OCTOBRE 2026

Marché 2026_023

Cahier des clauses techniques particulières (CCTP)

Maintenance des installations et logiciels de sûreté des immeubles de l'AMF et prestations annexes

AUTORITÉ DES MARCHÉS FINANCIERS

1. PRESENTATION GENERALE 3
2. RAPPEL DU CONTEXTE DE L'AMF EN MATIERE DE SURETE 5
3. PRESENTATION DES IMMEUBLES 6
4. DEFINITIONS 8
5. DESCRIPTION DES PRESTATIONS FORFAITAIRES 11
6. DESCRIPTIF DES PRESTATIONS A BONS DE COMMANDE 35
7. REGLES GENERALES D'EXECUTION 39
8. CONDITIONS PARTICULIERES D'EXECUTION 42
9. PRESCRIPTIONS TECHNIQUES GENERALES 45
10. INTERVENANTS DU TITULAIRE 49
11. OBLIGATIONS ET RESPONSABILITES DU TITULAIRE 53

1. PRESENTATION GENERALE

1.1. IDENTIFICATION DES INTERVENANTS

Maîtrise d'Ouvrage :	AMF / DRST[1] / DAF[2] / PSET[3]
Cyber Sécurité et Responsable de la sûreté AMF :	AMF / DRST / DCSR[4]
Exploitant et donneur d'ordres du Titulaire :	AMF / DRST / DAF / PSET / Q2SE[5]
Fournisseur pour le PSET de l'infrastructure informatique[6] :	AMF / DRST / DSI[7]

1.2. OBJET DU MARCHE

Le marché a pour objet des prestations de mise à niveau, de maintenance des installations de Sûreté des immeubles de l'AMF et des prestations annexes.

Celui-ci est constitué de prestations :

- ☐ **Forfaitaires** : Phase de démarrage et prestations de maintenance préventive, corrective et adaptative (des installations, et mises à jour logicielles mineures / majeures sur l'évolution de la version en cours et matérielles concernant toutes les évolutions notamment de sécurité, et notamment celles préconisées par l'ANSSI).

  Ces prestations constituent des forfaits détaillés à l'article 5 du présent CCTP.

- ☐ **Complémentaires** : Prestations permettant à l'AMF d'acquérir de nouveaux matériels, de réaliser des travaux complémentaires ainsi que d'effectuer des opérations de maintenance évolutive portant sur les installations. Les prestations complémentaires comprennent également la réversibilité. Elles font l'objet de commandes par l'AMF au titulaire, au fur et à mesure de la survenance des besoins.

  Ces prestations sont détaillées à l'article 6 du présent CCTP.

1.3. PERIMETRE GEOGRAPHIQUE

Le marché concerne les bâtiments suivants exploités par l'AMF :

- ☐ AMF1, situé 17 place de la Bourse 75002 Paris Cedex 02 ;
- ☐ AMF3, situé 119 rue Réaumur 75002 Paris Cedex 02.

1.4. PERIMETRE TECHNIQUE

Le périmètre technique comprend l'intégralité de l'infrastructure informatique (autrement appelé « Système d'Information ») de Sûreté et notamment les domaines suivants :

- ☐ Les moyens de vidéosurveillance (système VMS[8], archivage, encodage, caméras, câblage, alimentations électriques, organes d'exploitation, asservissement avec le contrôle d'accès etc.) ;

---

[1] Direction Ressources, Support et Transformation

[2] Directeur Administratif et Financière

[3] Pôle services et environnements de travail

[4] Directeur Cyber sécurité, Sûreté et Risques

[5] Responsable Qualité, Sûreté, Sécurité et Environnement

[6] Cf. limites de prestations § 5.9

[7] Directeur des systèmes d'information

[8] Vidéo Management software

- ☐ Les moyens de contrôle d'accès (système, contrôleurs, obstacles de contrôle d'accès automatiques, dispositifs de verrouillage électromécaniques, lecteurs et badges, câblage, alimentations électriques, organes d'exploitation, asservissement avec la vidéosurveillance etc.) ;
- ☐ Les moyens de détection d'intrusion (système, capteurs, câblage, alimentations électriques, organes d'exploitation, etc.) ;
- ☐ Les moyens d'interphonie de Sûreté (central, platines murales, poste mobile sur pupitre, câblage, alimentations électriques, organes d'exploitation, etc.) ;
- ☐ Les moyens de radiocommunication mobiles (base radio, relais, antennes, câblage, alimentations électriques, portatifs UHF (Ultra Haute Fréquence), chargeurs, talkie-walkie etc.) ;
- ☐ Les équipements de quincaillerie (ferme-porte, bec de canne, etc.) des portes sous contrôle d'accès et détection d'intrusion ;
- ☐ Toutes les liaisons câbles, avec tenants et aboutissants, permettant les connexions de tous les composants des systèmes de Sûreté ;
- ☐ Les asservissements au Système de Sécurité Incendie ;
- ☐ Les passerelles logicielles entre les systèmes ;
- ☐ Les outils de supervision des installations de Sûreté ;
- ☐ Les plates-formes informatiques et logicielles des systèmes (serveurs physiques, serveurs virtuels, postes clients dédiés ou non) ;
- ☐ L'administration et la supervision de l'architecture de Sûreté afin que cette dernière soit disponible 24/24 7jrs/7 ;
- ☐ Le maintien en condition opérationnelle des installations et équipements précités ;
- ☐ Le maintien en condition de sécurité des installations et équipements précités (Cybersécurité) ; fréquence minimale semestrielle avec une veille conseil obligatoire pour les vulnérabilités critiques ;
- ☐ Le SAS unipersonnel à unicité de passage ;
- ☐ Les organes de gestion de l'effet SAS des portes de garage AMF1 ;
- ☐ Interactions réglementaires avec les systèmes de Sécurité Incendie ;
- ☐ Interactions réglementaires avec la serrurerie des portes de compartimentage (sécurité incendie) ;
- ☐ Interactions réglementaires avec les ouvrants type menuiserie (portes / fenêtres).

2. RAPPEL DU CONTEXTE DE L'AMF EN MATIERE DE SURETE

2.1. PRESENTATION GENERALE DE L'AMF

Pour accomplir ses missions, l'AMF occupe intégralement, en tant que locataire, deux immeubles parisiens situés place de la Bourse dans le 2ème arrondissement. Un de ces immeubles fait face à l'immeuble de l'Agence France Presse (AFP). La place de la Bourse est régulièrement le lieu de rassemblement et de manifestations.

L'AMF emploie plus de 500 collaborateurs et fait intervenir en permanence plusieurs dizaines de prestataires externes, stagiaires ou auxiliaires. Ces collaborateurs sont majoritairement « sédentaires » et ne sont pas appelés à se déplacer dans leur cadre professionnel.

L'AMF reçoit de nombreux visiteurs dans le cadre professionnel, pour des rendez-vous ou des réunions avec du personnel AMF. L'AMF ne reçoit pas de public, à l'exception des séances de la commission des sanctions, de certaines audiences publiques et lors d'évènements.

Plusieurs fois par an, l'AMF organise des manifestations dans ses locaux avec parfois plusieurs dizaines d'invités externes.

Il existe des flux constants de personnes et d'informations entre AMF1 et AMF3.

2.2. IDENTIFICATION DES RISQUES DE L'AMF

En tant qu'acteur unique de la régulation des marchés financiers en France, l'AMF est principalement exposée à des risques :

- ☐ De vol d'information ;
- ☐ De sabotage, de blocage de son activité ;
- ☐ D'intrusion de manifestants ;
- ☐ D'actions visant à sa déstabilisation en tant qu'un des symboles du monde de la finance.

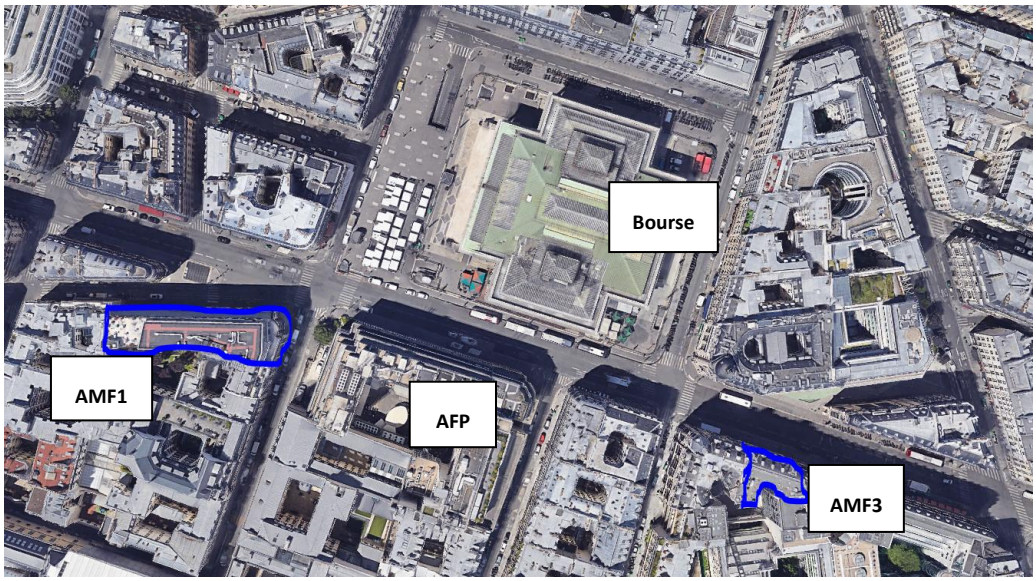
Compte tenu de la position unique de l'AMF, tout problème de sécurité et/ou de Sûreté aura potentiellement une forte visibilité médiatique et un important retentissement politique.

Dans ce contexte, les principaux objectifs de l'AMF en matière de sécurité et de Sûreté sont :

- ☐ La protection des personnes (personnels AMF, prestataires externes, visiteurs, ou personnalités) ;
- ☐ La protection des informations sensibles, via notamment un contrôle rigoureux des personnes ayant accès aux informations, et, de manière plus générale, un strict contrôle des accès physiques et des circulations à l'intérieur des bâtiments.

3. PRESENTATION DES IMMEUBLES

Les immeubles de l'AMF sont situés sur la Place de la Bourse en plein cœur de Paris, dans le 2ème arrondissement.



Place de la Bourse - Paris

3.1. IMMEUBLE AMF1

AMF1 est le « Siège » de l'AMF où celle-ci exerce son autorité : réunions du Collège, Commission des sanctions, etc. AMF1 est situé au 17, place de la Bourse et bénéficie d'une surface de 7 023 m² sur 4 niveaux de sous-sol et 8 niveaux de bureaux (capacité 500 personnes).

Bien que recevant du public à l'occasion de manifestations diverses, AMF1 est assujetti à la réglementation du Code du Travail (avec un dossier en cours d'instruction pour passage en ERP pour le RDC et le 8ème d'AMF1.



Entrée AMF1

3.2. IMMEUBLE AMF3

AMF3 est l'immeuble secondaire de l'AMF, regroupant notamment les services de support. AMF3 est situé au 119 rue Réaumur et bénéficie d'une surface de 2 300 m², comprend 2 niveaux de sous-sol, 7 niveaux de bureaux (capacité 200 personnes) et une terrasse. AMF3 est assujetti à la réglementation du Code du Travail.



Entrée AMF3

4. DEFINITIONS

4.1. DEFINITION NORMALISEE DES NIVEAUX DE MAINTENANCE

Conformément à la norme AFNOR NF X60-000, cinq niveaux de maintenance sont définis, comme suit :

1er niveau de maintenance : Réglages simples prévus par le constructeur au moyen d'organes accessibles sans aucun démontage ou ouverture de l'équipement ou d'échanges d'éléments consommables accessibles en toute sécurité tels que voyants ou certains fusibles, etc. Ce type d'intervention doit être effectué par l'exploitant du bien, sur place, sans outillage et à l'aide des instructions d'utilisation.

2ème niveau de maintenance : Dépannages par échange standard des éléments prévus à cet effet et opérations mineures de maintenance préventive, telles que graissage ou contrôle de bon fonctionnement. Ce type d'intervention doit être effectué par un technicien habilité de qualification moyenne, sur place, avec un outillage portable usuel. Ce dernier doit disposer des pièces de rechange transportables, sur le lieu d'exploitation et en quantité suffisante.

3ème niveau de maintenance : Identification et diagnostic des pannes, réparations par échanges de composants et des éléments fonctionnels, réparations mécaniques mineures, et toutes opérations courantes de maintenance préventive telles que le réglage général et les mesures de contrôle. Ce type d'intervention doit être effectué par un technicien de maintenance spécialisé, sur place ou dans un local de maintenance disposant des outillages spécifiques et la documentation technique de maintenance des équipements, ainsi que des pièces approvisionnées par le magasin.

4ème niveau de maintenance : Tous les travaux importants de maintenance corrective ou préventive à l'exception de la rénovation et de la construction. Ce niveau comprend également le réglage et la maintenance des appareils de mesure utilisés pour la maintenance, et éventuellement la participation à la visite de contrôle technique effectué par les organismes de contrôle. Ce type d'intervention doit être effectué par une équipe comprenant un encadrement technique très spécialisé, dans un atelier spécialisé doté d'un outillage général et spécialisé à l'aide de toutes les documentations générales et particulières.

5ème niveau de maintenance : Rénovation reconstruction ou exécution des réparations importantes confiées à un atelier central ou à une unité extérieure. Ce type de travaux est réalisé par le constructeur ou l'intégrateur.

4.2. GLOSSAIRE

Criticité : Évaluation d'un seuil de sensibilité critique pour l'exploitation, la sécurité des personnes des biens ou des informations d'un ensemble fonctionnel en cas de défaillance ou de perte de performance.

Dépannage : Action sur le bien en panne en vue de le remettre en état de fonctionnement au moins provisoirement. Compte tenu de l'objectif, un dépannage peut s'accommoder de résultats provisoires et de conditions de réalisation hors normes, et, dans ce cas, sera suivi d'une réparation.

Déverminage : Opération destinée à éliminer ou à détecter les pièces ou composants non satisfaisants ou susceptibles de présenter des défaillances précoces.

Disponibilité : Aptitude d'un bien, sous les aspects combinés de sa fiabilité, maintenabilité et de l'organisation de maintenance, à être en état d'accomplir une fonction requise dans les conditions de temps déterminées.

Durabilité : Durée de vie ou durée de fonctionnement potentielle d'un bien pour la fonction qui lui a été assignée dans les conditions normales d'utilisation et de maintenance données (MTBF)

Durée de fonctionnement : Durée pendant laquelle un bien accomplit effectivement la fonction qui lui a été assignée dans les conditions de performances minimales requises.

Durée de vie : Durée pendant laquelle un bien accomplit la fonction qui lui a été assignée.

Échange standard : Reprise d'une pièce, d'un organe ou d'un sous-ensemble usagé, et vente au même client d'une pièce, d'un organe ou d'un sous-ensemble identique, neuf ou remis en état de fonctionnement aux spécifications du constructeur, moyennant le paiement d'une soulte dont le montant est déterminé d'après le coût de remise en état.

Ensemble fonctionnel : Ensemble d'un ou de plusieurs composants matériel ou logiciel assurant une fonction.

Fiabilité : Aptitude d'un bien à accomplir une fonction requise dans les conditions données pendant un temps donné. Caractéristique d'un bien exprimée par la probabilité qu'il accomplisse une fonction requise dans des conditions données, avec des procédures et des moyens prescrits.

Jours : Sauf précision contraire, les délais sont indiqués en jours ouvrés.

Maintenabilité : Dans des conditions données d'utilisation pour lesquelles il a été conçu, aptitude d'un bien à être maintenu ou rétabli dans un état dans lequel il peut accomplir une fonction requise, lorsque la maintenance est accomplie dans les conditions données, avec des procédures et des moyens prescrits.

Maintenance : Ensemble des actions permettant de maintenir ou de rétablir un bien dans un état spécifié ou en mesure d'assurer un service déterminé.

Maintenance conditionnelle : Maintenance préventive subordonnée à un type d'événement prédéterminé révélateur de l'état de dégradation du bien (nombre de cycle de fonctionnement, nombre d'heure de service, etc.).

Maintenance corrective : Maintenance effectuée après défaillance.

Maintenance évolutive : Prestations et fournitures de matériel et de logiciel garantissant au cours de la vie des installations le maintien à un niveau de performances et de fonctionnalités comparable à ces mêmes installations proposées sur le marché. Elle n'intègre pas les upgrades majeures ou changement de version logicielle imposés par les éditeurs (fin de support d'une version par exemple) ceci est pris au titre de la maintenance adaptative. Seul le cas d'un changement de logiciel d'un éditeur par un autre produit d'un autre éditeur est concerné dans la maintenance évolutive.

Maintenance adaptative : Maintenance ajustée en fonction de l'évolution des besoins, des conditions d'utilisation ou des modifications règlementaires pour maintenir la conformité ou l'adéquation du bien ou service à son environnement.

Maintenance préventive : Maintenance effectuée à intervalles réguliers ou selon des critères prédéterminés (temps, usage, etc.) dans l'intention de réduire la probabilité de défaillance d'un bien ou la dégradation d'un service rendu.

Maintenance systématique : Maintenance préventive effectuée d'après un échéancier établi selon le temps ou le nombre d'unités d'usage.

Matières et matériels consommables : Sont considérés comme matériels ou matières consommables ceux dont la consommation est prévisible dans le cadre du programme d'entretien préventif courant d'une part, et d'autre part, ceux dont la valeur marchande est faible (joints, graisse, fusibles, etc.) et dont le coût est inclus dans le forfait.

Mode dégradé de fonctionnement : Aptitude d'un sous-ensemble à remplir temporairement ses fonctions principales dans l'attente d'une réparation. Action sur le bien en panne en vue de le remettre en état de fonctionnement partiel et provisoire.

Modernisation : Remplacement d'équipements, accessoires et appareils ou éventuellement de logiciel apportant, grâce à des perfectionnements techniques n'existant pas sur le bien d'origine, une amélioration de l'aptitude à l'emploi du bien.

Pièces détachées : Sont considérées comme pièces détachées, les matériels qui sont stockés sur le site ou dans les magasins pour accélérer les interventions de maintenance corrective soit parce que la pièce représente un élément stratégique pour la continuité de fonctionnement de l'installation, soit parce que les délais d'approvisionnement ne permettraient pas de respecter les clauses du marché.

Reconstruction : Remise en état définie par le cahier des charges initial, qui impose le remplacement de pièces vitales par des pièces d'origine ou des pièces neuves équivalentes. La reconstruction peut être assortie d'une modernisation ou de modification.

Rénovation : Inspection complète de tous les organes, reprise dimensionnelle complète ou remplacement des pièces déformées, vérification des caractéristiques et éventuellement réparation des pièces et sous-ensembles défaillants, conservation des bonnes pièces.

Réparation : Intervention définitive et limitée de maintenance corrective après défaillance.

Révision : Ensemble des actions d'examens, de contrôles et des interventions effectuées en vue d'assurer le bien contre toute défaillance majeure ou critique, pendant un temps ou pour un nombre d'unités d'usage donné.

GTI : Garantie de Temps d'Intervention. Délai à compter de l'identification d'un incident durant lequel le titulaire doit avoir initié une intervention.

GTR : Garantie de Temps de Rétablissement. Délai à compter de l'identification d'un incident durant lequel le titulaire doit rétablir le service.

HNO : Heures Non-Ouvrées. Horaires non-travaillés par le titulaire et l'AMF durant les jours ouvrés et non-ouvrés, correspondant ici à la tranche horaire de 20h30 à 07h30 le lendemain.

HO : Heures Ouvrées. Horaires travaillés par le titulaire et l'AMF durant les jours ouvrés, correspondant ici à la tranche horaire de 07h30 à 20h30**.**

JNO : Jours Non-Ouvrés. Jours de la semaine non-travaillés par le titulaire et l'AMF, correspondant ici au samedi et au dimanche, aux jours fériés ou aux journées de RTT (fermeture) imposées par l'AMF.

JO : Jours Ouvrés. Jours de la semaine travaillés par le titulaire et l'AMF, correspondant ici au lundi, mardi, mercredi, jeudi et vendredi.

5. DESCRIPTION DES PRESTATIONS FORFAITAIRES

Le marché comprend deux prestations forfaitaires : la phase de démarrage ainsi que la MCO et prestations associées.

