'un an après la fin de la prestation, la trace des actions réalisées dans son système à des fins de contrôle (audit) et de preuves. Le titulaire collecte et stocke à minima les informations suivantes :

- Connexion et déconnexion aux équipements et applications ;
- Consultations d'informations relatives à la vie privée ;
- Informations d'usage de l'Internet (accès aux sites Web) ;
- Accès en lecture et/ou en écriture à des fichiers et dossiers marqués « CONFIDENTIEL » ;
- Informations concernant les accès fructueux et infructueux (identifiant de l'utilisateur, date, heure) aux serveurs du titulaire.

Les traces enregistrées par le titulaire doivent être imputables à un individu, elles sont par ailleurs horodatées selon une référence horaire commune à l'ensemble des équipements d'un même réseau.

Gestion des traces : le titulaire prévoit dans sa procédure de traitement d'incident un chapitre sur la préservation des traces éphémères (volatiles) en cas de suspicion d'attaque. Une trace volatile est une trace potentiellement utile pour l'analyse forensique d'une attaque informatique mais qui ne peut pas, par nature, être journalisée (contenu de la RAM, du swap, journal des transactions d'un système de fichier, divers dates liées aux fichiers, clés de registres...). La procédure établit comment limiter l'activité susceptible de détruire ces traces éphémères.

Politique de mot de passe : le titulaire respecte la politique de définition des mots de passe de l'acheteur sur l'ensemble des comptes d'accès utilisateurs aux postes de travail et applications sous la responsabilité du titulaire.

- Usager externe = 12 caractères + complexité
- Utilisateur, agent de la collectivité = 12 caractères + complexité + renouvellement tous les 6 mois
- Administrateurs = 15 caractères + complexité + renouvellement tous les 6 mois
- Système = 20 caractères + complexité + changement dès qu'un personnel en ayant la connaissance n'est plus affecté au projet

Sources d'installation des logiciels : le titulaire dispose des sources d'installation des logiciels utilisés dans le cadre de la prestation, lorsque ces logiciels ne sont pas mis à disposition par l'acheteur.

Validité des licences : le titulaire s'assure de la bonne validité des licences des logiciels qu'il met à disposition de son personnel ou de l'acheteur dans le cadre de la prestation.

5. Sécurité du poste de travail

Protection contre le vol des postes de travail : le titulaire met en place des mécanismes de protection pour prévenir le vol des postes de travail. Le titulaire met notamment en place des câbles antivol de façon systématique.

Chiffrement du poste de travail : une solution de chiffrement, si possible qualifiée, est mise à disposition par le titulaire à ses intervenants afin de chiffrer les données sensibles stockées sur les postes de travail, les serveurs, les espaces de travail, ou les supports amovibles.

6. Traitement des incidents

Remontée d'alerte : le service de supervision du titulaire met en place un système de remontée d'alerte à l'acheteur, afin de détecter tout comportement anormal sur un périmètre SI lié à la prestation (ex : montée en charge du réseau), vol ou perte d'informations sensibles appartenant à l'acheteur (documentations techniques en particulier).

Enregistrement et traçabilité et gestion des incidents de sécurité : le titulaire assure l'enregistrement et la traçabilité des incidents de sécurité et dispose d'un processus formalisé et opérationnel de gestion des incidents de sécurité sur son domaine SI. Les procédures de gestion d'incident sont régulièrement testées

Traitement des incidents de sécurité : le titulaire contacte les interlocuteurs sécurité de l'acheteur désignés pour signaler tout incident de sécurité SI susceptible d'affecter les données ou le SI de l'acheteur. De plus :

- Si cet incident a lieu sur le SI de l'acheteur, le titulaire participera à la demande de l'acheteur au traitement de l'incident ;
- Si cet incident a lieu sur le SI du titulaire, le titulaire autorisera l'acheteur ou un tiers désigné à participer au traitement de l'incident (si l'acheteur le souhaite).

En outre, des réunions périodiques d'analyse post-incident devront être planifiées avec l'acheteur (traitement des causes profondes).

Base de connaissance : le titulaire capitalise les procédures de résolution des problèmes techniques récurrents dans une base de connaissance dédiée qu'il fournit à l'acheteur sur demande.

7. Continuité des services

Remplacement du matériel endommagé ou perdu : le titulaire prend toutes les dispositions nécessaires (matériel en spare, contrats de service), en relation avec l'acheteur, pour remplacer rapidement et sur les différents sites de l'acheteur tout matériel sous sa responsabilité endommagé ou perdu (poste de travail, serveur, équipement réseau).

Incident affectant la continuité des services : En cas d'incident affectant la continuité des services, le titulaire signale l'événement à l'acheteur selon la procédure d'alerte définie (gestion des alertes, incidents et situations de crise).

8. Conformité, audit, inspection, contrôle

Autocontrôles de sécurité : le titulaire effectue des autocontrôles de conformité aux exigences du CCTP et du PAS pour garantir le niveau de sécurité au démarrage de la prestation ainsi que son maintien tout au long de la prestation.

Une **politique de contrôles et d'audits de sécurité périodiques** est en place. Concernant les éventuels services exposés sur Internet il pourra être mis œuvre un outil de scan Internet des plages d'adresses IP du service numérique.

Régularisation des écarts ou des non-conformités au niveau d'exigence de sécurité de l'acheteur : en cas de constatation d'écarts avec le PAS et, plus généralement, en cas de non-conformité au niveau d'exigence de sécurité requis par l'acheteur, un plan de remédiation devra être formalisé par le titulaire 15 jours après la constatation des écarts. Le titulaire doit ensuite régulariser ces écarts par l'application du plan de remédiation dans un délai convenu en commun accord entre les deux parties.

