APPEL D'OFFRES N°78/2021/C

Acquisition Et Mise En Œuvre D'une Solution de gestion des vulnérabilités

PIECE N°3

CAHIER DES CLAUSES TECHNIQUES PARTICULIERES

C.C.T.P

NB : Le présent cahier de charges, visé par le soumissionnaire doit accompagner l'offre

SOMMAIRE

1. OBJECTIFS

REDAL vise à travers le présent appel d'offres à acquérir et à mettre en œuvre une solution de gestion des vulnérabilités lui permettant d'identifier et corriger les failles de sécurité existantes sur ses actifs IT et OT de façon proactive.

2. EXIGENCES GENERALES DE LA SOLUTION CIBLE

Dans le cadre de cet appel d'offres, le(s) soumissionnaire (s) devra fournir tous les prérequis nécessaires pour la mise en œuvre optimale et complète des solutions cibles (Hardware, software et licences). Les solutions proposées par le(s) soumissionnaire(s) doivent pouvoir répondre aux exigences suivantes :

- **Compatibilité** : Le prestataire doit justifier dans son offre technique la compatibilité de sa solution avec l'infrastructure existante au niveau des Datacenter de REDAL.
- **Fiabilité :** Les solutions proposées doivent offrir un niveau de résilience et de robustesse très élevé garantissant la fiabilité globale des systèmes mis en place.
- **Performance :** Toute la configuration proposée doit être optimale et évolutive permettant d'assurer un niveau maximal de performance.
- **La Sécurité :** Les solutions proposées doivent disposer d'un très haut niveau de sécurité et de mécanismes de protection avancés.
- **Facilité d'administration**: Toutes les briques des solutions proposées doivent être dotées d'un outil d'administration et de gestion à base d'interface utilisateur simple à utiliser.
- **Évolutivité et flexibilité :** Les solutions proposées doivent être évolutive en termes de capacité et de performance.
- **Impact sur les systèmes de production :** La mise en place des solutions proposées ne doivent pas impacter le niveau de performance et de disponibilité des systèmes de production de la REDAL.

La solution proposée pour répondre aux spécifications techniques décrites dans ce cahier des charges doit être fournie sous sa dernière version disponible au moment de la livraison, ainsi que toutes les licences garantissant le bon fonctionnement de la solution objet de cet appel d'offres.

3. DESCRIPTION DE L'EXISTANT

REDAL dispose d'une infrastructure informatique hétérogène basée sur des solutions et des équipements de différents constructeurs /éditeurs. Il dispose entre autres des technologies ci-dessous :

- Plate-forme de virtualisation: VMWARE / POWER VM …
- Différents serveurs d'application (Microsoft, Oracle, Apache, Tomcat…)
- Serveurs sous Windows et Unix (Linux, AIX…)
- Différents équipements réseau notamment CISCO, Fortinet, Forcepoint …

- Solutions SIEM et ITSM de Micro Focus

NB : Plus de détails techniques peuvent être fournis lors de la visite des lieux

3. CONSISTANCE DES PRESTATIONS

La solution attendue doit être installée et mise en œuvre par le(s) soumissionnaire(s) à travers des prestations de haute qualité permettant de tirer le maximum de la solution proposée.

L'implémentation des différentes composantes des plateformes proposées devra être assurée par des équipes certifiées par les éditeurs sur la solution proposée.

Toutes les opérations d'installations et configurations doivent être incluses dans le prix du marché.

Les opérations doivent comprendre ce qui suit :

- Le soumissionnaire est invité à effectuer une visite des lieux de chaque site, pour apprécier à juste valeur l'architecture technique des plateformes en exploitation et devant fonctionner en interaction avec la solution technique à mettre en place dans le cadre du présent appel d'offres et évaluer la consistance de la mission à réaliser.