Les prestations sont prises en charge par le Titulaire dans le respect du calendrier suivant :

- ☐ T0 = Date de notification du marché au Titulaire / début de la phase de démarrage ;
- ☐ T1 = T0 + 3 mois = fin de la phase de démarrage / début de de prise en charge autonome et intégrale des prestations.

5.1. MISE EN PLACE DU MARCHE - PHASE DE DEMARRAGE

La phase de démarrage du marché débute dès la date de notification (T0).

Elle a pour objectif de permettre au Titulaire une prise en charge progressive des prestations.

Le Titulaire prévoit dès cette date l'intervention sur site du personnel proposé, et fait en sorte qu'il soit opérationnel le plus rapidement possible.

Cette phase est d'une durée de trois (3) mois.

Pendant la phase de démarrage, les prestations de maintenance sont réalisées par le Titulaire sortant, qui y associe le Titulaire du présent marché.

Cette phase inclut notamment à la charge du Titulaire :

- ☐ L'initialisation et/ou la mise à jour de la Gestion de la Maintenance Assistée par Ordinateur (GMAO) mise à disposition par l'AMF ;
- ☐ La mise à jour éventuelle du stock des pièces détachées ;
- ☐ L'organisation des procédures d'appel en maintenance (émission des Demandes d'Intervention Technique (DIT) de suivi d'action et de conclusion d'intervention) ;
- ☐ La fourniture des outils et des documents de reporting soumis à validation de l'AMF ;
- ☐ Un projet de dimensionnement des stocks de pièces détachées nécessaires aux opérations de maintenances décrites au marché ;
- ☐ Le contrôle de la qualité, clarté, exhaustivité et actualité de la documentation ;
- ☐ Les tests d'accès aux différentes applications de l'architecture de sureté ;
- ☐ La fourniture des documents suivants :
  - Plan d'assurance qualité (PAQ)

    Word | PAQ
  - Plan d'assurance sécurité (PAS)

    Word | PAS
  - Procédure d'exploitation sécurisée (PES)

    Word | PES
  - Plan de continuité informatique (PCI) & Plan de reprise informatique (PRI)

    Word | PCI & PRI
  - Fichier CMDB

    Excel | CMDB

- Inventaire des pièces détachées

Excel	Inventaire des pièces détachées.

- Planning global annuel des maintenances

PDF	Calendrier annuel des interventions de maintenance préventive / adaptative, détaillé par équipement / logiciel et par gamme de maintenance, pour chaque bâtiment. Il devra détailler également les dates de mise à jour de plan, de mise à jour de stock, etc.

- Etat des lieux des niveaux de sûreté et cybersécurité du SI de sûreté AMF au regard des recommandations du guide de l'ANSSI en la matière

Power Point	Pour chaque recommandation sur la sécurisation des systèmes de contrôle d'accès physique et de vidéo protection du Guide7 ANSSI version 2.1, établir l'état des lieux du niveau de conformité de l'AMF aux exigences, et formaliser pour chaque écart une ou plusieurs préconisations unitaires qui permettrait à l'AMF de respecter l'exigence. Chaque préconisation doit être qualifiée par un niveau de difficulté, une estimation de charge (en jour-homme et euros) ainsi qu'une proposition affermie et réaliste de planning de mise en œuvre.

Le délai de remise des documents listés ci-dessus est de 1 mois à compter de la date de la réunion de lancement du marché. En cas de non-respect de ce délai, le titulaire encourt les pénalités prévues à l'article 17.2 du CCAP.

La phase de démarrage doit également permettre aux parties de convenir :

- d'un délai de test et d'observation pour chaque étape de la maintenance corrective ;
- d'une fréquence et des moyens mis en œuvre pour la MCS sur le SI de sûreté.

La phase de démarrage donne lieu à un état des lieux contradictoires :

Word	Un procès-verbal contradictoire de l'état des lieux et des matériels ou équipements est établi durant la phase de démarrage Dans un délai maximum de trente (30) jours suivant la remise de l'état des lieux, le Titulaire peut présenter des observations complémentaires sur l'état des installations qui lui sont confiées.

La réception de la phase de démarrage est matérialisée par la signature d'un procès-verbal de réception signé par les parties.

Le prix de la phase de démarrage est global et forfaitaire.

5.2. PRESTATIONS FORFAITAIRES DE MAINTENANCE (MCO) ET PRESTATIONS ASSOCIEES

Les prestations attendues au titre du forfait comprennent l'ensemble des actions et fournitures de maintenance de niveau 1 à 4 inclus (cf. définition des niveaux de maintenance à l'article 4.1 ci-dessus).

Elles sont déclenchées, à l'issue de la phase de démarrage, par un ordre de service.

Ainsi font partie intégrante de la prestation forfaitaire, dite de MCO, les prestations et fournitures liées à la maintenance :

☐ Préventive, systématique ou conditionnelle (maintenance logicielle adaptative, déverminage, consommables, maintien du stock de pièces détachées, rénovation, révision, échange standard) ;

[7] https://cyber.gouv.fr/publications/securisation-des-systemes-de-controle-dacces-physique-et-videoprotection

- ☐ Corrective (maintenance logicielle corrective, dépannage, réparation, échange standard, appel en garantie, utilisation et réparation des pièces détachées).
- ☐ Adaptative.

Les prestations complémentaires qui ne sont pas expressément comprises dans le forfait, ainsi que la maintenance évolutive, sont exécutées par voie de bons de commande.

Le Titulaire prend en charge :

- ☐ La maintenance préventive des installations et matériels, ainsi que les prestations associées ;
- ☐ La maintenance corrective, y compris l'intervention d'astreinte 24/24 et 7/7 ;
- ☐ La maintenance logicielle (adaptative et corrective) ;
- ☐ Le maintien en condition de sécurité (MCS) ;
- ☐ L'assistance à la conduite et à l'exploitation des installations ;
- ☐ La gestion du stock de pièces détachées ;
- ☐ La tenue du planning global des maintenances ;
- ☐ La tenue et la mise à jour de la base de données de gestion de configuration (CMDS) ;
- ☐ La fourniture du rapport des travaux à venir ;
- ☐ La revue documentaire, avec notamment la mise à jour, une (1) fois par an, des plans sur IHM (Interface Homme-Machine) et DOE (Dossier des Ouvrages exécutés), pour prendre en compte les éventuels changements de configuration des locaux ;
- ☐ Les travaux consécutifs aux vérifications des organismes de contrôle ;
- ☐ La gouvernance de la maintenance forfaitaire.

Ces prestations sont détaillées ci-après.

5.2.1. Maintenance préventive

Le Titulaire prend en charge forfaitairement la main d'œuvre et la fourniture nécessaires à la maintenance préventive (maintenance logicielle adaptative comprise) : pièces, consommables, outillage, etc.

La maintenance préventive est effectuée dans le but de réduire la possibilité de défaillance, la dégradation d'un service et le maintien des performances des installations.

Tout type de maintenance préventive confondue, chaque équipement, système ou dispositif inclus au périmètre technique du marché doit faire l'objet d'une visite de maintenance préventive au moins une fois par an, avec fourniture d'un compte-rendu.

Il est attiré l'attention du Titulaire sur le fait que l'architecture du système est mise en œuvre de telle façon à ce que les interventions en maintenance sur le système dans les 2 salles informatiques (salles blanches) soient exceptionnelles (interventions limitées à des interventions sur le hardware). Les interventions en maintenance seront majoritairement réalisées sur le poste du cadre de sécurité et Sûreté (RdC AMF1).

5.2.1.1. Maintenance préventive périodique

Suivant les matériels et systèmes concernés, les interventions de maintenance préventive pourront être périodiques. Elles sont déclenchées en fonction du calendrier établi par le Titulaire durant la phase de démarrage.

5.2.1.2. Maintenance préventive conditionnelle

Suivant les matériels et systèmes concernés, les interventions de maintenance préventive pourront être conditionnelles en fonction d'événements prédéterminés (nombre de cycle de fonctionnement, seuil bas de performance, accessibilité, etc.).

Le Titulaire devra mettre à profit la fermeture d'une zone pour anticiper une maintenance préventive.

5.2.1.3. Maintenance préventive des matériels sous-garantie

Le Titulaire prendra en charge la maintenance préventive des matériels sous garantie.

Il s'agit de :

- ☐ La maintenance des installations existantes ;
- ☐ La maintenance préventive ou corrective des matériels fournis à titre permanent ou temporaire ;
- ☐ La fourniture de matériels neufs ou l'échange standard dans le cadre d'une garantie sur un matériel fourni.

5.2.1.4. Nettoyage des équipements

Dans le cadre de la maintenance préventive périodique ou conditionnelle, le Titulaire prendra en charge le nettoyage des équipements inclus au marché.

5.2.1.5. Nettoyage des locaux

Au titre de la maintenance forfaitaire, le Titulaire prendra en charge le nettoyage des locaux qui lui sont confiés et les locaux techniques courants-faibles ou baies techniques qui hébergent les équipements de sécurité dont il a la charge.

5.2.2. Maintenance corrective

Le Titulaire prend en charge dans le cadre du forfait la main d'œuvre et la fourniture nécessaires à la maintenance corrective (maintenance logicielle corrective comprise) : pièces, consommables, outillage, etc.

La maintenance corrective consiste à réaliser des prestations de dépannage et de réparation. Elle est effectuée lors du dysfonctionnement d'une installation, d'un système ou d'un équipement constaté à la suite d'une défaillance ou d'une dégradation de service ou de performance.

Les niveaux d'incidents décrits ci-dessous sont pris en compte dans le cadre de la mise en œuvre de la GTI et de la GTR, telles que définies à l'article 5.3.9.1 ci-dessous.

Il est attiré l'attention du Titulaire sur le fait que l'architecture du système est mise en œuvre de telle façon à ce que les interventions en maintenance sur le système dans les 2 salles informatiques (salles blanches) soient exceptionnelles (interventions limitées à des interventions sur le hardware). Les interventions en maintenance seront majoritairement réalisées sur le poste du cadre de sécurité et Sûreté (RdC AMF1).

5.2.2.1. Incident critique

Une intervention urgente est requise lorsqu'un incident (par exemple une panne) qualifiée de « **critique** » survient.

Il est dit « **critique** » si les conséquences de la défaillance induisent un risque significatif pour la Sûreté des personnes, des biens et des informations avec :

- ☐ Une entrave significative de l'exploitation normale du site ;
- ☐ Ou des pannes sur les systèmes centraux du SI de Sûreté (logiciel d'exploitation, serveurs, disques durs, PC de gestion et d'exploitation, Unités de Traitement Local (UTL), etc.) ;

- Ou des pannes sur les équipements (sas d'entrée d'immeubles, obstacles automatiques dans les halls, SAS unipersonnel, gestion ascenseur, entrées parking, caméras périphériques, UTL, équipements intrusion, etc.) ;
- Ou des pannes sur des zones (salles informatiques, PC sécurité, périmètre des bâtiments niveau direction, bureau administrateur sécurité/Sûreté, etc.).

5.2.2.2. Incident bloquant

Une intervention rapide est requise lorsqu'un incident (par exemple une panne) qualifiée de « **bloquant** » survient.

Il est dit « **bloquante** » si les conséquences de la défaillance induisent un risque pour la sûreté des personnes, des biens et des informations et :

- Que des gênes perturbent l'exploitation normale du Site ;
- Que la panne remet en cause une partie de l'exploitation normale du site (organes de gestion : UTL, module de porte, carte de gestion intrusion, alimentations de secours, etc.).

5.2.2.3. Incident non bloquant

Une intervention est requise lorsqu'un incident qualifié de « **non bloquant** » survient.

Il est dit « **non bloquante** » si les conséquences de la défaillance n'induisent pas de risque pour la Sûreté des personnes, des biens et des informations et :

- Que les gênes ne perturbent pas l'exploitation normales du Site ;
- Que la panne n'empêche pas une exploitation normale du site (point par point : ferme-porte, radar volumétrique, lecteur de badges intérieurs, sirène d'alarme, etc.).

5.2.3. Maintenance logicielle

La maintenance logicielle, au sens de l'Association française de normalisation, consiste à réaliser des prestations et fournitures de logiciel garantissant au cours de la vie des installations le maintien à un niveau de performances et de fonctionnalités comparable à ces mêmes installations proposées dans le marché.

La maintenance logicielle peut être de trois types :

- Maintenance logicielle corrective (incluse au forfait) ;
- Maintenance logicielle adaptative (incluse au forfait) ;
- Maintenance logicielle évolutive. Cette dernière est une prestation à bons de commande, non comprise dans la maintenance forfaitaire. Elle est décrite à l'article 6.4 du présent CCTP.

Le Titulaire garantit ainsi la non-régression des fonctionnalités des matériels et logiciels.

Les interventions doivent avoir lieu selon la procédure de maintenance établie en phase de démarrage.

Le Titulaire doit tester toute évolution logicielle et/ou matérielle avant déploiement.

Toute modification ou évolution donnera lieu en fin d'opération à la mise à jour des données cartographiques matérielles, logicielles, flux réseau et comptes utilisés ainsi qu'à un contrôle des données de cartographie existantes.

5.2.3.1. Maintenance logicielle corrective

Au même titre que la maintenance corrective des installations, la maintenance logicielle corrective prévoit le traitement de toute défaillance logicielle qu'elle soit fonctionnelle, performancielle ou sécuritaire. À ce titre, le Titulaire doit toutes les prestations nécessaires au maintien des logiciels en état de fonctionnement et au niveau

de performance nominal à n'importe quel moment, sans limitation du nombre de ces interventions et de leur durée.

La maintenance logicielle corrective est intégrée au forfait.

Les versions correctives sont réputées ne pas contenir d'évolution fonctionnelle. En cas d'évolution fonctionnelle, la mise à jour doit être traitée selon la même procédure que la maintenance évolutive.

Les versions correctives et les modifications du paramétrage doivent être testées en respectant les étapes suivantes :

1. Plate-forme de test du Titulaire afin de s'assurer de leur bon fonctionnement avec des données de test ;
2. Intégration sur site AMF afin de s'assurer :
   - ↗ Du bon fonctionnement de la procédure / package d'installation ;
   - ↗ De la compatibilité avec l'environnement d'exécution AMF et avec des données réelles dans l'environnement de maquettage ;
   - ↗ Validation AMF de l'absence de régression avant déploiement.
3. Pilote sur un nombre réduit de composants afin de s'assurer de l'absence d'effet de bord dans l'environnement de production :
   - ↗ Validation AMF du bon fonctionnement en pilote ;
4. Généralisation à l'ensemble des immeubles de l'AMF.

Le délai de test et d'observation pour chaque étape sera convenu entre les parties durant la phase de démarrage et annexé au contrat.

En règle générale, les correctifs de sécurité sont publiés périodiquement par tous les éditeurs. Chez Microsoft, ceux-ci sont publiés mensuellement ; il faudra donc déployer des correctifs de sécurité mensuellement.

5.2.3.2. Maintenance logicielle adaptative

La maintenance logicielle adaptative correspond à la prise en compte :

- ☐ D'adaptation technique, fonctionnelle et performancielle pouvant apporter des améliorations d'exploitation (exemple : upgrade logiciel mineur) ;
- ☐ De changement ou de palier technique nécessaire pour garantir le bon fonctionnement des dispositifs (exemples : saut technologique d'un équipement, besoin de prendre en compte un changement de version majeure, d'une bibliothèque ou d'un système d'exploitation, fin de garantie d'un équipement par le constructeur, fin de production d'un équipement par le constructeur, upgrade de version logicielle imposé par l'éditeur, fin de support d'une version logicielle et upgrade nécessaire vers la nouvelle version de l'éditeur, etc.).
- ☐ Le changement de version majeure ou mineure de la version du logiciel de l'éditeur concerné.

Le Titulaire propose préalablement à toute intervention un mode opératoire soumis à la validation de l'AMF pour garantir la non-régression des fonctionnalités. Ce mode opératoire définit l'organisation, les essais prévus et l'étude d'impact.

Cette maintenance logicielle adaptative est réalisée forfaitairement dans le cadre de la maintenance préventive. Elle intègre naturellement le durcissement du logiciel à upgrader (cela comprend aussi si besoin la couche OS).

Le Titulaire devra informer les représentants de l'AMF des évolutions des logiciels des constructeurs/éditeurs et des conséquences de la non-évolution des installations dont il a la charge ainsi que les moyens nécessaires pour que les installations soient toutes au niveau standard d'aptitude à l'emploi et de maintenabilité.

Le Titulaire pourra être tenu pour responsable d'un manquement à son obligation de conseil et de mise en garde dans le cas où il n'aurait pas averti l'AMF de l'extinction de la maintenance constructeur ou éditeur d'un logiciel ou de la garantie d'un système pour quelque motif dans un délai suffisant permettre aux parties d'adopter les mesures

nécessaires. Cette responsabilité exclut les cas d'absence volontaire d'évolution logicielle, de logiciels irrégulièrement actualisée avant la prise en charge par le Titulaire ou auquel l'AMF aurait renoncé expressément.

Le Titulaire est tenu de fournir à l'AMF tout plan de progrès sur les installations dont il a la maintenance dont il aurait observé la nécessité. À ce titre, il est demandé au Titulaire de disposer tout au long du contrat exclusivement de logiciels, système ou applicatif, supportés par leur éditeur respectif. Ce plan de progrès doit permettre une action adaptative dans le respect des processus du marché et plus largement des processus de l'AMF.

Les montées de versions mineures des applications seront traitées de la même manière que les évolutions correctives (absence de recette usine).

Les montées de versions majeures seront traitées selon le même séquencement et nécessiteront une validation explicite sous la forme d'une recette « usine » selon une procédure similaire à la recette usine initiale complétée par le test des nouvelles fonctionnalités.

La qualification des applications et de leur socle d'exécution nécessite une mise à niveau préalable avant l'étape correspondante :

- ☐ De la plate-forme de test ;
- ☐ Des systèmes des postes et / ou serveurs ;
- ☐ De la cartographie.

Le déploiement devra suivre les étapes suivantes :

1. Plate-forme de test du Titulaire afin de s'assurer de leur bon fonctionnement avec des données de test ;
2. Intégration sur site AMF afin de s'assurer :
   - ↗ Du bon fonctionnement de la procédure / package d'installation ;
   - ↗ De la compatibilité avec l'environnement d'exécution de l'AMF et avec des données réelles dans l'environnement de maquettage ;
   - ↗ Validation de l'AMF de l'absence de régression avant déploiement.
3. Pilote sur un nombre réduit de composants afin de s'assurer de l'absence d'effet de bord dans l'environnement de production ;
   - ↗ Validation AMF du bon fonctionnement en pilote ;
4. Généralisation à l'ensemble des immeubles de l'AMF.

Le délai de test et d'observation pour chaque étape pourra être différent du délai d'observation des versions correctives ; il sera convenu entre les parties et consigné dans le cahier de recettes techniques.

5.2.4. Maintien en condition de sécurité (MCS)

Le titulaire doit effectuer les opérations de Maintien en Condition de Sécurité (MCS) sur le SI de Sûreté. Les opérations de MCS attendues sont décrites dans les sous-paragraphes suivants, et doivent être exécutées **selon une fréquence et des moyens proposés par le titulaire dans son offre et validés par l'AMF pendant la phase de démarrage.**

5.2.4.1. Principes et mesures de sécurité du SI de sûreté

L'état de l'art actuel en matière de cybersécurité et sûreté d'un SI de sûreté est notamment formalisé, comme exigé en §9, dans la publication ANSSI « *Sécurisation des systèmes de contrôle d'accès physique et vidéoprotection* »[8].

Ce guide, dont la première version date de l'année 2012, puis avec une mise à jour majeure en 2025, contient un très grand nombre de principes et mesures de cybersécurité et sûreté qui sont actuellement appliqués et doivent

[8] https://cyber.gouv.fr/publications/securisation-des-systemes-de-controle-dacces-physique-et-videoprotection

impérativement être maintenus sur le SI de sûreté de l'AMF : le titulaire doit appliquer et maintenir à tout instant les mesures actuellement appliquées et proposer à l'AMF un plan d'action pour celles qui ne sont pas encore appliquées.