D. Sécurité des développements applicatifs

1. Règles de développement

Le prestataire est tenu d'assurer la sécurité des développements conformément à l'état de l'art dans chacune des technologies mises en œuvre.

Voici une liste (non exhaustive) de **règles applicables** :

- 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 dans le code interdite ;
- Mise en œuvre d'une gestion efficace des erreurs.

Pour la mise en œuvre de technologies web, les développements pourront s'appuyer sur les recommandations de l'OWASP (Open Web Application Security Project).

La **recette de l'application** comprend une revue de code permettant de s'assurer d'une implémentation conforme aux exigences de sécurité. La correction d'éventuelles anomalies détectées lors de la revue de code sont à la charge du prestataire.

2. Gestion des évolutions

Les évolutions fonctionnelles ou techniques ne doivent pas remettre en cause le respect des exigences de sécurité ou compromettre une éventuelle opération de réversibilité. En cas d'évolution, le prestataire devra vérifier que sa mise en œuvre est conforme aux exigences contractuelles et en apporter la justification auprès du donneur d'ordres, avant validation par ce dernier.

V. MISE EN ŒUVRE

A. Calendrier et organisation projet

Le déploiement de la nouvelle armurerie de la ville d'Angers est lié à l'installation de la Direction Sécurité Prévention dans les locaux situés place Mendès France, dans les conditions prévues au Planning Général Prévisionnel de travaux du bâtiment et d'installation des services, sous responsabilité de la Direction des Bâtiments. A ce titre, l'armurerie devra être finalisée et réceptionnée au **31/05/2026** au plus tard.

Modalités de pilotage et instances de travail :

Le prestataire devra définir ses attentes quant à la participation de la collectivité : dans sa réponse, il précisera la répartition des rôles et la charge entre les acteurs de la collectivité (groupe pilote, utilisateurs) et ses propres intervenants.

L'équipe projet côté Angers Loire Métropole est détaillée dans le tableau ci-dessous :

Rôle	Noms Acteurs	Collectivité – Direction - Fonction
Référént DSP	Céline BENESTEAU	Ville d'Angers – DSP - Responsable du service Ressources Internes et Communication
	Olivier COHELEACH	Ville d'Angers – DSP - Responsable du service Police Municipale
Chef de projet	Amaury DELINOT	ALM – DSIN – Chef de Projet Numérique
Référént MOA	Louis DOSDAT	Ville d'Angers – DSP – Etat Major du service Police Municipale

B. Les intervenants du prestataire

Le prestataire devra désigner un responsable, interlocuteur privilégié tout au long du projet.

Afin de couvrir l'ensemble des compétences techniques requises, différents intervenants du prestataire travailleront sur ce marché.

Dans sa réponse, le prestataire devra préciser ses modalités d'intervention avec, entre autres :

- Le profil des différents intervenants ;
- Le profil du responsable, interlocuteur privilégié de la collectivité ;

Si le prestataire envisage de sous-traiter une partie des prestations prévues par le marché, il indiquera la nature et le montant des prestations, le nom du ou des sous-traitants, les conditions de paiement des contrats de sous-traitance. Les prestations en sous-traitance et les sous-traitants seront soumis à l'agrément préalable de l'acheteur.

C. Récapitulatif de la documentation projet à fournir

Les livrables listés ci-dessous seront restitués sous forme numérique :

1. Dans le cadre de la réponse :

- Proposition de plan d'aménagement de la future armurerie
- Planning de déploiement
- PAS (cadre de réponse fourni : « Mise en place d'une armurerie pour la ville d'Angers - PAS-cadre-de-réponse »)
- Matrice de couverture cyber (cadre de réponse fourni : « Mise en place d'une armurerie pour la ville d'Angers - PAS-matrice-de-couverture »)

2. A l'issu du déploiement :

a) Documentation technique :

- Rapport d'installation du système déployé reprenant l'ensemble des éléments listés en **chapitre 3 - Q – 1)**
- Les procédures d'exploitation du système déployé reprenant l'ensemble des éléments listés en **chapitre 3 - Q – 3)**
- Document d'architecture technique du système déployé incluant le schéma d'architecture applicative décrit en **chapitre 3 - Q – 2)** et les besoins techniques listés **en chapitre 3**

b) Documentation fonctionnelle :

- Manuel utilisateur des solutions déployées, incluant les procédures de récupération et de restitution de clés et d'armes
- Manuel d'administration fonctionnelle des solutions, incluant les procédures d'ajout/modification/suppression de clés, d'armes ou d'agent

VI. ANNEXES

A. Liste des sigles

ANSSI : Agence Nationale de la Sécurité des Systèmes d'Information

BPU : Bordereau de Prix Unitaires

CCAG-TIC : Cahier des Clauses Administratives Générales – Techniques de l'Information et de la Communication

CCTP : Cahier des Clauses Techniques Particulières

DCE : Dossier de Consultation des Entreprises

DPGF : Décomposition du Prix Global et Forfaitaire

DSIN : Direction du Système d'Information et du Numérique

MCS : Maintien en Conditions de Sécurité

PAS : Plan d'Assurance Sécurité

PCA : Plan de Continuité d'Activité

PRA : Plan de Reprise d'Activité

PSSI : Politique de Sécurité du Système d'Information

RGS : Référentiel Général de Sécurité (<https://www.ssi.gouv.fr/entreprise/reglementation/confiance-numerique/le-referentiel-general-de-securite-rgs/>)

SaaS : Software as a Service

SI : Système d'Information

VPN : Virtual Private Network

PM : Police Municipale

DSP : Direction Sécurité Prévention