  Une attestation de visite des lieux dûment signée est à fournir obligatoirement au dépôt de la soumission ;

- Le soumissionnaire doit fournir une attestation d'engagement signée par le constructeur, indiquant l'aptitude du soumissionnaire à livrer, installer et mettre en service les produits fournis ;
- Le soumissionnaire devra prévoir une présentation de son offre technique dans les locaux de la REDAL avant le jugement technique des offres ;
- Détermination d'architecture, prérequis nécessaire et plan de mise en œuvre de toutes les briques de la mise en œuvre de(s) solution(s) cible selon les besoins de REDAL et en tenant compte de l'existant et l'avancement des projets en cours.
- Lors de la phase d'installation : installer, paramétrer et configurer la solution selon l'architecture validée par l'équipe projet de REDAL.
- Le titulaire s'engage à assurer la mise en œuvre des fonctionnalités attendues de la solution cible en tenant compte du site d'hébergement des infrastructures (deux sites au total). Il doit également prendre à sa charge tout autre outil jugé nécessaire inclue l'installation, la configuration pour garantir le bon fonctionnement de la solution proposée.
- Assistance pendant après la mise en production en vue d'ajuster la configuration pour une utilisation optimale.
- Implication forte de l'équipe Projet de la REDAL tout au long de la durée de mise en œuvre, afin d'assurer un transfert de compétences et une maîtrise totale des technologies de l'infrastructure à mettre en place.
- Fournir et développer les procédures nécessaires pour sauvegarder et restaurer les environnements.

- Fournir un document de recette avec les procédures de test de bon fonctionnement.

- Le soumissionnaire doit proposer une formation sur l'ensemble des modules proposés et assurer un transfert de compétences aux équipes informatiques de la REDAL durant toute la phase de mise en œuvre.

4. SPECIFICATION DE LA SOLUTION CIBLE

La solution cible doit être sécurisée, basée sur une architecture simple, hautement disponible et hébergée sur un serveur central installé au Datacenter, elle doit permettre :

- **Gestion des accès et habilitations :** la solution doit intégrer un module pour le contrôle d'accès hiérarchique déterminé par le profil de l'utilisateur et des niveaux de privilège sur la solution.

- **Découverte statique des actifs (mappage) :** La solution doit être capable de mapper tous les systèmes présents sur le réseau. Le système doit identifier rapidement tous les actifs installés (constructeur/éditeur, services actifs, OS, logiciels installés,) à partir d'une adresse IP ou d'une plage d'adresse IP saisies.

- **Découverte dynamique des actifs (mappage):** La solution doit permettre de s'intégrer avec des recueils de machines tels VMware vSphere et DHCP afin de réaliser des scans de ces machines dès qu'elles sont actives sur le réseau sans avoir à préciser la liste des adresses IP.

- **Détection des vulnérabilités (Test de vulnérabilités) :** La solution doit disposer d'une base de connaissances fiable et actualisée plusieurs fois par jour avec des vérifications des nouvelles vulnérabilités et des améliorations apportées aux signatures existantes. Le processus de mise à jour doit être totalement automatisé.

- **Audit des configurations :** La solution doit prendre en charge les scans authentifiés afin de faire des analyses de conformité

- **Intégration :** La solution doit s'intégrer facilement avec les solutions existantes (SIEM, Patch management et ITSM). La solution doit aussi disposer d'une API ouverte/publique.

- **Notification et gestion des tickets et suivi de vulnérabilités :** La solution doit intégrer des fonctionnalités de suivi des vulnérabilités (génération de tickets, affectation, suivi des remédiations) et s'intégrer avec la solution SMAX et ServiceNow

- **Rapports :** Les rapports générés par la solution doivent permettre de répondre aux exigences de l'ISO 27001. La solution doit permettre entre autres de générer les rapports suivants:
  - Tableaux de Bords / Dashboards
  - Des analyses de tendances
  - Des analyses des vulnérabilités exploitables
  - Des informations détaillées sur les vulnérabilités découvertes

- Des options de filtrage et de tri pour obtenir des vues personnalisées des données
- Des rapports de conformité aux standards

La solution doit permettre l'exportation des rapports générés vers des applications externes aux formats PDF, HTML, CSV et XML.
La solution proposée doit supporter comme évolution future des fonctionnalités permettant de lancer des tests d'intrusion applicatifs via la même console.