Voici les grands principes phares actuellement appliqués :

- ☐ Les zones physiques au sein des bâtiments font l'objet d'une politique de sûreté, basée sur le besoin d'en connaitre (zone d'accès restreint, visiteur, collaborateur, maintenance etc.)
- ☐ Aucune connectivité sans-fil n'est déployée pour le SI de sûreté : tous les composants sont reliés entre eux au moyen de câbles
- ☐ Le SI de sûreté est physiquement (baies dédiées, câbles dédiés, composants dédiés) et logiquement isolé de tout autre SI de l'AMF et d'Internet
- ☐ Le SI de sûreté est cloisonné en zones réseaux aux besoins homogènes de sécurité, basées sur le principe du moindre privilège afin de réduire autant que possible la surface d'attaque des composants :
    - Le SI contient de multiples VLAN
    - Tous les composants périphériques telles que les caméras, lecteurs de badge, UTL etc. sont positionnés dans des **P**VLAN
    - Tous les flux entre VLAN (ou PVLAN) sont filtrés par un cluster de pare-feux déployés sous forme physiques. Ce cluster est formé par un pare-feu *actif* sur AMF1 couplé à un autre pare-feu *passif* sur AMF3.
- ☐ Tous les composants périmétriques sont authentifiés au moyen du protocole 802.1X sur le réseau
- ☐ Tous les flux de communication inter-composants sont et doivent être chiffrés :
    - Y compris pour le flux transitant via fibre noire entre les deux bâtiments AMF1 et AMF3, qui est chiffré au moyen du protocole MACSec (niveau 2 OSI) entre les piles de switchs cœur de réseau de chaque bâtiment
- ☐ Tout chiffrement, de flux ou de données, doit être réalisé aux moyens de protocoles et d'algorithmes considérés comme actuellement robustes par l'ANSSI[9]. Par exemple, concernant l'infrastructure de contrôle d'accès, tous les badges AMF sont basés sur le protocole DESFire EV2 ou EV3.
- ☐ Les patchs de sécurité des composants physiques et logiques doivent, conformément aux exigences décrites dans le CCCS, faire l'objet d'une veille par le titulaire, et de déploiement selon des exigences temporelles qui sont fonction de la criticité des vulnérabilités corrigées par ces patchs de sécurité (score CVSS)
- ☐ L'infrastructure de contrôle d'accès est basée sur la configuration dite « ANSSI type n°1 », à savoir que tous les lecteurs de badges sont « transparents » (non possession des secrets d'authentification [clés de chiffrement des badges]) et relaient les flux, via connexion filaire, à une UTL qualifiée par l'ANSSI qui elle dispose des secrets d'authentification
- ☐ Tous les composants, physiques et logiques, font l'objet d'un durcissement qui est documenté au sein de guides formalisés par le titulaire. Ces guides prennent en compte les consignes et exigences de l'AMF, et sont formellement validés par l'AMF. Ils doivent être appliqués à chaque intervention sur un composant (modification de configuration, remplacement de composant etc.).
- ☐ L'authentification des comptes utilisateurs, humains et technique (comptes de services), est réalisée par un annuaire Microsoft Active Directory
- ☐ Les serveurs et postes de travail sont inscrits dans le domaine mono-forêt Microsoft Active Directory déployé sur le SI de sûreté

[9] https://cyber.gouv.fr/publications/mecanismes-cryptographiques

- Les mises à jour des composants Microsoft sont réalisées par le composant WSUS, alimenté chaque mois de façon hors-ligne par le titulaire, via disque dur sécurisé AMF (cf. ci-dessous), avec les nouvelles mises à jour à appliquer
- L'horloge de chaque composant doit être synchronisée sur le serveur de temps GPS NTP déployé à cet effet au sein du SI de sûreté
- Les secrets (mots de passe, certificats etc.) doivent être consignés, de façon exclusive, et à tout instant maintenu à jour par le titulaire, dans un fichier KeePass
- Seule l'AMF détient les secrets des badges, à savoir les clés de chiffrement. Pour toute opération de configuration (injection) des secrets dans les UTL, le titulaire nécessite le concours de l'AMF pour fournir les clés de chiffrement
- Les logs/traces/journaux de tous les composants physiques et logiques sont déversés en temps réel sur le NAS, à des fins de supervision sécurité et débogage en cas d'incident sécurité ou technique
- Le titulaire utilise, pour les besoins de ce marché, un ou plusieurs disques durs externes fournis par l'AMF lors de transferts de fichiers entre composants
- Tous les composants impliqués dans le SI de sûreté doivent faire l'objet de courant ondulé : le titulaire doit informer l'AMF au plus vite lorsqu'il constate un défaut lié à l'onduleur fourni par l'AMF, ou un défaut de raccordement au courant ondulé pour les composants du SI de sûreté

5.2.4.2. Plan d'Assurance Sécurité (PAS) et Procédure d'Exploitation Sécurisée (PES)

Le titulaire doit proposer pendant la phase de démarrage, faire valider par l'AMF, appliquer et maintenir à jour tout au long du marché un Plan d'Assurance Sécurité (PAS) contextualisé à l'AMF, précisant les dispositions prises pour répondre aux exigences de sécurité physique et cybersécurité du SI de Sûreté de l'AMF formalisées dans le présent CCTP. La validation de l'AMF est systématiquement requise pour toute mise à jour du PAS, et chaque mise à jour doit être communiquée à l'AMF dans les meilleurs délais pour validation.

Il est précisé pour rappel que le PAS fourni par le titulaire à l'appui de son offre n'a pas pour objectif à ce stade de consolider toutes les exigences de sécurité formalisées dans le présent CCTP et ses annexes. Il est demandé pour permettre à l'AMF d'évaluer la maturité du titulaire en termes de structuration et formalisation de PAS.

Dès la notification et durant toute la durée du marché, ce sont les exigences du présent marché qui font foi : le PAS est attendu principalement afin de disposer d'un document consolidant les différentes exigences de sécurité (CCTP, CCCS etc.) du présent marché. Tout écart constaté au PAS est soumis à pénalités.

Les procédures permettant d'effectuer concrètement les opérations de MCS sont regroupées dans une Procédure d'Exploitation Sécurisée (PES). La rédaction de cette PES **est à la charge du Titulaire.** Elle est soumise à la validation de l'AMF. Chaque composant d'un SI de Sûreté doit faire l'objet d'une PES, ou du moins un chapitre dans la PES globale.

5.2.4.3. Revue documentaire

Le titulaire tiendra à jour la documentation relative au SI de la sûreté, en particulier dans les cas suivants :

- Remplacement de matériel ;
- Modification des règles de filtrage sur les équipements réseau ;
- Modification d'une configuration réseau ;
- Modification de configuration des équipements du SI de sûreté ;
- Modification d'architecture ;
- Ajout d'un nouveau type de composant

- ☐ Mode d'emplois nécessaire au fonctionnement opérationnel du SI de sûreté (création d'un badge, ajout d'un composant…).

Selon les cas, le titulaire tiendra à jour les documents suivants :

- ☐ Les fiches techniques des équipements (fiche de présentation, guide d'installation, guide utilisateur, guide administration etc.) ;
- ☐ Les plans et carnets de câblage et urbanisation des composants physiques (baies, switchs, routeurs etc.) ;
- ☐ Les documents de nomenclature et codification ;
- ☐ Les plans d'implantation des équipements ;
- ☐ L'inventaire matériel des équipements du SI de sûreté ; ceci inclut les équipements ou supports amovibles (CMDB) ;
- ☐ L'inventaire logiciel ; ceci inclut les versions des systèmes d'exploitation, la date de mise à jour et les clefs de licence (CMDB) ;
- ☐ Les documents d'analyse fonctionnelle des cas d'usage ;
- ☐ Les fiches d'autocontrôle ;
- ☐ Les guides de durcissement sécurité ;
- ☐ Le diagramme réseau, incluant le nom des machines ;
- ☐ Le plan d'adressage IP ;
- ☐ Le schéma filaire du réseau ;
- ☐ La liste des ports de tous les équipements (Switch, Serveur, UTL…) connectés incluant le nom de l'équipement de destination connecté ;
- ☐ La liste des comptes sur les machines, maintenu dans un fichier sécurisé KeePass
- ☐ La matrice des flux autorisés, comprenant a minima les éléments suivants :
    - Description du flux
    - IP/FQDN source
    - Port source
    - IP/FQDN de destination
    - Port de destination
    - Protocole
    - Service

Le titulaire effectue également la mise à jour, une (1) fois par an, des plans sur IHM (Interface Homme-Machine) et DOE (Dossier des Ouvrages exécutés), pour prendre en compte les éventuels changements de configuration des locaux.

De plus, lorsque ceci est nécessaire, le titulaire effectuera une mise à jour des documents notamment :

- ☐ La charte d'encodage des badges ;
- ☐ PES ;
- ☐ Politique de sauvegarde et restauration ;
- ☐ PCI/PRI (Plans de Continuité et de Reprise Informatique) ;
- ☐ CMDB (base de données de gestion de configuration) ;

- ☐ PAQ ;
- ☐ PAS ;
- ☐ Schémas d'architecture, représentant distinctement les vues physique, logique, et fonctionnelle ;
- ☐ Matrice des règles de filtrage (sur validation du RQ2SE) ;
- ☐ La liste des comptes et des mots de passe associés.

5.2.4.4. Mise à jour du fichier de la base de données de gestion de configuration (CMDB) du SI de Sureté

Au titre de la maintenance forfaitaire, le Titulaire doit mettre à jour mensuellement le fichier CMDB du SI de Sureté de l'AMF.

Le titulaire doit s'assurer que chaque équipement / licence de l'architecture dispose d'un contrat de maintenance / support en vigueur et à jour auprès du constructeur/éditeur.

Si tel n'est pas le cas, il doit proposer à minima 4 mois avant l'échéance de fin de contrat concerné, un devis de renouvellement à l'AMF. Les contrats de maintenance / support peuvent être d'une durée d'un an ou de trois ans.

Si le devis est validé, l'AMF établit un bon de commande.

Le fichier CMDB à date est détaillée en annexe du présent CCTP (annexe 2).

La mise à jour du fichier CMDB doit s'effectuer mensuellement et est proposée pour validation à chaque Cosec.

5.2.4.5. Mise à jour des systèmes d'exploitation

Le titulaire doit informer l'AMF des vulnérabilités et correctifs de sécurité lorsque ceux-ci sont publiés.

Le titulaire doit exécuter les opérations d'installation de ces correctifs sur les machines du SI, selon le schéma suivant :

- ☐ Pour les ordinateurs et serveurs, les correctifs de sécurité des systèmes d'exploitation doivent être installés aux fréquences suivantes :
  - 1 mois au maximum pour les vulnérabilités critiques ;
  - 3 mois pour les autres vulnérabilités.
- ☐ Pour les équipements réseaux et système (hyperviseur, switches, éventuels pares-feux, routeurs, sauvegarde), les nouvelles versions ou correctifs de sécurité doivent être installés aux fréquences suivantes :
  - 1 mois au maximum pour les vulnérabilités critiques ;
  - 3 mois pour les autres vulnérabilités.
- ☐ Pour les autres équipements (UTL, caméras, etc.), les nouvelles versions ou correctifs de sécurité doivent être installés à fréquence trimestrielle.

Les délais mentionnés ci-dessus débutent à compter de la date de diffusion des vulnérabilités au Bulletin du CERT.

Pour les autres machines (switches, éventuels pares-feux, caméras et UTL), le Titulaire installera les nouvelles versions lorsque des vulnérabilités critiques seront rendues publiques.

Le titulaire exécutera ces opérations en suivant la PES validée par l'AMF.

5.2.4.6. Gestion des antivirus

Le titulaire doit effectuer les opérations de mise à jour :

- ☐ **Des moteurs d'antivirus**, lorsque des nouvelles versions sont disponibles ; lorsqu'une nouvelle version est publiée, celle-ci doit être installée dans les délais suivants :

- 1 mois si cette version corrige une ou plusieurs vulnérabilités critiques ;
- 3 mois pour tout autre cas.

☐ **Des bases de définition d'antivirus, à fréquence hebdomadaire.**

Les délais mentionnés ci-dessus débutent à compter de la date de diffusion des vulnérabilités au Bulletin du CERT.

Par ailleurs, le titulaire effectuera une vérification des éventuelles alertes levées par les antivirus, et préviendra le RQ2SE en cas d'anomalie.

Le titulaire effectuera ces opérations en suivant la PES validée par l'AMF.

5.2.4.7. Mise à jour des autres applications

Le titulaire doit informer l'AMF lorsque de nouvelles versions des applicatifs (version majeure / nouvelle version) sont disponibles, ainsi qu'installer les mises à jour. Tout correctif relatif à des applicatifs métier ou à la montée de version aura préalablement été validé par l'éditeur.

Le titulaire effectuera ces opérations en suivant la PES validée par l'AMF.

5.2.4.8. Gestion des opérations de sauvegarde et restauration

Afin d'assurer la continuité et la reprise d'activité, le titulaire doit effectuer les opérations de sauvegarde et restauration prévus dans le **PCI/PRI** qu'il aura rédigé durant la phase de démarrage et que l'AMF aura validé.

Ces opérations concernent principalement les ordinateurs et serveurs, ainsi que la configuration des équipements réseau. Les fréquences sont définies dans le PCI/PRI.

Le titulaire effectuera ces opérations en suivant la PES validée par l'AMF.

Le titulaire doit réaliser, en présence de l'AMF, au moins un test du PCI/PRI par an : tout écart de résultat au PCI/PRI lié à un défaut imputable au titulaire doit être pris en charge sans surcoût par le titulaire.

5.2.4.9. Revue des règles de filtrage

Le titulaire ne peut en aucun cas modifier des règles de filtrage sans l'accord du RQ2SE. Tout changement doit faire l'objet d'une demande.

5.2.4.10. Revue des comptes et des droits d'accès

A fréquence mensuelle, le titulaire effectuera, sur chaque composant, une revue des comptes et droits présents.

La liste sera fournie à l'AMF mensuellement.

En particulier, le titulaire supprimera, après validation de l'AMF, les comptes inutiles et s'assurera que chaque compte ne dispose que des droits nécessaires au fonctionnement du système (principe du *moindre privilège*).

Cette exigence est applicable à l'ensemble des comptes systèmes ainsi qu'aux comptes des applications métier.

Les comptes ainsi que les mots de passe associés seront listés à l'aide du gestionnaire de mot de passe KeePass. Ce dernier sera installé sur un ordinateur de maintenance dédié au SI de sûreté, ainsi que sur une clé sécurisée.

Les comptes à forts privilèges feront l'objet d'un traitement spécial qui sera développé avec le RQ2SE.

5.2.4.11. Installation sécurisée de nouveau composant physique ou logique

Lorsqu'un nouvel équipement doit être installé, le titulaire appliquera la PES. Une fois le fonctionnement de l'équipement assuré, il doit durcir la sécurité de l'équipement afin de réduire sa surface d'attaque.

Pour cela, le titulaire procède, à sa charge, à un durcissement systématique de chaque composant impliqué dans le SI de Sûreté, et documente un guide de durcissement associé. Dans chaque guide de durcissement formalisé, le

titulaire indique sur quelles sources publiques il s'appuie en matière de durcissement et configuration sécurisé d'un composant, d'une technologie, ou d'un protocole, à titre d'exemple :

- ☐ Les guides de configuration fournis directement par les éditeurs / constructeurs / fabricants ;
- ☐ Les guides de sécurisation des agences de sécurité, nationale (ANSSI[10]) et internationales[11] ;
- ☐ Les guides de sécurisation des associations à but non-lucratif[12].

En particulier, le titulaire appliquera les mesures suivantes :

- ☐ Suppression des comptes inutiles ;
- ☐ Changement de mot de passe, et attribution de mot de passe forts ;
- ☐ Si applicable, activation du pare-feu logiciel ;
- ☐ Installation des mises à jour de sécurité ;
- ☐ Désactivation des protocoles d'administration non sécurisés ;
- ☐ Désinstallation de tout logiciel ou service inutile au fonctionnement attendu ;
- ☐ Configuration de la source de temps (NTP) ;
- ☐ Configuration du serveur de journaux d'évènements ;
- ☐ Désactivation des ports Ethernet non utilisés.

5.2.4.12. Mise au rebut de composant

Avant de mettre au rebut un composant physique ou logique, le titulaire dispose, documente, fait valider par l'AMF, et applique un processus de mise au rebut sécurisée, impliquant notamment des mécanismes d'effacement sécurisé conformes à l'état de l'art.

5.2.5. Assistance à la conduite et à l'exploitation des installations

Certaines prestations d'assistance à la conduite et à l'exploitation technique des installations entrent dans le cadre du forfait de maintenance.

Il s'agit de :

- ☐ Toutes les prestations d'administration et de supervision de l'architecture de Sûreté afin que cette dernière soit disponible 24/24 et 7/7 ;
- ☐ La vérification des espaces disques, RAM, CPU, Bande passante, etc. de l'architecture pour alerter l'AMF en cas de besoin (saturation, etc.) ;
- ☐ La vérification du bon fonctionnement de l'architecture haute disponibilité avec à minima un test du PRA par an ;
- ☐ La vérification de la bonne exécution des sauvegardes et la réalisation de tests de restauration ;

[10] https://cyber.gouv.fr/publications

[11] https://public.cyber.mil/stigs/downloads/
https://www.ncsc.gov.uk/collection/device-security-guidance
https://www.nsa.gov/Press-Room/Cybersecurity-Advisories-Guidance/
https://www.cyber.gov.au/resources-business-and-government/maintaining-devices-and-systems/system-hardening-and-administration/system-hardening

[12] https://www.cisecurity.org/cis-benchmarks

- ☐ Les mises à jour des OS, interface graphique, logiciel de sauvegarde, différents pilotes et progiciels spécifiques des serveurs et postes informatiques ;
- ☐ La consultation des historiques et l'impression ou l'extraction de rapports ;
- ☐ L'extraction des données vidéo sur demande de l'AMF ;
- ☐ L'assistance aux arrêts électriques réalisés une (1) fois par an sur les deux bâtiments (participation aux réunions de préparation, présence le jour de l'arrêt, accompagnement) ;
- ☐ Sur demande de l'AMF, la déclaration, l'activation ou la désactivation de zones, etc. ;
- ☐ Sur demande de l'AMF, la mise en ou hors fonction de systèmes ou parties de systèmes ;
- ☐ Sur demande de l'AMF, la création, suppression, désactivation de compte ainsi que le déblocage de compte, session et changement de mot de passe.
- ☐ Etc.

Des prestations d'assistance à la conduite et à l'exploitation n'entrent pas dans le cadre du forfait, notamment, sur demande de l'AMF, le nouveau paramétrage des systèmes, création de zone d'alarme, de détection, etc.

Il est à noter que la coordination des actions de paramétrage avec les exploitants se fera de manière systématique et autant de fois que nécessaire pour garantir l'obligation de résultats.

5.2.6. Gestion du stock de pièces détachées

Un stock de maintenance déjà présent sur site sera remis au Titulaire à la fin de phase de démarrage. Les pièces détachées qui le constituent sont mises à disposition du Titulaire par l'AMF.

Pour répondre à ses obligations de résultat, notamment de délai, et si les temps d'approvisionnement sont incompatibles avec les délais de réparation, le Titulaire doit proposer à l'AMF un dimensionnement du stock de maintenance des consommables et pièces détachées au terme de la phase de démarrage.

Ce dimensionnement doit être réalisé en cohérence avec les niveaux de sensibilité des équipements et systèmes et des délais d'intervention imposés dans le présent CCTP.

À la suite de la validation de l'AMF, la constitution de ce stock est à réaliser par le Titulaire ainsi que la réception et le stockage des éléments commandés. L'AMF est et restera le propriétaire du stock de maintenance.

En contrepartie le Titulaire, quand il est contraint d'utiliser le stock de pièces détachées pour assurer sa prestation, doit assurer la maintenance des pièces détachées, leur échange standard ou leur remplacement par du matériel neuf qu'il réintègre dans le stock dans les meilleurs délais. La gestion, le réapprovisionnement et le maintien de ce niveau de stock sont par conséquent entièrement à la charge du Titulaire.

A minima une (1) fois par an, ou en tant que de besoin lorsque de nouveaux équipements ont été installés, le Titulaire devra proposer à l'AMF la variation du stock qu'il juge nécessaire pour respecter ses obligations de résultat en fonction de l'historique de maintenance et de l'évolution quantitative des matériels maintenus.

La liste des pièces détachées disponibles (inventaire) est détaillée en annexe du présent CCTP (annexe 1).

5.2.6.1. Fourniture des pièces détachées

Pour la constitution et le réapprovisionnement du stock, les règles suivantes sont appliquées :

- Le Titulaire doit au titre du forfait la fourniture de toute pièce détachée dont le coût unitaire d'achat auprès du fournisseur, toute remise déduite, hors frais de port et avant application du coefficient du Titulaire, est inférieur ou égal à 500 € HT ;
- Pour les pièces détachées dont le coût unitaire d'achat auprès du fournisseur, toute remise déduite, est supérieur à 500 € HT, le Titulaire émet un devis conformément au BPU ou au coefficient de majoration pour les pièces ne faisant pas partie du BPU. Sur la base de ce devis l'AMF émet un bon de commande.

5.2.6.2. Inventaire des pièces détachées

Le Titulaire réalise un inventaire mensuel du stock des pièces détachées (à minima sur Tableau Excel) en fonction des mouvements d'entrées et de sorties de ses pièces, présenté en COPIL.

5.2.7. Planning global des maintenances

Au titre de la maintenance forfaitaire, le Titulaire doit mettre à jour le planning global des maintenances à réaliser au fur et à mesure de l'organisation et de l'exécution des prestations. Il doit être en mesure à tout moment de fournir à l'AMF un état précis de l'avancement des opérations planifiées.

Dans le cas d'un retard dans les opérations planifiées, le Titulaire doit en avertir les représentants de l'AMF.

Le planning global des maintenances est proposé pour validation à chaque Copil.

5.2.8. Rapport travaux à venir

Au titre de la maintenance forfaitaire, le Titulaire fournira semestriellement un rapport de préconisations sur :

- ☐ Les travaux (petits / conséquents) à prévoir ;
- ☐ Les matériels / logiciels à changer;
- ☐ Les améliorations possibles en terme d'organisation, d'outillage, etc.

Le titulaire présentera ce rapport lors du COPIL.

5.2.9. Travaux consécutifs aux vérifications techniques des organismes de contrôle

Le Titulaire s'engage à exécuter les travaux dus au titre du marché, nécessaires à la remise en ordre des anomalies constatées et mentionnées sur le rapport d'un organisme de contrôle mandaté par l'AMF, dans un délai maximal d'un (1) mois après transmission du rapport au Titulaire.

Si l'organisme de contrôle agréé préconise l'arrêt d'un appareil pour raison de sécurité, le Titulaire fait le nécessaire immédiatement pour remettre en état l'appareil.

Le Titulaire organise la planification de l'entretien préventif de façon à mettre, dans le cadre du marché, le personnel nécessaire à la disposition de l'organisme de contrôle et notamment pour préparer le matériel pour qu'il puisse être visité.

Il est également tenu de signaler à l'AMF les contrôles et mises en conformité qui lui semble nécessaires en complément de ceux qui lui sont indiqués par l'organisme de contrôle.

5.2.10. Interventions de tiers

Sont définies comme tiers les sociétés spécialisées, les organismes de contrôle et les services internes de l'AMF.

L'AMF se réserve le droit de faire effectuer, dans toutes les parties du site, les contrôles qu'il jugera utiles par tout tiers ou organisme spécialisé en la matière.

Le Titulaire met, dans le cadre du marché, le personnel et le matériel requis à la disposition des services internes de l'AMF ou des sociétés ou organismes pour qu'ils remplissent les missions qui leur sont confiées.

Le Titulaire en est informé par les représentants de l'AMF avant les interventions, le plus en amont possible.

Les interventions du personnel mis à la disposition de ces sociétés ou organismes sont incluses dans le marché.

Le Titulaire effectue aussi en collaboration avec les exploitants ou mainteneurs des autres corps d'état tels que la Sûreté, la menuiserie, la gestion technique centralisée, les installations électriques, les installations de climatisation et de désenfumage, etc. les contrôles nécessitant sa présence.

Certaines visites sont susceptibles d'entraîner des travaux de préparation (avant la visite) et de remise en état (après la visite). L'ensemble de ces prestations est compris dans les prestations forfaitaires de la maintenance.

5.2.11. Gouvernance à assurer lors de la maintenance forfaitaire

Au titre de la maintenance forfaitaire, le Titulaire doit assurer la gouvernance telle que décrite ci-dessous :

5.2.11.1. COPIL

Le comité de pilotage se réunit mensuellement ou sur demande expresse d'une des deux parties.

Les participants au comité sont :

- AMF – Direction Ressources, Support et Transformation (présence facultative)
- AMF – Directeur Administratif et Financière (présence facultative)
- AMF – Directeur Cyber sécurité, Sûreté et Risques (présence facultative)
- AMF – Responsable Pôle services et environnements de travail (présence facultative)
- AMF – Responsable Qualité, Sûreté, Sécurité et Environnement
- AMF – Autres (A la demande AMF ou du titulaire)
- AMF – Membre de la DG (présence facultative)
- Titulaire – Responsable client (présence obligatoire)
- Titulaire – Responsable de site (présence obligatoire)
- Titulaire – Autres (A la demande AMF ou du titulaire)
- Titulaire – Membre de la DG du titulaire (présence facultative)

Instances	Titulaire	AMF	Périodicité	Livrables
COPIL à organiser 5 jours après la fin de chaque mois	R	A	Mensuellement	Support de COPIL (1) à fournir par « R » à « A » 5 jours ouvrés avant le COPIL. Compte-rendu du COPIL (2) à fournir par « R » à « A » 5 jours ouvrés après le COPIL

Définition des rôles :

- R : Réalise l'activité.
- A : A l'autorité pour approuver le travail de R.

(1) Le support du Copil doit comprendre *a minima* :

- ☐ Le rapport d'activité (actions opérationnelles réalisées) de la période écoulée ;
- ☐ La météo de la prestation sur la période écoulée ;
- ☐ Les indicateurs type pour ce type de prestation mais à minima :
  - Le nombre d'incidents/demandes ainsi que leur criticité sur la période ;
  - Le nombre de rapports d'incidents/demandes transmis sur la période ;
  - Pour chaque rapport d'incident/demande le délai de transmission post GTR ;
  - Le nombre et les types de tickets ouverts sur la période ;
  - Le taux de disponibilité de l'infrastructure Sureté sur la période écoulée ;
  - Nombre d'opérations de maintenance réalisée sur la période en cours ;
  - Nombre de bons de commande en cours ;
  - Pour chaque incident/demande GTR et GTI constatés ;
- ☐ L'analyse de chaque indicateur et les préconisations associées ;
- ☐ Un tableau des mesures des indicateurs sur les douze derniers mois glissants avec comparaison entre chaque mois et tendance ;
- ☐ Un état financier (suivi des montants de la MCO et des bons de commande) ;
- ☐ Un état sur les pénalités applicables ;
- ☐ Un état des lieux des incidents en cours ;
- ☐ Un état des lieux des demandes par priorité en cours formulées par l'AMF ;
- ☐ Les axes d'amélioration de la prestation (Plan progrès) ;
- ☐ Fichier inventaire du stock de pièces détachés ;
- ☐ Planning global des maintenances ;
- ☐ Une proposition de mise à jour du PAQ si mise à jour.

(2) Le compte rendu du comité de pilotage doit faire apparaitre les pénalités applicables (actées lors du comité de pilotage vu supra). Le titulaire est en charge de l'organisation et de la planification des comités de pilotage.

Lorsque celui-ci est réalisé par visioconférence, le titulaire s'engage à utiliser la solution utilisée en interne par l'AMF. Certaines instances peuvent être annulées si nécessaire, sous réserve de l'accord des deux parties. L'adaptation des périodicités, la modification des comités de pilotage ne pourra se faire que sur accord de l'AMF.

Livrables :

- Fichier stock pièces détachés

Excel	Fichier inventaire mis à jour

- Support du comité de pilotage (COPIL)

Power Point	Présentation des éléments mentionnés ci-dessus

- Compte-rendu du comité de pilotage (COPIL)

Word	Synthèse du comité de pilotage.

5.2.11.2. COSEC

Le comité de sécurité se réunit mensuellement ou sur demande expresse d'une des deux parties.

Les participants au comité sont :

- AMF – Direction Ressources, Support et Transformation (présence facultative)
- AMF – Directeur Administratif et Financière (présence facultative)
- AMF – Directeur Cyber sécurité, Sûreté et Résilience
- AMF – Responsable Pôle services et environnements de travail (présence facultative)
- AMF – Responsable Qualité, Sûreté, Sécurité et Environnement
- AMF – Membre de la DG (présence facultative)
- AMF – Autres (A la demande AMF ou du titulaire)
- Titulaire – Responsable client (présence obligatoire)
- Titulaire – Responsable de site (présence obligatoire)
- Titulaire – Autres (A la demande AMF ou du titulaire)

Instances	Titulaire	AMF	Périodicité	Livrables
COSEC à organiser 5 jours après la fin de chaque mois	R	A	Mensuellement	Support de COSEC (1) et fichier CMDB (mis à jour) à fournir par « R » à « A » 5 jours ouvrés avant le COSEC. Compte-rendu du COSEC (2) à fournir par « R » à « A » 5 jours ouvrés après le COSEC

Définition des rôles :

- R : Réalise l'activité.
- A : A l'autorité pour approuver le travail de R.

(1) Le support du Cosec doit comprendre *a minima* :

- ☐ Un état des lieux des demandes sécurité par priorité en cours formulées par l'AMF ;
- ☐ Les projets et évolutions ;
- ☐ Un état des lieux des incidents de sécurité physique (par ex. portes verrouillées/déverrouillées qui ne devraient pas l'être, incidents de contrôle d'accès) et cybersécurité du SI de sûreté ;
- ☐ Les indicateurs type pour ce type de prestation mais à minima :
  - Le nombre d'incidents sécurité ainsi que leur criticité sur la période ;
  - Le nombre d'équipement / logiciel de disposant pas de contrats de support/maintenance ;
  - Le nombre de version logicielle plus supportée par l'éditeur ;
- ☐ L'analyse de chaque indicateur et les préconisations associées ;
- ☐ Un tableau des mesures des indicateurs sur les douze derniers mois glissants avec comparaison entre chaque mois et tendance ;

- ☐ Le suivi des vulnérabilités ;
- ☐ La revue des comptes et des accès (habilitations) ;
- ☐ La météo des versions des composants basée sur le fichier CMDB à jour ;
- ☐ La revue des antivirus ;
- ☐ La météo des contrats et licences des composants ;
- ☐ Le suivi des certificats X.509 déployés (nom de la famille composant couvert, type de la famille, date d'expiration des certificats, nombre de certificats) ;
- ☐ La météo des mises à jour Windows (désignation du composant, nom de la machine, version OS, date de dernière mise à jour sécurité appliquée) ;
- ☐ La météo des sauvegardes ;
- ☐ La météo des tests de restaurations ;
- ☐ Le suivi des métriques (stockage, RAM, CPU) ;
- ☐ Le suivi des dérogations et mesures temporaires ;
- ☐ Le taux de disponibilité ;
- ☐ Les axes d'amélioration de la prestation (Plan progrès). Les projets, évolutions, actions, revues, tests en cours par le titulaire et pouvant impacter l'AMF ;
- ☐ Fichier CMDB mis à jour ;
- ☐ Une proposition de mise à jour du PAS si mise à jour ;
- ☐ Une proposition de mise à jour du plan de sauvegarde si mise à jour ;
- ☐ Une proposition de mise à jour du Plan de continuité et reprise d'activité (PCA/PRA) si mise à jour.

(2) Le titulaire est en charge de l'organisation et de la planification des comités de sécurité. Lorsque celui-ci est réalisé par visioconférence, le titulaire s'engage à utiliser la solution utilisée en interne par l'AMF. Certaines instances peuvent être annulées si nécessaire, sous réserve de l'accord des deux parties. L'adaptation des périodicités, la modification des comités de pilotage ne pourra se faire que sur accord de l'AMF.

Livrables :

- Fichier CMDB

Excel	Fichier CMDB mis à jour

- Support du comité de sécurité (COSEC)

Power Point	Présentation des éléments mentionnés ci-dessus

- Compte-rendu du comité de pilotage (COSEC)

Word	Synthèse du comité de sécurité.

5.2.12. Horaires et délais d'intervention

Le Titulaire doit maintenir en permanence, vingt-quatre heures sur vingt-quatre (24h/24h) et sept jours sur sept (7j/7j), en parfait état de fonctionnement et de performance des installations dont il a la charge.

5.2.12.1. Jours et heures de présence minimum obligatoire

Pour respecter son obligation de résultat, le Titulaire n'est tenu à aucune présence minimale à assurer sur les immeubles. Les interventions de maintenance préventives sont en principe réalisées durant les heures ouvrées. Le Titulaire peut demander l'autorisation à l'AMF pour exécuter des prestations en dehors des heures ouvrées notamment pour respecter les délais contractuels.

Il faut noter que des coupures régulières de l'alimentation électrique pour maintenance sont réalisées une à deux (2) fois par an et par bâtiment (ces coupures sont réalisées généralement un samedi, dimanche ou un jour férié). Ces prestations sont intégrées dans le forfait sur la base d'un arrêt technique par bâtiment, prévoyant la présence du chef de site pendant onze (11) heures (généralement de 06h00 à 17h00) un samedi, dimanche ou un jour férié. Précédemment, et lors de la coupure et de la remise sous tension, le Titulaire détache sur le site les moyens nécessaires aux contrôles du bon fonctionnement des installations secourues ou non. Ces moyens sont inclus dans le montant du forfait.

5.2.12.2. Astreinte

En dehors des heures et jours ouvrés, et pour assurer une maintenance corrective, l'AMF doit pouvoir joindre à tout moment et ce quelle que soit l'heure ou le jour, toute personne qualifiée, ayant la connaissance du site et des installations ; à défaut et en second lieu un responsable du Titulaire doit pouvoir être joint et enfin, et uniquement en cas d'urgence et de force majeure et parce que le contact n'a pu être établi, un troisième niveau hiérarchique (pour cet ultime niveau les coordonnées peuvent être maintenues sous enveloppe cachetée sous la responsabilité d'un nombre limité de représentants de l'AMF).

Sur simple appel téléphonique et/ou mail et/ou demande d'intervention, le Titulaire doit dépêcher une personne d'astreinte disposant des droits d'accès et connaissant le site et les installations capable de pallier la défaillance ou, en cas d'impossibilité de remise en service normal rapide, de prendre les mesures conservatoires et d'activer les modes dégradés de fonctionnement.

Les interventions en période d'astreinte sont assurées forfaitairement ainsi que la mise à disposition des moyens de communication fiables et de déplacement du service d'astreinte.

5.2.12.3. Garantie du temps d'intervention (GTI) et du temps de rétablissement (GTR)

Le délai d'intervention est le délai compris entre le moment où l'incident/demande est signalé au Titulaire par tout moyen et le moment où l'intervention sur site commence.

Le délai de rétablissement est le temps imparti entre le moment où l'incident/demande est signalée au Titulaire le moment où l'incident est définitivement terminé.

Incident/Demande	GTI	GTR
Critique	2 heures calendaires	4 heures calendaires
Bloquant	4 heures calendaires	8 heures calendaires
Non bloquant	1 jour calendaire	5 jours calendaires

Dans le cas où l'incident/demande nécessiterait des réparations qui justifieraient un délai complémentaire lié à des travaux d'autres corps d'état, et sur demande du Titulaire auprès de l'AMF, le délai pourra être prolongé avec l'accord de l'AMF. La coordination éventuelle et l'organisation voire le suivi des interventions d'autres corps d'état relève des missions du Titulaire.

L'ensemble des incidents/demandes seront saisis par l'AMF dans l'outil de GMAO. Pour chaque incident il sera indiqué la criticité (sans que le titulaire puisse modifier le niveau de criticité retenu par l'AMF) et la date/heure de l'incident ou la demande. Les délais GTR/GTI seront calculés en fonction de cette date et heure.

Quelles qu'en soient les raisons, si exceptionnellement le Titulaire ne pouvait satisfaire aux délais prévus, il est tenu d'en informer immédiatement les représentants de l'AMF afin que ces derniers puissent prendre les dispositions nécessaires (mise en place de personnel de sécurité ou de surveillance, etc.).

Le fait d'avoir informé préalablement l'AMF du retard ne saurait faire obstacle à l'application éventuelle des pénalités de retard.

Le Titulaire établit pour chaque incident/demande un rapport d'incident comportant a minima les éléments suivants :

- ☐ La date de survenance de l'incident ainsi que la chronologie des événements ;
- ☐ La nature de l'incident/demande ;
- ☐ Le périmètre affecté ;
- ☐ Le ou les services et/fonctions impactés ;
- ☐ L'impact de l'incident, sur les personnes et les biens ;
- ☐ La méthode et chronologie de détection ;

- Le résultat des investigations menées ;
- Le plan d'action prévu pour remédier à l'incident/demande ;
- Les mesures prises pour éviter qu'un incident similaire se reproduise à l'avenir ;
- Toute autre information pertinente en lien avec l'incident.
- Une proposition de mise à jour du plan de sauvegarde si mise à jour.

Le rapport d'incident est transmis à l'AMF 48h au plus tard après la résolution de l'incident.

5.3. NATURE DES OBLIGATIONS

Le Titulaire s'engage à prendre en charge la maintenance des installations incluant la main-d'œuvre et la fourniture de pièces dans les conditions et selon les obligations figurant au marché.

La prise en charge des prestations définies dans le marché constitue, selon les cas, une obligation de moyens ou une résultat.

Obligation de moyens :

- Optimiser la maintenance préventive ou préventive conditionnelle et la maintenance corrective de façon à assurer la qualité de service aux utilisateurs et la performance des installations pour les exploitants ;
- Limiter les gênes et ne pas entraver l'exploitation normale du site.

Obligation de résultat :

- Garantir en permanence les performances et le niveau de Sûreté des personnes, des biens et des informations tels que définis par l'AMF au moyen du maintien des équipements et des systèmes de Sûreté et de son architecture ;
- Garantir les modes de fonctionnement dégradés ;
- Maintenir le niveau de performance et de durabilité des équipements et des systèmes ;
- Respecter les délais prévus au marché : de remise des livrables, de présence, d'intervention, de dépannage et de remise en état. L'AMF sera notamment très attentive au respect des délais de GTI et de GTR ;
- Diminuer constamment les quantités d'anomalies relevées par les organismes de contrôle.

Le Titulaire prend en charge la fourniture de pièces dans les conditions et selon les obligations figurant au marché, la main-d'œuvre et la mise à disposition temporaire de matériels.

Il appartient au Titulaire de proposer et d'adapter les moyens qu'il met en œuvre pour répondre à ses obligations.

Notamment, il appartient au Titulaire de dimensionner les équipes sur sites de sorte à pouvoir réaliser les prestations définies dans le marché et atteindre son obligation de résultat.

5.4. TELEMAINTENANCE (CLAUSE DE REEXAMEN)

La télémaintenance n'est pas autorisée pour réaliser les prestations de maintenance.

Toutefois, l'AMF se laisse la possibilité d'introduire une part de télémaintenance dans l'exécution des prestations en cours de marché, par l'intermédiaire d'une clause de réexamen, laquelle donnera lieu à la conclusion d'un avenant, conformément à l'article 18.2 du CCAP.

En cas d'activation de la clause de réexamen, le dispositif de télémaintenance mis en place devra respecter les principes suivants :

Principes généraux

L'architecture de télémaintenance devra garantir un niveau de sécurité adapté aux enjeux de sûreté et de cybersécurité des installations concernées.

Elle devra être conçue et mise en œuvre conformément aux exigences réglementaires applicables, aux principes de la directive NIS2, ainsi qu'aux recommandations et bonnes pratiques de l'ANSSI, notamment en matière de segmentation des réseaux, de contrôle des accès, de traçabilité, de supervision et de protection des comptes à privilèges.

Le titulaire devra fournir, avant toute mise en œuvre, une description détaillée de l'architecture de télémaintenance, précisant notamment les flux, les équipements de sécurité, les mécanismes d'authentification, les dispositifs de journalisation et les mesures de protection mises en œuvre.

Toute évolution de cette architecture devra être préalablement soumise à validation du pouvoir adjudicateur.