5. PRESENTATION DE L'OFFRE

5.1 Présentation générale de l'offre

L'offre technique doit inclure obligatoirement les informations ci-dessous :

- La description détaillée des solutions techniques proposées ainsi que les éléments d'appréciation de ces solutions. Il y a lieu notamment de fournir :
  - Les schémas d'architecture technique à mettre en place au niveau de chaque site de la REDAL.
  - La description des moyens prévus pour assurer la haute disponibilité de la solution.
  - La description de toutes les fonctionnalités de la solution proposée.
  - La description détaillée fonctionnelle et technique des procédures et stratégies à mettre en œuvre.
  - La description de l'évolutivité de la solution proposée
  - La description de la méthodologie et organisation de la mise en œuvre du projet
  - La description de l'intégration avec l'existant
  - La description des livrables du projet
  - Les CVs de l'équipe projet
  - Les prérequis et recommandations hardware et software d'installation de la solution

- Un planning détaillé de réalisation du projet : Livraison des licences, Installation, Paramétrage et configuration, Intégration avec les plateformes existante, Elaboration des procédures et Mise en œuvre des solutions proposées, Formation et Transfert de compétences ;
- Un support éditeur de minimum **(01)** an doit être fourni avec les licences ;
- La politique de tarification sur une période de 5 ans comprenant en détail un engagement sur le coût des add-on des toutes les composantes logicielles proposées : liste à fournir ;
- Une proposition de contrat de maintenance conforme au niveau de service décrit dans le présent cahier des charges ;
- Le tableau de conformité technique dûment complété tel que décrit ci-dessous renseignant ainsi sur la conformité totale, partielle, ou la non-conformité de l'offre par rapport aux exigences demandées dans le cadre du présent cahier des charges.

5.2 Tableau de conformité

Chaque soumissionnaire est tenu de remplir le tableau de conformité ci-après. Ce tableau représente ce même cahier des charges mis sous format de tableau où la première colonne représente les clauses et les spécifications de ce cahier des charges et les deux autres colonnes sont réservées au soumissionnaire pour apporter ses remarques ou ses réponses en termes de conformité ou non-conformité.

Exigence CPT	CONFORMITE (T: Totale, P: partielle, N : Non conforme)	OBSERVATION (Si applicable)
L'offre technique contient la description détaillée des solutions techniques proposées		
Les schémas d'architecture technique à mettre en place au niveau de chaque site		
Les spécifications techniques de chaque plateforme technique et de chaque variante logicielle proposée au niveau de la plateforme.		
Le planning détaillé de réalisation du projet :		
mise en œuvre des solutions proposées, formation et transfert de compétences		
L'offre contient tous les équipements qui ne seraient pas mentionnés dans le bordereau des spécifications techniques et qui seraient nécessaires au bon fonctionnement du logiciel livré et/ou à intégrer ainsi qu'à la mise en œuvre de la solution ciblée pour chaque site		
Présentation détaillée des moyens du soumissionnaire : -Moyens humains et logistiques -Attestations de prestations similaires -Certificats et/ou attestations de partenariat délivré par les éditeurs/constructeurs		
Exigences techniques		
Précision de l'Editeur et du nom de la solution proposée		
Précision du type de licence et la version proposée		
La solution doit s'installer dans l'environnement virtuel de l'entreprise.		
La solution proposée doit être fournie en mode on-premise, autrement dit pas d'offres en cloud.		

La distribution et la version la plus recommandée par l'éditeur.		
L'OS de la solution doit être sur 64 bits		
Installation sur Linux		
La solution doit supporter l'authentification à 2FA		
Soumettre des simulations d'attaques aux utilisateurs		Détailler les simulations possibles
La solution intègre un module pour le contrôle d'accès hiérarchique déterminé par le profil de l'utilisateur et des niveaux de privilège sur la solution.		
Les soumissionnaires sont invités à proposer une solution pour au moins 128 adresses IP.		
La solution doit être extensible, en permettant une architecture distribuée avec console centralisée et possibilité de dispatcher plusieurs moteurs de scans ou d'analyses sans couts additionnels pour supporter une infrastructure évolutive.		
L'administration de la solution doit être centralisée.		
La solution doit supporter la découverte automatique des actifs de l'entreprise (serveurs, postes de travail, routeurs, points d'accès sans fil et autres équipements réseau) et la catégorisation de ces derniers en se basant sur multiples critères.		
La solution proposée doit contenir des templates de scan prédéfinis et personnalisables selon nos besoins de sécurité.		
La solution proposée doit offrir la possibilité de lancer des scannes en spécifiant une vulnérabilité spécifique sur un ensemble de catégories de vulnérabilités.		
La solution proposée doit offrir la possibilité d'inclure ou d'exclure des types de vérifications / checks au sein des templates de scan.		
La solution doit être capable de traquer un actif malgré le changement de son adresse IP.		
La solution doit disposer de mécanismes pour exécuter des scans authentifiés sur différentes plateformes, et la solution doit aussi proposer un moyen de créer un		