Séparation et segmentation des réseaux

L'architecture devra assurer une séparation stricte des différents environnements, et notamment :

- le réseau IT, destiné aux systèmes bureautiques et informatiques ;
- le réseau OT, destiné aux systèmes techniques et de sûreté ;
- une DMZ, dédiée aux échanges avec les réseaux externes et aux accès de télémaintenance.

Aucune communication directe entre le réseau OT et Internet ne devra être autorisée.

Les accès entre les différentes zones de sécurité devront obligatoirement transiter par les équipements de sécurité prévus à cet effet et être limités aux seuls flux strictement nécessaires au fonctionnement et à la maintenance des équipements concernés.

Cloisonnement et filtrage des communications

Le titulaire devra mettre en œuvre une politique de segmentation et de filtrage permettant de limiter les possibilités de propagation d'une compromission d'un système à un autre.

Les différentes zones réseau devront être séparées par des pare-feu configurés selon une politique de sécurité restrictive.

Par défaut, tout flux devra être interdit, sauf lorsqu'il est explicitement autorisé et justifié par un besoin fonctionnel ou de maintenance.

Les règles de filtrage devront être documentées et préciser au minimum :

- la source ;
- la destination ;
- le protocole ;
- le port utilisé ;
- le sens de communication ;
- la justification du flux ;
- la durée de validité, lorsqu'il s'agit d'un accès temporaire.

Les systèmes critiques devront, lorsque cela est techniquement possible, être isolés au moyen de VLAN ou de mécanismes de segmentation équivalents.

Accès distant et télémaintenance

Tout accès distant aux systèmes de sûreté ou aux équipements techniques devra être réalisé au travers d'un bastion d'administration sécurisé, constituant le point d'entrée unique pour les opérations de télémaintenance.

Les accès directs depuis Internet vers les équipements du réseau OT seront interdits.

Les connexions externes devront obligatoirement utiliser un canal de communication chiffré, reposant sur des protocoles et algorithmes cryptographiques reconnus et maintenus à jour.

L'utilisation d'un VPN IPsec ou TLS, avec un niveau de sécurité conforme aux recommandations de l'ANSSI et aux standards cryptographiques en vigueur, sera exigée.

Les mécanismes cryptographiques obsolètes ou présentant des vulnérabilités connues devront être proscrits.

Authentification forte

Tout accès distant devra faire l'objet d'une authentification forte multifacteur (MFA).

L'authentification devra reposer sur au minimum deux facteurs d'authentification distincts, dont, selon la solution retenue :

- un facteur de connaissance ;
- un facteur de possession, tel qu'un certificat numérique ou un dispositif d'authentification à usage unique ;
- et/ou un facteur biométrique lorsque celui-ci est autorisé et techniquement pertinent.

L'utilisation de comptes génériques ou partagés pour les opérations d'administration ou de télémaintenance devra être interdite.

Chaque intervenant devra disposer d'un compte nominatif permettant d'assurer son identification et sa traçabilité.

Gestion des comptes à privilèges

Les comptes disposant de privilèges d'administration devront être gérés au moyen d'une solution de type PAM (Privileged Access Management) ou d'un dispositif offrant des fonctionnalités de sécurité équivalentes.

Les droits devront être attribués selon le principe du moindre privilège et limités aux seuls besoins nécessaires à l'exécution des opérations autorisées.

Lorsque les fonctionnalités le permettent, les droits d'administration devront être attribués de manière temporaire et révoqués automatiquement à l'issue de l'intervention.

Le titulaire devra également mettre en œuvre des mécanismes permettant de contrôler et de tracer l'utilisation des comptes à privilèges.

Gestion des sessions

Les sessions de télémaintenance devront être limitées dans le temps.

Une déconnexion automatique devra être appliquée après une période d'inactivité n'excédant pas 10 minutes, sauf justification technique particulière validée préalablement par le pouvoir adjudicateur.

La fermeture d'une session devra entraîner la suppression ou la révocation des droits temporaires accordés pour l'intervention.

Lorsque cela est techniquement possible, les sessions d'administration devront pouvoir être enregistrées afin de permettre leur analyse a posteriori.

Supervision et détection

L'architecture devra permettre la supervision des accès et la détection des événements de sécurité.

Les équipements et systèmes concernés devront transmettre leurs journaux de sécurité vers une solution centralisée de type SIEM (Security Information and Event Management) ou vers une solution offrant des fonctionnalités équivalentes.

Lorsque cela est techniquement pertinent, des mécanismes de détection et de prévention des intrusions de type IDS/IPS devront être mis en œuvre sur les points d'interconnexion appropriés.

La supervision devra notamment permettre de détecter :

- les tentatives d'accès non autorisées ;
- les échecs répétés d'authentification ;
- les connexions inhabituelles ;
- l'utilisation de comptes à privilèges ;
- les modifications de configuration ;

- les ouvertures de flux inhabituelles ;
- les anomalies susceptibles de caractériser une compromission.

Journalisation et traçabilité

L'ensemble des opérations de télémaintenance devra faire l'objet d'une journalisation permettant d'identifier précisément l'intervenant, l'action réalisée et le contexte de l'intervention.

Les journaux devront permettre, a minima, de déterminer :

- qui est intervenu ;
- quoi a été réalisé ;
- quand l'opération a été effectuée ;
- depuis où la connexion a été établie ;
- sur quel équipement ou système l'intervention a porté ;
- et, lorsque cela est applicable, pour quel motif ou dans le cadre de quelle demande d'intervention.

Les journaux devront être protégés contre toute modification ou suppression non autorisée.

Ils devront être horodatés de manière fiable et synchronisés sur une source de temps de référence.

Conservation des journaux

Les journaux de sécurité et de télémaintenance devront être conservés pendant une durée permettant d'assurer la détection, l'analyse et l'investigation des incidents de cybersécurité.

Sauf exigence réglementaire plus contraignante applicable au système concerné, la durée minimale de conservation sera fixée à 12 mois.

Lorsque des exigences réglementaires, contractuelles ou de classifications particulières s'appliquent, la durée de conservation devra être adaptée en conséquence.

Le titulaire devra préciser dans son offre :

- la durée de conservation proposée ;
- le dispositif de stockage utilisé ;
- les mesures de protection contre l'altération ou la suppression des journaux ;
- les modalités permettant leur extraction et leur transmission au pouvoir adjudicateur en cas d'incident.

Sécurisation des opérations de télémaintenance

Toute opération de télémaintenance devra être réalisée dans le respect du principe du moindre privilège et être limitée aux équipements strictement nécessaires.

Les accès devront, lorsque cela est possible, être :

- préalablement autorisés ;
- limités dans le temps ;
- limités au périmètre technique concerné ;
- associés à un intervenant nominativement identifié ;
- tracés dans les journaux de sécurité.

Le titulaire devra être en mesure de fournir, sur demande du pouvoir adjudicateur, l'historique des connexions et opérations réalisées dans le cadre de la télémaintenance.

Aucun accès permanent et non justifié aux systèmes de sûreté ou aux systèmes techniques ne pourra être maintenu.

Validation préalable de l'architecture

Avant toute mise en production, le titulaire devra transmettre au pouvoir adjudicateur un dossier d'architecture technique et de sécurité comprenant au minimum :

- un schéma d'architecture réseau ;
- la description des différentes zones de sécurité ;
- les flux autorisés entre les zones ;

- les règles de filtrage ;
- les mécanismes d'authentification ;
- les dispositifs de chiffrement ;
- la gestion des comptes à privilèges ;
- les mécanismes de journalisation ;
- les dispositifs de supervision et de détection ;
- les durées de conservation des journaux ;
- les mesures prévues en cas de compromission d'un compte ou d'un équipement.

La mise en œuvre de la solution de télémaintenance sera subordonnée à la validation préalable de cette architecture par l'AMF.

Toute modification ultérieure susceptible d'avoir un impact sur le niveau de sécurité devra faire l'objet d'une validation préalable.

6. DESCRIPTIF DES PRESTATIONS A BONS DE COMMANDE

6.1. GENERALITES

Les prestations définies au présent article s'exécutent par bons de commande émis au fur et à mesure des besoins.

Afin de permettre aux représentants de l'AMF un contrôle des prestations à bon de commande du Titulaire, chaque prestation à bon de commande à l'exception de celles prévues à l'article 6.2 ci-dessous, sera préalablement cadrée.

Ainsi, avant toute opération, l'AMF se rapprochera du Titulaire afin de connaître sa meilleure proposition en termes de prestation, de fourniture, d'intervenant, et de planification. Cette proposition détaillée devra se conformer aux taux horaires et aux coefficients de majoration sur lesquels le Titulaire s'est engagé au Bordereau des Prix Unitaires (BPU). La proposition ainsi établie constituera le cadre de la prestation commandée.

Notamment, le délai de réalisation de la prestation attendue sera indiqué dans le bon de commande. En cas de non-respect de ce délai, le titulaire encourt l'application des pénalités prévues à l'article 17.5 du CCAP.

Dans tous les cas, le Titulaire devra planifier l'opération dans le respect des règles, normes et réglementations citées dans le présent CCTP qu'il s'agisse de sécurité, d'hygiène, de comportement, de circulation et toutes autres spécifications en rapport avec la correcte exécution des prestations à bon de commande.

Le Titulaire dispose d'un délai maximum de cinq (5) jours ouvrés à compter de la demande de l'AMF, pour réaliser et transmettre une proposition détaillée correspondant à la prestation demandée.

La mise à jour des plans sur IHM et DOE à l'issue de prestations à bon de commande devra être systématique et sera chiffrée séparément par le Titulaire dans sa proposition détaillée s'il est nécessaire d'en réaliser au-delà de celle prévue au titre du marché.

6.2. DIMENSIONNEMENT DU STOCK DE MAINTENANCE

Comme indiqué à l'article 5.2.6 ci-dessus, pour les pièces détachées dont le coût unitaire d'achat auprès du fournisseur, toute remise déduite, est supérieur à 500 € HT, le Titulaire émet un devis conformément au BPU ou au coefficient de majoration pour les pièces ne faisant pas partie du BPU.

Sur la base de ce devis l'AMF émet un bon de commande.

6.3. ASSISTANCE A LA CONDUITE ET A L'EXPLOITATION TECHNIQUE

Les prestations d'assistance à la conduite et à l'exploitation technique, à bons de commande, pourront être les suivantes :

- ☐ Sur demande de l'AMF, le nouveau paramétrage des systèmes, création de zone d'alarme, de détection, de catégorie, de profils d'accès, de plage horaire, d'enregistrement vidéo, etc. ;
- ☐ Sur demande de l'AMF, la déclaration, l'activation ou la désactivation de zones, etc. ;
- ☐ Sur demande de l'AMF, la mise en ou hors fonction de systèmes ou parties de systèmes ;
- ☐ etc.

Il est à noter que la coordination des actions de paramétrage avec les exploitants se fera de manière systématique et autant de fois que nécessaire pour garantir l'obligation de résultats.

6.4. MAINTENANCE LOGICIELLE EVOLUTIVE

La maintenance évolutive correspond à la prise en compte de nouveaux besoins fonctionnels à l'initiative de l'AMF notamment ajout de fonctions, nouvelles règles de gestion, prise en compte des évolutions d'autres applications, extension du champ d'automatisation, changement de l'organisation, évolution de la réglementation, amélioration fonctionnelle, y compris formations des opérateurs, des gestionnaires et des administrateurs.

Elle exclut l'upgrade de version majeur ou changement de version imposé notamment par les éditeurs (fin de support d'une version ou changement de version par exemple), intégrée à la maintenance adaptative décrite à l'article 5.2.3.2 du présent CCTP.

6.5. EXTENSION OU MODIFICATION DES INSTALLATIONS DE SÛRETE

Travaux :

L'AMF se réserve le droit de faire effectuer toute extension ou modification importante d'installation par le Titulaire ou tout sous-traitant qualifié de son choix, après validation de l'AMF.

Cela peut notamment intervenir en cas de migration du système vers la solution Genetec Security Center.

L'AMF en avertit le Titulaire au moins un (1) mois à l'avance.

Durant une période de deux (2) semaines, le Titulaire peut demander des compléments d'informations et formuler d'éventuelles recommandations/objections relatives à ces transformations.

L'AMF commande ensuite les extensions ou modifications convenues au titulaire.

Le Titulaire ne peut effectuer aucune modification de son fait, sans l'accord écrit des représentants de l'AMF, sous forme d'ordre d'exécution qui fixe la date et le délai de l'intervention.

Durant les travaux, le Titulaire prend toutes les dispositions pour que le fonctionnement des installations ne soit pas perturbé. Il doit obligatoirement faire part, par écrit, de tout risque d'empêchement occasionné par ces travaux ou une mise à niveau du SI sûreté. En dehors de cette déclaration préalable, il est tenu pour responsable du manquement de fonctionnement éventuel.

Il a toute faculté, tant au cours des travaux ou de la mise à niveau, qu'au moment de leurs réceptions, auxquelles il est tenu d'assister, de signaler tout point apparaissant comme anomalie dans l'installation.

Ces constatations doivent être présentées dans le plus court délai par écrit, sous forme d'un rapport standardisé. L'AMF reste seule juge de la suite à donner dans le cadre de sa responsabilité.

À l'issue de chacune des réceptions, un procès-verbal de prise en charge est dressé contradictoirement. Ce procès-verbal marque l'obligation faite du Titulaire d'assurer à dater du jour de la réception, la maintenance des installations en cause, au même titre que celles qui font l'objet du marché dans sa forme initiale.

Maintenance (clause de réexamen) :

Dans le cas d'évolution du périmètre de maintenance consécutive aux travaux, un ajustement de la maintenance forfaitaire pourra être négocié entre les parties et, en cas d'accord, donner lieu à la conclusion d'un avenant conformément à l'article 18.3 du CCAP.

Si les discussions ne permettent pas d'aboutir à un accord, créant de fait une situation d'absence de maintenance d'une partie du périmètre, l'AMF se réservera la possibilité de résilier le marché.

6.6. EXIGENCES DE CYBERSECURITE

Les prestations à bon de commande ne doivent pas entrer en contradiction avec les principes et exigences de cybersécurité définis dans le CCCS.

Tout choix d'architecture et de conception doit être formellement validé par l'AMF, de même que les livrables projet.

6.7. REVERSIBILITE

La réversibilité donne lieu à l'émission d'un bon de commande par l'AMF sur la base du prix figurant dans le bordereau de prix.

La réversibilité intervient en fin de marché, y compris en cas de résiliation.

Elle est d'une durée de 3 mois.

Dès réception du bon de commande, le titulaire nomme un responsable en charge de la mise en œuvre des prestations de réversibilité qui organisera sous 5 jours, après réception du bon de commande de cette phase, une réunion de démarrage de cette dernière.

Au titre de la réversibilité, le titulaire s'engage a minima à :

- Assurer, y compris pendant la réversibilité, les niveaux de service prévus au marché, jusqu'au transfert de la responsabilité des prestations à l'AMF ou à un futur titulaire ;
- Le cas échéant, mener les diligences nécessaires à la bascule des services fournis à l'AMF vers un autre fournisseur en minimisant les interruptions de service éventuelles et en maintenant pendant cette période de réversibilité des prix identiques à ceux des prestations fournies au titre du marché ;
- Constituer parmi ses collaborateurs ayant participé aux prestations du marché une équipe suffisante pour exécuter le processus de réversibilité (l'AMF mettra en place, symétriquement et dans le même temps, une équipe suffisante pour la phase de réversibilité) ;
- Assurer un transfert de compétences auprès du titulaire du futur marché avant la date d'expiration du présent marché, qu'il ait fait ou non l'objet d'une ou plusieurs reconductions. Ce transfert de compétences sera assuré par un technicien compétent dont le niveau de qualification permettra de réaliser le transfert sur l'ensemble des prestations objet du présent marché, dédié à cette mission, en plus de l'effectif habituel. Il sera réputé bien connaître les locaux, les installations et l'ensemble des procédures de l'AMF. Le Titulaire sortant s'engage à communiquer aux personnels du Titulaire entrant chargés des prestations les informations nécessaires à la reprise du marché. Cette information doit en particulier comprendre la communication de tous les plans, documents et instructions reçues, de tous les supports informatiques tels que la base de DIT, état des stocks, et l'autorisation au personnel du nouveau Titulaire d'accéder aux installations et locaux avant expiration du marché. À l'issue de ce transfert de compétences, une attestation détaillée du transfert des compétences sera établie et signée par les deux parties et comprendra au minimum :
    - Connaissance des locaux et des installations :
        - Localisation des équipements,
        - Procédure d'accès aux locaux spécifiques,
        - Etc.
    - Connaissance de gestion et d'administration des systèmes (redondance, sauvegardes, etc.),
    - Connaissance de la gestion de l'astreinte (délais d'intervention, escalade, procédure de demande d'intervention, etc.),
    - Formation à l'utilisation des outils de gestion mis à disposition du Titulaire pour exercer ces missions :
        - Contrôle d'accès (gestion des alarmes, gestion des badges, etc.),
        - Vidéosurveillance,
        - Anti-intrusion,
        - Interphonie et équipements radio portatifs,
        - Installations/équipements du Plan Particulier de Mise en Sûreté (PPMS),
        - GMAO,
        - Etc.
- Fournir à l'AMF le détail des surveillances et protocoles mis en œuvre pour l'exploitation quotidienne ;
- Restituer à l'AMF l'ensemble de la documentation de tout type produite à l'occasion du marché (procédures, modes opératoires, documentation technique, Support de Copil, etc.) et afférente à son exécution.

Le titulaire reconnaît qu'il est parfaitement informé que, durant cette phase de réversibilité, il doit nécessairement collaborer et composer avec la présence d'un tiers et/ou de représentants de l'AMF.

Les opérations de réversibilité comprendront également :

1/ La restitution par le Titulaire :

- De tous les Matériels dont l'AMF est propriétaire (incluant les licences) ;
- De tous les documents et éléments matériels de toute nature, propriété de l'AMF ou pour lesquels elle dispose les droits nécessaires, mis à la disposition du titulaire pour l'exécution des prestations objet du présent marché subséquent ;
- De tous les documents créés spécifiquement pour l'AMF pour l'exécution des prestations objet du présent accord cadre.

Le Titulaire s'engage alors à ne pas en conserver de copies et ne plus les utiliser, sauf, le cas échéant, pour permettre les opérations d'extraction ci-dessous visées et de réversibilité. Le Titulaire s'engage, après en avoir informé l'AMF, à détruire les documents ou données propriété de l'AMF ayant servi à l'exécution des prestations du présent accord cadre. Le Titulaire remettra à l'AMF, toutes les preuves nécessaires à démontrer la bonne exécution de la suppression ou de la destruction des données et des documents.

A moins que, dans les trente (30) jours suivant l'expiration de l'accord cadre, l'AMF n'ait donné au Titulaire l'instruction écrite de les effacer ou de les détruire, le Titulaire devra extraire toutes les données propriété de l'AMF ou pour lesquelles elle dispose des droits nécessaires, de ses systèmes et les transférer à l'AMF sur un support agréé par les parties.

2/ La communication par le Titulaire des informations qui sont nécessaires à l'AMF pour lui permettre de préparer la réversibilité :

Ces informations seront rassemblées dans un chapitre du PAQ, chapitre « plan de réversibilité » décrivant notamment le périmètre des prestations et les tâches respectives à accomplir par le Titulaire d'une part et par l'AMF ou le Tiers repreneur, d'autre part, pour assurer la réversibilité. Le chapitre de réversibilité est impérativement validé par l'AMF au plus tard au jour d'activation de la prestation de réversibilité par l'AMF.

3/ L'assistance technique du Titulaire afin de permettre l'acquisition des connaissances par l'AMF ou par un Tiers :

Cette tâche consiste à permettre à l'AMF ou à un Tiers désigné par l'AMF de prendre connaissance des prestations dans le dernier état connu, de leurs conditions de réalisation, ainsi que les méthodes et outils utilisés pour réaliser les prestations afin de les reprendre sans discontinuité de service.

L'AMF ou le Tiers collecte auprès du Titulaire, et avec sa collaboration, les informations nécessaires à la reprise des Prestations. Cette information est effectuée, tant par la mise à profit de la documentation d'exploitation, procédures, bases et paramétrages que par l'assistance aux travaux opérationnels et par la participation aux réunions spécifiquement organisées à cet effet. Le Titulaire présente et communique de manière précise les caractéristiques des Prestations.

Les engagements du titulaire au titre de la réversibilité pour lesquels il encourt l'application de pénalités en cas de non-respect sont :

- L'obligation de restitution des matériels et de la documentation ;
- L'obligation de destruction propriétaire des données en fin de marché ;
- Le transfert des données propriétaire sur un support agréé.

Ces obligations doivent être réalisées dans un délai maximum de 1 mois suivant l'émission du bon de commande de réversibilité.

7. REGLES GENERALES D'EXECUTION

7.1. LIMITES DES PRESTATIONS RESEAU SURETE

Le Titulaire devra s'appuyer sur le Système d'Information (SI) existant qui est placé sous sa responsabilité au titre de la maintenance forfaitaire. **Ce Système d'Information est géré par le PSET et non par la DSI de l'AMF.**

Pour éviter toute confusion entre les équipements DSI et PSET, les jarretières de brassage utilisées pour le réseau de Sûreté sont de couleur rose. Les équipements du périmètre du SI de Sûreté sont dans des baies fermées dont l'accès est réservé au titulaire.

La DSI de l'AMF reste responsable des éléments de l'infrastructure ci-dessous :

- ☐ Salle blanche pour l'hébergement des serveurs centraux ;
- ☐ Baies informatiques ;
- ☐ Fibre optique permettant l'interconnexion des 2 bâtiments et liaisons cuivre dans les bâtiments jusqu'au point VDI ;
- ☐ Lignes FT pour les systèmes avec transmetteurs téléphoniques (alarme incendie, PTI, etc.).

En cas d'incident supposé sur l'infrastructure, la DSI teste la continuité / qualité du câblage.

Le Titulaire est responsable de la maintenance et de la sauvegarde des systèmes hardware et software en place :

- ☐ Plates-formes matérielles et logicielles des serveurs de Sûreté (y compris hyperviseurs, OS, base de données, etc.) ;
- ☐ Logiciels de Sûreté (contrôle d'accès, vidéosurveillance, interphonie, etc.) ;
- ☐ Équipements actifs tels que les commutateurs Ethernet dans les salles informatiques hébergeant les serveurs et commutateurs Ethernet d'étage dans les locaux VDI (locaux de brassage) ;
- ☐ Il est attiré l'attention du Titulaire sur le fait que l'architecture du système est mise en œuvre de telle façon à ce que les interventions en maintenance sur le système dans les 2 salles informatiques (salles blanches) soient exceptionnelles (interventions limitées à des interventions sur le hardware). Les interventions en maintenance seront majoritairement réalisées sur le poste du cadre de sécurité et Sûreté (RdC AMF1).

7.2. OUTIL DE GMAO

L'AMF dispose d'un système Gestion de la Maintenance Assistée par Ordinateur (GMAO) pour ses installations techniques. Le Titulaire s'engage à utiliser cet outil, mis à disposition par l'AMF, pour gérer la maintenance des installations de Sûreté, dès le début d'exécution du marché.

L'achat des licences GMAO et de la formation à l'outil sont pris en charge par l'AMF.

7.3. PLANS ET NOTICES DESCRIPTIVES DES INSTALLATIONS

L'AMF met à la disposition du Titulaire l'ensemble des plans (par exemple DOE câblage Sureté des deux bâtiments) et notices dont elle dispose.

7.4. FOURNITURE DES CONSOMMABLES

Le Titulaire prend en charge forfaitairement la fourniture des consommables de maintenance.

Sont considérés comme « consommable de maintenance » tous les petits matériels ou produits non réparables dont la durée de fonctionnement est limitée, dans le cadre d'un usage normal de l'installation, à l'exclusion des consommables liés à l'exploitation même du système. À titre d'exemple sont inclus :

- ☐ Les fusibles, les relais thermiques, les disjoncteurs,
- ☐ Les batteries d'accumulateurs, les batteries des appareils radios portatifs,

- ☐ Les joints, les voyants lumineux,
- ☐ Les produits lubrifiants,
- ☐ Les produits de nettoyage, (les aérosols à gaz dépoussiérants, etc.).

7.5. FOURNITURE DE L'OUTILLAGE

Le Titulaire fournit à son personnel, et sous sa seule responsabilité, les moyens de déplacement, l'outillage nécessaire courant ou spécialisé et les appareils de mesure et de contrôle.

Dans le cas où des outillages spéciaux étaient fournis par le constructeur d'un équipement, ces outillages seraient réputés faire partie intégrante de l'équipement considéré et devraient donc être maintenus au même titre que l'équipement lui-même.

Le Titulaire a notamment à sa charge :

- ☐ Les moyens d'élévation pour les travaux en hauteur (plate-forme de travail individuelle roulante, échafaudage, nacelle, échelle, escabeau, etc.),
- ☐ Les équipements de manutention (palans, chariots électriques, etc.),
- ☐ Les moyens et frais de transport,
- ☐ Les équipements de sécurité de son personnel,
- ☐ Les équipements de protection des ouvrages pendant ses prestations de maintenance,
- ☐ Les équipements de protection et de balisage des zones en travaux.

7.6. MATERIELS MIS A DISPOSITION DU TITULAIRE

Les documents, équipements et matériels qui pourraient être mis à disposition du personnel du Titulaire pour effectuer les missions qui lui sont confiées, sont placés sous sa responsabilité.

En cas de dégradation de ces équipements (matériels informatiques, moyens de communication, badges, clefs, etc.) faisant suite à une mauvaise utilisation, il est demandé au Titulaire d'assumer les frais de réparation ou de remplacement du matériel hors usage.

En général, toute dépense pour remise en état des équipements, matériels et des installations ou documents provenant d'un manquement du Titulaire, lui sera automatiquement retenue sur la dernière facture ou, à défaut, facturée ultérieurement. En couverture de ces dépenses devront se subsister les garanties et cautionnements constitués dans le cadre du marché. Ces garanties et cautionnements devront rester constitués tant que subsisterait un litige éventuel en la matière.

7.7. GESTION DES TIERS

Le Titulaire a à sa charge la gestion des interventions des sous-traitants ou avec les Titulaires d'autres marchés avec lesquels l'AMF aurait contracté dans le cadre de la garantie, de la maintenance corrective ou préventive des systèmes et équipements de Sûreté.

7.8. PROTECTION DES BIENS

Le Titulaire doit à ses frais la remise en état des biens qu'il aurait pu dégrader pendant ses prestations et les frais éventuellement engagés pour pallier la défaillance qu'il a engendrée.

À défaut d'exécution rapide de ces réparations, l'AMF se réserve le droit, sans qu'il soit nécessaire de recourir à une mise en demeure, de les faire exécuter aux frais du Titulaire par tout moyen qu'elle jugerait bon.

7.9. TRAVAUX ANNEXES

Le Titulaire a à sa charge tous les frais et travaux annexes ou matériels nécessaires aux opérations de maintenance tels que :

- ☐ L'ouverture et la remise en place des faux planchers ou des faux plafonds nécessaires à l'exécution de ces prestations de maintenance,
- ☐ La protection des matériels ou des installations des autres corps d'état,
- ☐ La manutention de ces matériels et outillages,
- ☐ La remise en état des locaux de son fait après interventions,
- ☐ Le respect des procédures de traitement des déchets (tri sélectif, utilisation de sacs spécifiques, dépose dans des containers adaptés).

8. CONDITIONS PARTICULIERES D'EXECUTION

8.1. REGLES D'ACCES ET DE CIRCULATION DU PERSONNEL

Chaque personne intervenant sur site dans le cadre de l'exécution du marché devra renseigner une « demande de badge », signer un engagement de confidentialité et prendre connaissance du règlement intérieur de l'AMF.

Le Titulaire s'engage à désigner des intervenants intègres et dignes de confiance, qui n'ont pas fait l'objet de condamnations incompatibles avec l'exercice des missions qu'ils réaliseront dans le cadre du marché. Le Titulaire s'engage sur l'honneur pour chacun de ses intervenants avant toute intervention sur les sites de l'AMF.

Le Titulaire devra être en mesure de démontrer qu'il a mis en œuvre les niveaux de contrôle suffisants et proportionnés (par exemple consultation de l'extrait du bulletin n°3 du casier judiciaire) pour vérifier l'intégrité de ses intervenants , et ce, sur simple demande de l'AMF.

8.1.1. Liste du personnel

Le Titulaire transmettra au représentant de l'AMF, lors de la phase de démarrage, la liste nominative des personnels amenés à travailler régulièrement sur le site.

8.1.2. Badges d'identification

L'AMF réalisera les badges d'identification pour les personnels du Titulaire amenés à travailler régulièrement sur le site ou sur une période supérieure à huit (8) jours.

Le port du badge est obligatoire dans l'enceinte de l'établissement.

Sauf si l'intervention est programmée et le personnel encadré par l'AMF, il ne donne pas accès aux zones à risques en dehors des heures d'exploitation.

8.1.3. Accès au site

L'accès aux immeubles de l'AMF est autorisé durant les heures d'exploitation de 07h30 à 20h30 les jours ouvrés.

8.1.4. Travaux hors horaires d'accès au site

Pour une intervention en dehors des horaires normaux d'accès au site, l'accès se fera sur accord préalable des représentants de l'AMF.

8.1.5. Acheminement du matériel et évacuation des gravats

L'acheminement du matériel et évacuation des gravats devra être effectué sur l'accès présentant le risque minimum pour les personnes et les biens dans le respect des règles de circulation en vigueur à l'intérieur du site et sur la voie publique. Le Titulaire s'attachera à ne pas gêner le trafic.

8.2. REGLES DE SECURITE

8.2.1. Matériels

Les matériels appartenant au Titulaire ou mis à disposition par l'AMF, doivent être tenus en bon état de marche et seront régulièrement contrôlés. Ils devront être conformes aux règles de sécurité. Si le matériel mis à disposition par l'AMF n'est pas conforme ou en état, il appartient au Titulaire d'en refuser la mise à disposition et de ne pas l'employer.

8.2.2. Biens

Toutes précautions sont prises pour que l'état des meubles, aménagements, machines, etc. ne soit pas altéré par les opérations de maintenance.

Il est rigoureusement interdit au personnel du Titulaire, de manipuler, pour quelle que raison que ce soit, les appareils et matériels se trouvant dans les locaux et ne faisant pas l'objet des prestations du marché.

8.2.3. Personnes

Le Titulaire instruit son personnel sur les règles de sécurité du travail, tant générales que particulières.

Le Titulaire fait observer, par son personnel, les règles de sécurité du travail, notamment en ce qui concerne :

- ☐ Les alarmes de sécurité,
- ☐ Le travail en hauteur,
- ☐ L'encombrement de passages,
- ☐ Les zones interdites,
- ☐ L'utilisation des prises de courant destinées au raccordement des outils,
- ☐ L'utilisation des chaussures isolantes quand cela est nécessaire,
- ☐ La demande de permis et autorisations nécessaires en fonction du type de travaux effectués,
- ☐ Etc.

8.2.4. Discipline de chantier

Le Titulaire s'engage à faire respecter auprès de son personnel les règlements intérieurs et de sécurité propres au site.

Il sera interdit au personnel du Titulaire :

- ☐ De s'immiscer de quelque manière que ce soit dans la vie sociale de l'AMF,
- ☐ D'utiliser les moyens de communication de l'AMF de façon personnelle, sous peine de se voir refacturer une partie des communications,
- ☐ De prendre des repas à l'intérieur des locaux techniques ou dans les locaux accessibles au public,
- ☐ De fumer dans l'ensemble des locaux et bureaux à l'exception de ceux expressément désigné à cet effet,
- ☐ D'introduire ou de consommer des boissons alcoolisées dans les locaux, aussi bien que d'y pénétrer en état d'ivresse,
- ☐ De provoquer du désordre, d'une façon quelconque, sur les lieux du travail et les zones publics,
- ☐ De tenir des réunions dans l'enceinte des locaux n'ayant pas de rapport avec l'objet du contrat,
- ☐ D'inviter ou introduire dans les bâtiments des personnes tierces non autorisées,
- ☐ De manquer de respect aux usagers,
- ☐ De se faire aider, dans l'exécution de son travail, par une personne étrangère à l'entreprise exception faite des sous-traitants acceptés et agrées.

Cette liste n'est pas limitative.

8.3. HYGIENE ET SECURITE

Le Titulaire est tenu de prendre toutes dispositions afin d'assurer la sécurité des biens, l'hygiène, la sécurité des travailleurs et la sécurité publique, et de se soumettre à toutes les obligations mises à sa charge par les lois et décrets en vigueur, ainsi que celles qui sont prescrites dans ces mêmes domaines par le règlement intérieur de l'AMF.

Le Titulaire s'engage à :

- ☐ Fournir le plus tôt possible la liste de ses sous-traitants et faire parvenir aux représentants de l'AMF leur plan de prévention spécifique à la nature des travaux confiés,
- ☐ Déclarer ses sous-traitants dans les conditions prévues par le CCAP,

- L'harmonisation de leurs différents plans de prévention,
- La formation du personnel de chaque sous-traitant,
- La préparation à l'inspection préalable du démarrage des prestations et de l'établissement du Plan de Prévention Commun,
- Dispenser aux salariés qu'il affecte à l'exécution des prestations, la formation nécessaire à assurer leur sécurité en prenant notamment en compte les dangers spécifiques auxquels ils sont exposés, tant pour les risques liés à la présence de plusieurs entreprises, que pour ceux résultants de l'activité tels que définis dans le plan de prévention et ses additifs.

Le Titulaire doit vérifier ou faire vérifier sous sa responsabilité, par un organisme agréé, la conformité et la sécurité des outils et appareils soumis à règlement et requis sur l'établissement et procéder ou faire procéder aux épreuves et vérifications réglementaires nécessaires.

Le Titulaire est responsable de l'application de ces prescriptions.

8.4. PLAN D'ASSURANCE SECURITE (PAS)

Les SI de l'AMF respectent la Politique de Sécurité des Systèmes d'Information de l'État (PSSIE), qui impose des règles de conduite et de gestion des SI. Cependant, des exigences de sécurité spécifiques à l'AMF doivent être appliquées.

Conformément aux exigences exprimées à l'article 5.2.4.2, le PAS est mis au point par le Titulaire au cours de la phase de démarrage, sur la base du modèle remis dans son offre. Il pourra être ajusté au cours du marché, autant de fois que nécessaire

Chaque mise à jour du PAS fait l'objet d'une validation en COSEC, conformément aux stipulations de l'article 5.2.11.2 du présent CCTP.

8.5. PLAN D'ASSURANCE QUALITE (PAQ)

Le Plan d'Assurance Qualité (PAQ) est l'engagement du Titulaire quant à la politique d'assurance qualité applicable aux prestations. Il s'applique depuis le démarrage du contrat jusqu'à sa clôture.

Le PAQ est consultable par chaque membre de l'équipe du Titulaire en tant que document à mettre en application.

Il est également utilisé pour apporter la visibilité à l'AMF sur l'organisation mise en œuvre pour réaliser les prestations et sur les méthodes appliquées pour obtenir le niveau de qualité répondant aux exigences contractuelles (obligation de résultat).

Le PAQ décrit notamment :

- La présentation générale et le processus d'élaboration et de maintien à jour du PAQ
- Les documents applicables dans le cadre du contrat,
- Le glossaire des principaux termes ainsi que les abréviations utilisées,
- Les prestations objets du contrat et l'organisation associée,
- La méthodologie applicable pour la réalisation des prestations,
- Le processus de gestion de la qualité, et plus particulièrement dans le cadre de l'obligation de résultats,
- Le processus de gestion de la sécurité et de la confidentialité.
- Une description précise de la phase de réversibilité

Le PAQ du marché est mis au point par le Titulaire au cours de la phase de démarrage, sur la base du modèle remis dans son offre. Il pourra être ajusté au cours du marché, autant de fois que nécessaire.

Chaque mise à jour du PAQ fait l'objet d'une validation en COPIL, conformément aux stipulations de l'article 5.2.11.1 du présent CCTP.

9. PRESCRIPTIONS TECHNIQUES GENERALES

Les travaux et prestations de maintenance seront exécutés suivant les règles de l'Art, avec du matériel de qualité reconnue. Tous les appareils neufs seront présentés, avant pose ou approvisionnement, à l'agrément des représentants de l'AMF.

Le Titulaire devra fournir tous les renseignements techniques (catalogues, photographies, plans, fiches techniques, etc.) permettant de se rendre parfaitement compte des caractéristiques de ces appareils et de leur conformité aux règles et performances.

9.1. NORMES ET REGLEMENTS A PRENDRE EN COMPTE

Les normes à prendre en compte, avec leurs éventuels additifs, sont les suivantes :

Domaine	Référence	Intitulé / objet
Qualité	NF EN ISO 9001	Systèmes de management de la qualité – Exigences
Maintenance	NF X60-000	Maintenance – Fonction maintenance
Maintenance	NF EN 13306	Maintenance – Terminologie de la maintenance
Maintenance	NF EN 15341+A1 : 2022	Maintenance – Indicateurs de performance clés pour la maintenance
Maintenance	NF EN 17007 : 2017	Maintenance – Processus maintenance et indicateurs associés
Maintenance / sécurité	NF EN 17975 : 2025	Maintenance – Processus de maîtrise des risques liés aux énergies et fluides lors d'opérations de maintenance
Risque électrique	NF C18-510 et amendements en vigueur	Opérations sur les ouvrages et installations électriques et dans un environnement électrique – Prévention du risque électrique
Électricité BT	Série NF C15-100	Installations électriques à basse tension
Batteries / chargeurs	NF C58-311	Procédure d'essai de type des ensembles redresseurs-chargeurs batteries d'accumulateurs
Intrusion	Série NF EN 50131	Systèmes d'alarme – Systèmes d'alarme contre l'intrusion et les hold-up
Intrusion	NF EN 50131-1	Systèmes d'alarme contre l'intrusion – Exigences système
Intrusion	APSAD R81	Détection d'intrusion – Installation et maintenance
Vidéoprotection	Série NF EN 62676	Systèmes de vidéosurveillance destinés à être utilisés dans les applications de sécurité
Vidéoprotection	APSAD R82	Vidéosurveillance – Installation et maintenance
Contrôle d'accès	NF EN 60839-11-1	Systèmes d'alarme et de sécurité électroniques – Systèmes de contrôle d'accès électronique
Contrôle d'accès	APSAD D83	Contrôle d'accès – Installation et maintenance
Cybersécurité	APSAD D32	Cybersécurité – Installation de systèmes de sécurité ou de sûreté sur un réseau informatique
Cybersécurité	ANSSI	Recommandations sur la sécurisation des systèmes de contrôle d'accès physique et de vidéoprotection
Cybersécurité	ANSSI	Référentiel d'exigences de sécurité pour les prestataires d'intégration et de maintenance de systèmes industriels
Cybersécurité	ANSSI	Guide d'hygiène informatique et recommandations associées

Domaine	Référence	Intitulé / objet
Cybersécurité	ANSSI	Recommandations relatives à la sécurité des accès distants et à l'administration des systèmes
Cybersécurité	NIS2	Directive (UE) 2022/2555 et textes nationaux de transposition applicables
Réseaux informatiques	Série NF EN 50173	Technologies de l'information – Systèmes de câblage générique
Réseaux informatiques	Série NF EN 50174	Technologies de l'information – Installation de câblage
CFO/CFA	UTE C15-900	Mise en œuvre et cohabitation des réseaux de puissance et des réseaux de communication
Conduits	Série NF EN 61386	Systèmes de conduits pour la gestion du câblage
Goulottes / plinthes	Série NF EN 50085	Systèmes de goulottes et systèmes de conduits pour installations électriques
CEM	Série NF EN 61000	Compatibilité électromagnétique
CEM – environnement industriel	NF EN 61000-6-2	Immunité pour les environnements industriels
CEM – émission	NF EN 61000-6-4	Émission pour les environnements industriels
Équipements électroniques	NF EN 62368-1	Équipements des technologies de l'audio/vidéo, de l'information et de la communication – Exigences de sécurité
Protection des équipements	Normes produits applicables	Exigences de sécurité, CEM, environnement et compatibilité des équipements
Réseaux / cybersécurité	Référentiels ANSSI applicables	Architecture réseau, segmentation, administration sécurisée, authentification, journalisation, sauvegarde et accès distants
Télémaintenance	Référentiels ANSSI applicables	Sécurisation des accès distants et des opérations d'administration
Télémaintenance	Exigences du présent CCTP	Bastion, VPN, MFA, comptes nominatifs, limitation temporelle, journalisation, contrôle des sessions
Sécurité des interventions	Procédures de consignation et de mise en sécurité du site	Mise en sécurité avant intervention
Documentation	Exigences du présent CCTP	DOE, plans, schémas, configurations, inventaires, historiques et comptes rendus
Gestion des évolutions	Exigences du présent CCTP	Validation préalable des modifications matérielles, logicielles et réseau

Les références normatives et réglementaires mentionnées dans le tableau ci-dessus sont applicables dans leur dernière édition en vigueur, y compris leurs amendements, compléments et documents d'application, sauf disposition contractuelle contraire.

Lorsqu'une norme ou un référentiel cité est remplacé par une nouvelle édition ou par un document normatif venant en assurer la succession, le Titulaire applique la référence en vigueur correspondant au domaine concerné, sous réserve que cette évolution n'entraîne pas de modification substantielle des prestations ou des conditions contractuelles.

Le Titulaire assure une veille réglementaire, normative et technique pendant toute la durée du marché et informe l'AMF de toute évolution susceptible d'avoir une incidence sur la conformité, la sécurité, la sûreté, la cybersécurité, la disponibilité ou la maintenabilité des installations.

La liste figurant dans le tableau ci-dessus n'est pas limitative, notamment en ce qui concerne les normes propres aux matériels et à leur fabrication.

Les cahiers des charges DTU (Dossier Technique Unifié) publiés par le CSTB (Centre Scientifique et Technique du Bâtiment) sont tous applicables.

9.2. QUALITE DES MATERIELS

Le Titulaire aura l'entière responsabilité de tous les matériels qu'il fournit.

Tous les matériaux fournis seront neufs, conformes aux normes et décrets en vigueur, et exempts de tous vices visibles ou cachés.

Les matériels fournis neufs dans le cadre du marché seront garantis à minima deux (2) ans à compter de leur réception par l'AMF.

En cas de contestation sur la qualité, seules les règles d'essais normalisées seront applicables et les frais d'expertise seront à la charge du Titulaire. Si les essais décèlent une défaillance évidente d'un équipement, le Titulaire devra procéder au remplacement du dit équipement par du matériel dont les caractéristiques de fonctionnement sont identiques à celles décrites du matériel qu'il aura remplacé.

Les appareils devront être de marques connues, de technologie et de fabrication récente et d'un fonctionnement éprouvé. De même que les logiciels, qui devront être fournis avec leur licence dans la version la plus récente.

La responsabilité du Titulaire couvrira également et dans les mêmes conditions, toutes les fournitures qu'il aura éventuellement sous-traitées.

9.3. PROCEDURE EN CAS DE SINISTRE

En cas de sinistre/dommage, le Titulaire a, pour les installations relevant de sa compétence telles que décrites dans le CCTP, la responsabilité :

- ☐ De déclencher toutes les actions nécessaires de sauvegarde,
- ☐ De prévenir les représentants de l'AMF.

9.4. PRISE EN CHARGE ET REMISE DES MATERIELS ET EQUIPEMENTS

Le Titulaire déclare parfaitement connaître la constitution des locaux, la consistance des matériels et équipements et l'état des dossiers administratifs et techniques des installations dont il assure l'exploitation technique et la maintenance, ainsi que des règles de sécurité et règlements applicables en pareille matière.

A la prise en charge des installations, le Titulaire ne peut faire valoir des oublis des entreprises qui ont réalisé ou entretenu auparavant les installations dans les domaines du réglage, des finitions, ou du nettoyage pour se substituer à son obligation de résultat et au maintien en parfait état de propreté des équipements.

Les mises en conformité nécessaires sont à la charge financière de l'AMF, à condition que le Titulaire ait fait connaître aux représentants de l'AMF, par écrit, la nature des mises en conformité qui lui paraissent nécessaires.

Un procès-verbal contradictoire de l'état des lieux et des matériels ou équipements est établi dans un délai d'un (1) mois à compter de la notification (durant la phase de démarrage) et d'un (1) mois avant le terme du marché (pendant la phase de réversibilité). La rédaction de cet état des lieux est à la charge du Titulaire.

Dans les trente (30) jours suivant la remise de l'état des lieux initial, le Titulaire peut présenter des observations complémentaires sur l'état des installations qui lui sont confiées.

Passé ce délai, seules les réserves indiquées à ce procès-verbal sont prises en compte.

9.5. LOCAUX MIS A DISPOSITION DU TITULAIRE

Le Titulaire dispose d'un local ou d'un emplacement dédié et d'un stock de pièces détachées. Le Titulaire doit la surveillance et la maintenance en bon état de propreté de cet emplacement et de son mobilier.

L'AMF et ses représentants se réservent le droit d'accès à ce local ou à cet emplacement.

L'AMF se réserve également la possibilité de les échanger contre d'autres locaux, sous réserve de proposer d'autres locaux équivalents.

Le Titulaire, sur la base d'un état des lieux contradictoire, prend les locaux dans l'état où ils lui sont remis par l'AMF, sans pouvoir n'exercer aucun recours contre celui-ci, ni faire aucune réclamation pour quelque cause que ce soit.

Le Titulaire peut, s'il le juge utile, proposer aux représentants de l'AMF l'adjonction à ses frais de tout aménagement complémentaire. Les projets correspondants doivent recevoir l'accord écrit des représentants de l'AMF sur le descriptif des aménagements avant tout commencement d'exécution. Les aménagements à caractère immobilier resteront acquis à l'AMF ou, à son choix, feront l'objet d'une remise en état des lieux par le Titulaire et avant la fin du marché ou postérieurement à la fin du marché, par l'AMF mais à la charge financière du Titulaire.

9.6. DOCUMENTATION TECHNIQUE

Des copies des documents techniques d'exécution disponibles sont accessibles pour le Titulaire à la prise en charge. Il appartient au Titulaire de dupliquer, de créer et de compléter cette documentation suivant ses besoins.

Cette documentation reste la propriété de l'AMF et n'est utilisée par le Titulaire qu'à des fins d'exécution du marché. **En aucun cas ces documents ou leurs copies ne sont autorisés à quitter l'AMF.**

Le Titulaire est chargé de la mise à jour des documents originaux et reproductions, en cas de modification des appareils ou équipements consécutive à des interventions, adjonctions et modifications.

Chaque fois que le Titulaire constate une erreur sur les documents mis à sa disposition, il doit en informer l'AMF et apporter les corrections nécessaires.

Toute mise à jour des documents techniques se fait de manière immédiate et permanente et en tout état de cause ne peut accuser de retard excédant trente (30) jours à compter du jour où la mise à jour était nécessaire.

À aucun moment, et de quelque manière que ce soit, sauf accord préalable et spécifique de l'AMF, le Titulaire n'est autorisé à faire sortir de l'information vers l'extérieur et ce quelle qu'en soit la nature ou le moyen. Notamment les liaisons par modem sont proscrites.

10. INTERVENANTS DU TITULAIRE

10.1. GENERALITES

Le personnel intervenant dans le cadre du marché devra être conforme aux profils présentés dans l'offre du titulaire, et sera soumis à un accord préalable de l'AMF.

L'AMF s'autorise à récuser tout intervenant qui ne présenterait pas les compétences nécessaires ou les caractéristiques requises. Dans ce cas, le titulaire propose un nouvel intervenant.

10.2. CONFIDENTIALITE

Le titulaire a une obligation de confidentialité, précisée à l'article 10 du CCAP.

Le Titulaire informera préalablement les personnes susceptibles de travailler sur le site de cette obligation de confidentialité et rappellera régulièrement cette règle.

Après notification du marché, chaque intervenant du Titulaire et de ses sous-traitants éventuels devra signer un engagement de confidentialité fourni par l'AMF.

Sur demande de l'AMF, le Titulaire communiquera les engagements de confidentialité signés.

Le respect de l'obligation de confidentialité est une condition essentielle du marché.

Le non-respect de l'obligation de confidentialité peut entraîner la résiliation du marché.

10.3. LE RESPONSABLE CLIENT

Le Responsable Client est l'interlocuteur direct auprès des représentants de l'AMF et sera, dans la mesure du possible, la même personne durant toute la durée du marché. Il est désigné dans l'offre du Titulaire.

De manière ponctuelle, il est présent sur le site et exerce une supervision complète de la bonne exécution du marché.

Il est également présent sur le site sur convocation des représentants de l'AMF.

Il participe aux instances de gouvernances telles que décrites dans le présent CCTP.

Il est précisé que le personnel du Titulaire est sous le contrôle et la responsabilité de l'encadrement défini ci-dessus.

10.4. LE PERSONNEL SUR SITE

10.4.1. Généralités

À cette fin le Titulaire devra communiquer les coordonnées complètes de ses personnels, co-traitants ou sous-traitants susceptibles d'intervenir sur le site.

L'ensemble des personnes susceptibles de travailler sur le présent dossier sera tenu à un engagement signé de confidentialité. Cet engagement de confidentialité ne sera pas limité dans le temps.

10.4.2. Personnel permanent et régulier

Le Titulaire s'engage à fidéliser au maximum son personnel dans le cadre de l'exécution du marché.

Pour tout intervenant sur site, le titulaire doit délivrer avant la prise de poste de ce dernier les informations suivantes, et au plus tard sous 48 heures. Ces informations font l'objet d'une fiche signée par le Titulaire, accompagnée d'un engagement de confidentialité signé par l'intervenant.

Pour les personnes appelées à intervenir de manière permanente ou régulière, la demande est accompagnée d'une fiche d'engagement à laquelle est notamment annexé un Curriculum Vitæ (CV) complet, détaillant entre autres l'expérience professionnelle acquise pour la fonction.

Le titulaire s'engage à vérifier au préalable pour chacun des intervenants les diplômes et certificats acquis par ces derniers (copie à l'appui). Il s'assure également que les personnes intervenant dans le cadre du marché ont les qualités morales pour intervenir (par exemple pas de ex-hacker, etc.).

10.4.3. Engagement de compétence - Qualifications

Le Titulaire s'engage à faire exécuter les prestations objet du marché par un ou plusieurs intervenants de compétences et de qualification adaptées aux besoins de l'AMF (cf. article 10.4.4 ci-dessous). Le Titulaire est seul responsable des intervenants qui demeurent sous son contrôle, sa direction et son autorité hiérarchique.

Le Titulaire s'engage à exécuter les prestations en application de son savoir-faire, de ses méthodes et de son expérience. En conséquence, le Titulaire s'engage notamment à :

- Constituer des équipes de personnels compétents, c'est-à-dire formés en conformité avec les besoins de l'AMF ;
- Veiller et contrôler le maintien constant des compétences, de leur homogénéité, de leur disponibilité, de leur réactivité, de leur composition ;
- Maintenir une forte réactivité, notamment en adaptant très rapidement la composition de ses équipes en cas de difficulté.

Les intervenants du titulaire doivent disposer d'une expertise technique et organisationnelle en gestion, conception et réalisation des Systèmes d'information et des installations de sureté pour effectuer les prestations objet du marché

Les intervenants du Titulaire doivent en tout état de cause posséder les qualifications et habilitations requises pour l'exécution des tâches qui lui sont confiées.

Le Titulaire est responsable de la qualification et du choix de sa main d'œuvre. La qualification de tout le personnel intervenant sur le site doit pouvoir être vérifiée par les représentants de l'AMF.

Le Titulaire prend en charge la formation de son personnel nécessaire pour assurer les prestations qui lui sont confiées (formation technique générale et spécifique sur la maintenance des systèmes objet du marché et l'outil de GMAO). Il produit les justificatifs de formation de ses personnels à l'AMF.

Le personnel d'intervention du Titulaire est soumis :

- ☐ Aux dispositions générales prévues par la législation du travail,
- ☐ Aux règles qui sont appliquées au personnel extérieur intervenant sur le site.

La liste du personnel du Titulaire sur le site est tenue à jour régulièrement et une mise à jour est transmise à l'AMF lors de toute modification.

Il convient de rappeler que le Titulaire a une **obligation de résultat**. Il appartient au Titulaire dans le cadre du marché, de définir le nombre, les durées et horaires de présence, et la qualité du personnel mis en place pour faire face à ses obligations contractuelles. Il informe cependant l'AMF des horaires et plannings établis et exécutés.

10.4.4. Formation des intervenants affectés à la réalisation des prestations

Le Titulaire doit prendre en charge la formation générale des personnels qu'il emploie dans le cadre de l'exécution du marché.

En plus des prérequis nécessaires, des formations spécifiques devront être obligatoirement dispensées aux personnels de maintenance. Ces formations concernent l'ensemble des systèmes définis comme essentiels et/ou figurant dans le tableau de maintenance ci-après.

Concernant la maintenance préventive et corrective de niveau 3, le Titulaire doit justifier que les intervenants affectés à la réalisation de la prestation, ou le cas échéant les intervenants de son co-traitant ou de son sous-traitant, a suivi une formation dispensée par le constructeur, l'éditeur, l'importateur ou le distributeur du matériel concerné et dispose éventuellement de l'outillage spécifique nécessaire.

Désignation des matériels et systèmes	Maintenance préventive	Maintenance corrective
Système de contrôle d'accès et d'intrusion	3 & 4ème niveaux	3 & 4ème niveaux
Système de vidéosurveillance	3 & 4ème niveaux	3 & 4ème niveaux
Réseau	3 & 4ème niveaux	3 & 4ème niveaux

Le Titulaire devra fournir la justification des formations nominativement dispensées. Si le personnel ne dispose pas du prérequis initial nécessaire, la formation devra être dispensée dans les trois (3) premiers mois.

10.4.5. Responsable de site

L'équipe détachée sur un site par le Titulaire est placée sous la responsabilité d'un chef de site désigné dans l'offre.

Sont considérés comme site un ensemble de bâtiments défini dans le périmètre géographique et les modifications éventuelles ultérieures.

Pendant toutes ses absences (congés légaux, arrêt maladie), le responsable de site est remplacé par une personne désignée comme responsable de site adjoint et approuvée par l'AMF et possédant les mêmes capacités et attributions.

Il est responsable :

- ☐ Du respect de l'exécution des plannings de contrôle,
- ☐ Du contrôle de la qualité des prestations,
- ☐ Des documents techniques et rapports tels que définis dans le présent CCTP,
- ☐ De l'organisation du travail,
- ☐ De la préparation et du suivi des prestations,
- ☐ Du suivi des sous-traitants, et coordonne les mesures de sécurité des sous-traitant,
- ☐ De l'information des représentants de l'AMF,
- ☐ De la discipline du chantier et du personnel,
- ☐ De la formation des intervenants sur les postes de travail et du respect du plan de prévention,

Cette personne est l'interlocuteur journalier des représentants de l'AMF. Il fait des points hebdomadaires de suivi de son activité avec compte-rendu.

Il a un pouvoir suffisant pour commander du matériel ou faire appel à des renforts pour répondre aux obligations de résultats contractuelles.

Il participe activement aux réunions annuelles, semestrielles et mensuelles avec les représentants de l'AMF.

Il devra :

- ☐ Connaître tous les documents contractuels du marché,
- ☐ Gérer le marché sous tous ses aspects, qu'ils soient techniques, de sécurité, relationnels, de maintenance, de travaux.

Le Titulaire doit disposer d'un personnel assurant la fonction de « secrétariat technique » qui doit notamment permettre d'assurer sous la responsabilité du chef de site :

- ☐ La coordination des interventions,

- La réception des demandes émanant de l'AMF,
- La saisie sur la GMAO,
- La préparation des rapports,
- La préparation et la saisie des compte-rendu des réunions (annuelles, semestrielles et mensuelles),
- L'archivage de tous documents à caractère technique et la préparation et le collationnement de tous documents demandés par l'AMF sur base d'éléments chronologiques, thématiques ou autres,
- Le personnel de secrétariat technique nommément désigné par le Titulaire en vue de l'exécution des prestations du marché, doit également être préalablement agréé par les représentants de l'AMF et fournir les certificats demandés.

10.5. VETEMENT DE TRAVAIL ET EPI

Le Titulaire dote le personnel d'exécution d'un vêtement de travail sur lequel le nom de l'entreprise est visible, et de protection individuelle (EPI), adapté à son activité et notamment à la réglementation.

Tous les personnels du Titulaire intervenant en permanence ou régulièrement sur le site, y compris le personnel d'encadrement et administratif, doivent porter en permanence une tenue de travail ou un insigne spécifique de leur entreprise ainsi que le badge résident du site.

Aucun agent n'est admis s'il n'est pas revêtu de son vêtement de travail, s'il est démuni de son insigne ou s'il présente une tenue négligée.

11. OBLIGATIONS ET RESPONSABILITES DU TITULAIRE

11.1. EXIGENCES DE CYBERSECURITE

Des exigences de cybersécurité sont applicables pour les prestations de maintenance et de travaux, et sont décrites dans le CCCS.

11.2. ORGANISATION DES PRESTATIONS

Le Titulaire s'engage à :

- ☐ Assumer, sous sa responsabilité exclusive, l'organisation du travail, la discipline, le respect des consignes, l'administration et la bonne tenue de son personnel, et les personnels sous-traitants,
- ☐ Contrôler régulièrement le bon déroulement de la mission qui lui est confiée, et le respect des consignes données à son personnel, et aux personnels sous-traités,
- ☐ Assurer la permanence de ses prestations, de telle façon que la mission, objet du marché, soit parfaitement remplie,
- ☐ Se conformer aux normes et règlements pour l'exécution des tâches qui lui incombent,
- ☐ Faire en sorte que ses interventions ne provoquent aucune gêne des occupants, ni désordre sur le site,
- ☐ Restituer les installations, équipements et locaux en bon état à l'expiration du marché,
- ☐ À dispenser un rôle de conseil technique auprès de ses interlocuteurs à l'AMF qui lui en font la demande habituelle.

11.3. GARANTIES

11.3.1. Garantie des installateurs

Les appareils pris en charge peuvent être :

- ☐ Des matériels achetés directement par l'AMF,
- ☐ Des installations nouvelles réceptionnées à la date de prise d'effet de la commande correspondante,
- ☐ Des installations nouvelles non réceptionnées à la date de prise d'effet mais dont le Titulaire assurerait cependant la responsabilité.

Au cas par cas, tel que défini dans les trente (30) jours du début du marché, il sera établi les circonstances et installations pour lesquelles l'AMF et ses représentants subrogent le Titulaire dans ses droits et actions liés ou à naître à l'encontre du constructeur ou de l'installateur, et de tout tiers responsable ou estimé responsable d'une avarie ou dommage survenant aux appareils dont il a la charge.

En cas d'avarie sur des matériels ou installations sous garantie, le Titulaire prend les mesures conservatoires nécessaires et procède sans délai aux appels en garantie auprès des entreprises de marché de travaux en cause. Ces dispositions ne doivent pas être un frein à la continuité du service à laquelle le Titulaire est obligé.

Il prend soin de faire en sorte que ses interventions de maintenance préventive ne soient pas de nature à empêcher l'application des clauses de garantie. Il avertit immédiatement les représentants de l'AMF des actions à mener pour bénéficier de cette garantie.

En outre, pendant cette période, le Titulaire prend toutes les dispositions en accord avec le constructeur ou l'installateur pour assurer la coordination de leurs interventions.

Le Titulaire est réputé connaître les clauses de garanties légales et particulières attachées aux marchés de travaux.

11.3.2. Pièces remplacées par le Titulaire

Pour toute pièce remplacée par le Titulaire, celui-ci tiendra à jour un listing mentionnant la date d'effet de la garantie ainsi que la durée de toute pièce remplacée.

11.4. MATERIELS ET OBJETS CONFIES AU TITULAIRE

Le Titulaire est responsable de la conservation, de l'entretien et de l'emploi de tout matériel et objet qui lui sont confiés, dès que ce matériel ou objet est entré effectivement en sa possession.

Il ne peut en disposer qu'aux fins prévues par le présent marché et ne peut le faire sortir du site sans l'accord écrit de l'AMF.

Si le Titulaire ne peut restituer un matériel ou objet, pour quelque motif que ce soit, l'AMF et ses représentants décident, après s'être informé de ses possibilités, la mesure de réparation à appliquer (remplacement ou remise en état).

Le cas échéant, l'AMF dote le Titulaire de récepteurs de recherche de personnes, de clés, de badges en quantité suffisante, avec les droits associés permettant l'accès à certains locaux intéressés par les prestations. Le Titulaire s'interdit d'en faire une copie.

En cas de perte ou de vol, le Titulaire avise aussitôt les représentants de l'AMF des articles manquants. Ceux-ci sont remplacés et font l'objet d'une facturation au Titulaire, au tarif en vigueur. Pour les passes, le Titulaire doit le remplacement à ses frais des canons accessibles à partir du passe considéré. Son attention est attirée sur le coût potentiellement élevé d'un tel remplacement. Spécifiquement, le Titulaire se fera couvrir des risques liés à une perte ou un vol de passe ou déclarera avoir suffisamment évalué le risque et en couvrir les conséquences lui-même. La perte d'une clé implique automatiquement le droit pour l'AMF de faire remplacer le système ou l'ensemble du système aux frais du Titulaire et de faire couvrir par celui-ci sous forme d'indemnité équivalente à 50% de la valeur des matériels remplacés les coûts administratifs subséquents. Ceci sans préjudice de l'existence de coûts supérieurs prouvés par l'AMF. L'AMF retiendra automatiquement sur facture l'ensemble de ces coûts et la non-reconnaissance par un assureur de la responsabilité du Titulaire demeurera en tout état de cause un dossier à régler entre le Titulaire et son assureur.

En fin de marché, le Titulaire est tenu de remettre à l'AMF la totalité des clés et des badges confiés initialement.

11.5. NETTOYAGE DES LOCAUX TECHNIQUES ET DES INSTALLATIONS

Le Titulaire s'engage :

- ☐ À remédier aux carences éventuelles des entreprises qui ont assuré l'entretien précédemment en matière de nettoyage,
- ☐ À maintenir en parfait état de propreté les locaux techniques, principaux, secondaires et les coffrets spécifiques,
- ☐ À trier et évacuer à la décharge les matériels, matières et équipements usagés conformément à la réglementation en vigueur.

11.6. SIGNALISATION DES TRAVAUX

Chaque fois que cela est nécessaire, le Titulaire doit, à ses frais et après approbation par l'AMF, placer les barrages ou déviations, poser les écriteaux et prendre toutes les dispositions pour assurer la signalisation et prévenir les divers usagers de la présence de zones interdites.

En cas de carence du Titulaire, ou en cas de danger, l'AMF se réserve le droit de prendre toute mesure utile aux frais du Titulaire, et sans mise en demeure préalable, sans que cette action puisse dégager la responsabilité du Titulaire en cas d'accident.

11.7. RESPONSABILITE DU TITULAIRE

11.7.1. Obligations de conseil et d'information

De manière générale, le Titulaire doit informer l'AMF de tous les problèmes qu'il rencontre pour assurer sa prestation.

Le Titulaire doit, en tout état de cause, signaler à l'AMF, dès qu'il a été normalement en mesure de les déceler, les incidents prévisibles, susceptibles d'affecter la sécurité des personnes, des biens ou des informations, et lui indiquer les conséquences qui pourraient en résulter dans le cas où il n'y serait pas porté remède.

Si les installations mises à disposition du Titulaire venaient à ne plus être conformes à la réglementation, le Titulaire est tenu d'en informer par écrit et sans délai les représentants de l'AMF. Il appartient aux représentants de l'AMF de prendre aussitôt les dispositions nécessaires en vue de leur mise en conformité.

Le Titulaire doit assistance aux représentants de l'AMF soit :

- ☐ Par téléphone pour tout complément d'information,
- ☐ Lors des réunions provoquées par les représentants de l'AMF si nécessaire,
- ☐ En transmettant aux représentants de l'AMF les nouveaux textes réglementaires relatifs à ses prestations, accompagnés éventuellement d'une note expliquant l'influence de ces textes sur son activité.

En aucun cas, les précédentes dispositions relatives à l'obligation de conseil ne dispensent le Titulaire d'assurer les prestations définies objet du marché.

Dans la mesure où il est défaillant pour quelque raison que ce soit, les représentants de l'AMF peuvent faire appel à toute autre forme de service, aux frais du Titulaire.

Le Titulaire est tenu de vérifier les indications portées sur les documents qui lui sont communiqués et de signaler dans l'état actuel connu des connaissances et de la technique toute anomalie, non-concordance et autres qui lui appartiendraient sous peine d'en subir seul et de convention expresse toutes les conséquences.

Le Titulaire est tenu de s'informer sur les répercussions directes des fournitures ou prestations autres que les siennes et de fournir les renseignements relatifs aux répercussions directes de ses prestations sur les autres. Il est responsable de tout retard apporté à ces informations.

Le Titulaire doit demander aux représentants de l'AMF tous les renseignements que celui-ci peut détenir et qu'il estime utiles et nécessaires à tous les stades de l'exécution du marché.

Le Titulaire doit attirer l'attention par écrit des représentants de l'AMF sur les inconvénients qui peuvent résulter des ordres reçus, sur les vices ou les malfaçons que ceux-ci peuvent entraîner soit pour ses propres prestations soit pour des tiers.

11.7.2. Assistance et formation du personnel utilisateur de l'AMF

Sur demande ponctuelle, le Titulaire peut être sollicité dans le cadre de son forfait pour former et assister les utilisateurs des systèmes dont il a la responsabilité.

Il devra également assurer la sensibilisation des personnels à l'utilisation des matériels si ces derniers, par leur méconnaissance des matériels exploités, peuvent entraîner une défaillance.

11.7.3. Limite de responsabilité technique

La responsabilité du Titulaire n'est pas engagée dans le cas de force majeure.

Constituent un cas de force majeure au sens du marché :

- ☐ Les faits de guerre,
- ☐ Les injonctions administratives ou judiciaires de suspendre l'exploitation du site, sauf quand celles-ci sont imputables au Titulaire,
- ☐ Les cataclysmes et catastrophes naturelles ou causées par un tiers.

Dans le cas de force majeure prolongée entraînant ou risquant d'entraîner des restrictions permanentes ou même un arrêt prolongé dans la fourniture du Titulaire, celui-ci doit proposer aux représentants de l'AMF les mesures à prendre afin d'éviter un arrêt définitif et organise la poursuite des prestations minimales, au besoin éventuellement assorti de nouvelles conditions contractuelles adoptées aux dites circonstances.

Les grèves du personnel du Titulaire ainsi que les grèves des transports en commun, même prolongées, ne sont pas considérées comme un cas de force majeure.

Le Titulaire doit, en toute circonstance, assurer les prestations définies dans le présent CCTP. Dans la mesure où il est défaillant pour quelque raison que ce soit, les représentants de l'AMF peuvent faire appel à toute autre forme de service, aux frais du Titulaire.

La responsabilité du Titulaire ne peut être recherchée pour les conséquences d'interventions de personnes ou société étrangères effectuées sans son accord express ou dans des conditions qu'il n'aurait pas approuvées.

De même toutes les prestations et fournitures liées à un mauvais usage du matériel, à une dégradation accidentelle ou volontaire n'entre pas dans le cadre du forfait.

11.7.4. Responsabilité sociale

Le Titulaire assure pour son personnel la responsabilité de son affiliation à tous les organismes sociaux, ainsi que son entière responsabilité vis-à-vis des règlements de la législation du travail et de la sécurité des travailleurs.

11.8. EXIGENCES DE SECURITE

Les infrastructures et applications relatives aux prestations prévues dans le marché assurent le stockage et le traitement d'une quantité importante de données sensibles, confidentielles et à caractère personnel. Toutes collectes, transmissions et utilisations des données à caractère personnel effectuées dans le cadre des prestations doivent être effectuées par le Titulaire conformément aux dispositions législatives et réglementaires sur la protection des données ainsi que sur l'ensemble des exigences de l'AMF telles que figurant dans pièces du marché.

Le Titulaire s'engage ainsi à mettre en œuvre, d'une manière conforme à l'état de l'art, toutes les mesures techniques et organisationnelles nécessaires pour garantir la confidentialité, l'intégrité et la disponibilité des données de l'AMF auxquelles ils pourraient avoir accès dans le cadre des prestations.

Dans le cas où des accès externes au SI Sûreté de l'AMF seraient utilisés dans le cadre des prestations, ceux-ci ne pourraient l'être que depuis le réseau interne sécurisé du Titulaire, à partir du territoire de l'Union Européenne.

Dans ce cadre, le Titulaire est directement responsable de l'utilisation des accès distants au système d'information de l'AMF réalisés par ses personnels et éventuels sous-traitants.

En cas d'incident de sécurité relatif au SI Sûreté du Titulaire ou celui de ses sous-traitants affectant ou pouvant affecter la confidentialité ou l'intégrité des informations de l'AMF, le Titulaire s'engage à en informer par écrit sous 24 heures le DCRS de l'AMF.

Les données confidentielles (notamment : les données de connexion des administrateurs, les données à caractère personnel, les données métiers contenues dans l'application, définies dans le plan d'assurance qualité) doivent être stockées sur le territoire national.

Le SI Sûreté est un outil critique pour les activités de l'AMF, sur les plans financier, compétitivité, réglementaire et image de marque. C'est pourquoi la protection du SI Sûreté de l'AMF et des informations qu'il contient demande un engagement du Titulaire quant au respect des règles de sécurité SI Sûreté, que ce soit en termes de confidentialité, d'intégrité ou de traçabilité, tout autant que de disponibilité.

Pour réaliser leur mission, les équipes du Titulaire doivent avoir de bonnes connaissances en sécurité SI Sûreté et être sensibilisées au respect de la politique et des règles de sécurité applicables au SI Sûreté de l'AMF. Le Titulaire assurera la sensibilisation, et si nécessaire la formation, de ses équipes dans ce sens.

Cet article a pour objectif de faire le point sur les exigences en sécurité SI Sûreté :

- ☐ L'organisation de la gestion de la sécurité ;
- ☐ Les aspects humains ;
- ☐ La protection physique et logique des environnements ;
- ☐ La sécurité dans les développements applicatifs ;
- ☐ La continuité des activités.

Il vise à expliciter les éléments indispensables pour satisfaire aux exigences de sécurité de l'AMF dans le cadre de la prestation. Ainsi, chacun des points mis en avant peut voir sa mise en œuvre vérifiée par des contrôles permanents à réaliser par le Titulaire ou des audits mandatés par l'AMF.

Les différents éléments indiqués s'appuient sur des pratiques reconnues, issues des normes ISO 27001 et ISO 27002.

Les exigences générales applicables au Titulaire sont les suivantes :

- Pour l'organisation : l'implication du management, son soutien et le contrôle qu'il exerce doivent garantir la bonne application des principes de sécurité identifiés pour les services rendus dans le cadre du marché ;
- Pour le personnel : tous les intervenants sur les services objet du marché (Titulaire et sous-traitants agréés) sont habilités personnellement et seulement sur le périmètre précis de leur activité. Tous les intervenants sont sensibilisés aux enjeux et règles de sécurité généraux et spécifiques à leur activité dans le cadre du service rendu ;
- Pour les actifs techniques du Titulaire (serveurs…) : la criticité des actifs du Titulaire et de ses sous-traitants utilisés pour le service fourni à l'AMF doit être identifiée et caractérisée, même ceux dont l'AMF n'a pas directement connaissance. Les actifs du Titulaire (systèmes, réseaux, télécommunications, protections environnementales, …) destinés directement ou indirectement à l'exécution du service sont référencés et protégés conformément à leur criticité ;
- Pour les actifs informationnels du Titulaire (données, programmes…) : les actifs informationnels du Titulaire et de ses sous-traitants doivent être exploités dans des conditions de sécurité permettant d'assurer l'exécution du service rendu à l'AMF dans les conditions fixées au marché. Les actifs informationnels du Titulaire et de ses sous-traitants ne doivent pas disposer de lien logique avec le SI Sûreté de l'AMF hébergé chez le Titulaire, même pour un hébergement mutualisé ;
- Pour les actifs de l'AMF : les actifs de l'AMF hébergés par le Titulaire doivent être isolés ou protégés de façon à interdire tout accès non autorisé, volontaire ou involontaire d'un tiers et toute manipulation non prévue au contrat ou non autorisée par l'AMF (dans « la limite du périmètre de responsabilité du Titulaire ou de ses sous-traitants »). Les actifs de l'AMF hébergés par le Titulaire doivent être placés dans un environnement permettant de garantir leur bon fonctionnement selon les paramètres définis par l'AMF.

11.8.1. Domaine d'application

La sécurité est indissociable des services objet du marché.

Les éléments décrits dans cet article s'appliquent au Titulaire pour :

- Tous les services objet du marché ;
- Toutes les activités propres au Titulaire qui concourent à la réalisation du service et peuvent provoquer l'apparition d'un risque de sécurité non identifié préalablement par l'AMF ;
- Toute activité sous-traitée par le Titulaire et qui concourt à la réalisation du service pour l'AMF ;
- Ils s'appliquent aussi à l'ensemble des actifs informationnels et physiques propriétés du Titulaire ou de ses sous-traitants, s'ils concourent à la réalisation du service pour l'AMF.

11.8.2. Formalisme et révision

Les exigences fournies par cet article doivent être traitées soit dans la PSSI du Titulaire, ou à défaut dans le PAS spécifique au marché.

L'identification des éléments du dispositif sécurité est une démarche itérative conforme à la norme ISO 27001. Les principes énoncés pourront évoluer en fonction des risques liés au domaine de la sécurité ou de la réglementation applicable à l'AMF.

Le Titulaire à l'initiative des évolutions de la PSSI, qu'il doit faire évoluer en fonction de son système de gestion des risques. Il doit au minimum procéder à une revue annuelle et réaliser la mise à jour si nécessaire.

En cas d'évolution de la PSSI, l'AMF doit être informée des conséquences de ces évolutions tant sur le plan des risques traités que des mesures applicables. Une modification du PAS spécifique au marché peut être effectuée pour intégrer les évolutions de la PSSI.

11.8.3. Organisation de la sécurité

11.8.3.1. Dispositions générales

Le Titulaire doit disposer d'une organisation de gestion de la sécurité prédéfinie et opérationnelle. Cette dernière doit être détaillée dans sa PSSI. Le Titulaire devra être en mesure de démontrer la bonne déclinaison opérationnelle des règles fixées dans sa PSSI.

L'organisation sécurité du Titulaire, voire de ses sous-traitants, participant à la sécurité des actifs de l'AMF sera portée à la connaissance de l'AMF, ainsi que toutes ses modifications durant la période de validité du marché.

De la même façon, l'AMF communiquera au Titulaire tout élément relatif à l'organisation de la sécurité de l'AMF indispensable à l'exécution du contrat. Ces éléments sont confidentiels et ne doivent pas être portés à la connaissance de tiers sans l'accord explicite de l'AMF.

Chaque partie désignera un « correspondant sécurité ».

Le Titulaire s'assurera du respect par ses sous-traitants des exigences de sécurité présentes dans sa PSSI.

11.8.3.2. Gestion des incidents de sécurité

Tout Incident de sécurité subi par le Titulaire et pouvant avoir des conséquences, avérées ou supposées, sur les actifs de l'AMF gérés par le Titulaire doit être signalé à l'AMF dans un délai de 24h à compter de sa survenance, afin qu'il puisse en mesurer l'impact sur son activité et prendre des dispositions d'escalade éventuelles.

Les différents types d'incidents de sécurité seront définis dans la PSSI (ou le PAS).

11.8.3.3. La gestion des biens

- **La classification des actifs**

L'ensemble des actifs participant à l'exécution du service rendu par le Titulaire est inventorié et classifié selon les modalités propres au Titulaire. Le Titulaire décrira à l'AMF les grandes lignes de la méthode de classification mise en œuvre dans sa PSSI.

Le Titulaire fera valider par l'AMF la classification des actifs dédiés à l'AMF pour l'exécution du service et mettra en place toutes les mesures nécessaires au respect de l'exigence de sécurité validée conjointement.

- **La vie de l'actif**

Le cycle de vie de l'actif devra être clairement défini dans le PAS. Les grandes lignes du cycle de vie de ces actifs telles que mises en œuvre par la Titulaire doivent y être décrites.

Le Titulaire doit systématiquement faire valider à l'AMF toute modification devant survenir sur les actifs qui lui sont dédiés. En particulier si elles sont susceptibles de provoquer une perturbation voire une interruption du service.

Pour les actifs du Titulaire concourant au service mais non dédiés à l'AMF, le Titulaire s'engage à prévenir l'AMF de toute modification pouvant avoir un impact sur le fonctionnement des actifs de l'AMF avec un délai de prévenance suffisant pour permettre à l'AMF d'analyser l'impact du changement sur ses actifs.

11.8.4. Moyens dédiés par le titulaire concernant les aspects sécurité

11.8.4.1. Rôles et responsabilités

L'identité, le rôle et les responsabilités des collaborateurs du Titulaire, affectés à la réalisation de la prestation au profit de l'AMF doivent être clairement définis dans le plan d'assurance qualité. Cette définition doit permettre d'attribuer clairement les accès de ces personnes aux actifs de l'AMF.

Cette définition des rôles liée à la nature de la prestation doit être établie et tenue à jour par le Titulaire et communiquée à l'AMF.

Concernant les infrastructures mutualisées nécessaires à l'exécution du service, le Titulaire décrira les principes de séparation des fonctions mise en œuvre pour assurer leur sécurité.

Sur le plan organisationnel, il est notamment attendu une séparation effective des rôles sécurité et production.

Le Titulaire doit répercuter l'ensemble des obligations liées à la sécurité et la confidentialité à ses collaborateurs ou ses sous-traitants participant à l'exécution de la prestation.

11.8.4.2. Délivrance et retrait des accès aux actifs de l'AMF

Les processus de délivrance et retrait des accès physiques aux actifs qui supporteront le SI Sûreté de l'AMF devront être décrit dans la PSSI ou le PAS.

Les accès aux actifs du Titulaire participant à l'exécution du service doivent faire l'objet de mesures de restriction appropriées au contexte de sécurité. Le Titulaire fournira à l'AMF une description synthétique des modalités d'accès mises en place.

11.8.5. La protection physique et logique des environnements

Le Titulaire est tenu d'assurer la protection physique et logique des environnements portant des données de l'AMF.

Il est demandé à ce titre que :

- ☐ L'environnement applicatif soit maintenu en tenant compte des recommandations d'application de correctifs par les éditeurs, sauf spécification contraire de l'AMF ;
- ☐ Les entrées utilisateurs soient rigoureusement contrôlées ;
- ☐ Les accès aux fonctions d'administration soient sécurisés.

11.8.6. La sécurité des développement applicatifs

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

Voici les règles minimales qu'il sera demandé d'appliquer :

- ☐ Le minimum de fonctions nécessaires sont embarquées lors de l'installation ;
- ☐ Le principe du moindre privilège est appliqué ;
- ☐ L'utilisation de mots de passe dans le code est interdite ;
- ☐ Une gestion efficace des erreurs est mise en œuvre ;
- ☐ La possibilité d'autoriser ou d'interdire l'accès aux informations de son Smartphone est toujours laissée à l'utilisateur ;
- ☐ L'utilisateur a un ID unique et un mot de passe que lui seul connaît ;
- ☐ Les données doivent être conservées dans un but clairement défini et pas au-delà du temps nécessaire ;
- ☐ Les communications doivent être chiffrées avec des protocoles robustes, autant que possible.

Pour la mise en œuvre de technologies web et mobile, les développements devront être conformes aux recommandations de l'ANSSI (Agence Nationale de Sécurité des Systèmes d'Information).

Le code de l'application est régulièrement revu, à minima à chaque nouvelle version, afin de s'assurer d'une implémentation conforme aux exigences de sécurité. La correction d'éventuelles anomalies ou vulnérabilités applicatives détectées lors de la revue de code par le Titulaire ou l'AMF sont à la charge du Titulaire et devront être implémentée selon un planning choisi et communiqué par l'AMF.

11.8.7. La continuité de service

Le Titulaire indiquera les mesures techniques, organisationnelles, procédurales qu'il s'engage à prendre pour assurer la continuité d'activité du système, ou en cas de sinistre la reprise d'activité conformément aux exigences définies dans le PAQ.

Les procédures de sauvegarde et de secours seront décrites.