recueil des identifiants et mots de passe couramment utilisés.		
La solution doit supporter la planification des scans selon des templates prédéfinis ainsi que l'envoi des rapports par email automatiquement.		
La base de vulnérabilité de la solution proposée doit inclure les bulletins de vulnérabilités publiés par les éditeurs/constructeurs des solutions de système d'information, et les bulletins publiés dans les bases mondiales telles que SANS, CERT, NVD,…		
La base des vulnérabilités doit être mise à jour fréquemment pour couvrir les vulnérabilités récentes (0-Day).		
L'éditeur doit être reconnu comme un leader du domaine de la gestion des vulnérabilités par des analystes indépendants (Gartner, Forrester, ou équivalent…).		
L'éditeur de la solution proposée doit être reconnu CNA (CVE Numbering Authority) par l'organisme MITRE qui gère la base publique des vulnérabilités.		
La solution doit supporter la possibilité d'ajouter une signature de vulnérabilité définis par l'utilisateur.		
La solution doit donner la possibilité à l'utilisateur de choisir de faire une découverte des actifs, scanner des vulnérabilités et faire des audits de conformité.		
La solution proposée doit pouvoir scanner tous les systèmes sans installation ni utilisation d'agents.		
La solution proposée doit intégrer un modèle d'analyse SCADA (une Template moins agressive adaptée aux systèmes sensibles afin d'évacuer tout risque de saturation de ces systèmes lors des opérations de scan)		
La solution doit intégrer un mécanise de calcul de valeur de risque qui ne submerge pas l'administrateur avec un nombre important de corrections à faire. En plus de la valeur CVSS (Common Vulnerability Scoring System), la valeur du risque doit prendre en considération d'autres facteurs, tel que l'age des vulnérabilités, l'exploitabilité des vulnérabilités, la disponibilité de malwarekit, ...etc.		

Dans le cas où le risque d'une vulnérabilité est accepté par l'utilisateur, la solution proposée doit permettre d'exclure cette vulnérabilité au niveau globale ou au niveau de l'actif avec documentation.		
La solution doit fournir des modèles de rapports préconfigurés et l'option de personnaliser les rapports.		
La solution doit fournir la capacité de générer des rapports selon un planning prédéfinis.		
Les rapports doivent être envoyés par e-mail aux équipes concernées.		
La solution doit permettre une flexibilité dans la génération des rapports, en donnant la possibilité de créer des filtres ou des attributs pour cadrer les rapports au besoin.		
La solution proposée doit permettre à l'utilisateur d'extraire des rapports selon plusieurs formats: PDF, HTML, XML, CSV.		
La solution proposée doit permettre à l'utilisateur de vérifier que la configuration des actifs est sécurisée en se référant à des références et des benchmarks mondiales, tel que: CIS, PCI, SOX.		
La solution doit permettre de de mettre en place des politiques de compliance personnalisées.		
La solution doit être intégrable avec l'environnement virtuel de Redal		
La solution doit être intégrable avec la solution SIEM « Arcsight »		
La solution doit s'intégrer avec LDAP/Active Directory		
La solution doit s'intégrer avec Kerberos et SAML 2.0		
La solution doit être construite sur une API ouverte et documentée qui permet d'automatiser un maximum d'actions sans avoir recourt à la console de management.		
La solution doit supporter l'attribution des privilèges aux utilisateurs avec une capacité à mettre en œuvre des filtres pour les hôtes qu'un utilisateur est autorisé à		

scanner.		
La solution doit permettre les mises à jour d'une manière automatique ou manuelle.		
Les mises à jour doivent couvrir une alimentation régulière de la base des vulnérabilités avec les dernières vulnérabilités découvertes.		
La solution permet d'implémenter toutes les exigences d' ISO 27001 en matière de gestion des vulnérabilités		
La solution doit être capable d'identifier les vulnérabilités exploitables et de fournir des informations détaillées associées aux exploits. Les résultats de ces informations doivent être utilisés dans le calcul de risque pour permettre une gestion de risque performante (Minimum Pour un utilisateur)		
La solution doit scanner les applications web pour trouver les vulnérabilités et les configurations non sécurisées, y compris celles du OWASP TOP 10.		Critère devant être pris en compte par la solution proposée pour une évolution future
L'offre inclut tous les prérequis permettant de scanner différents réseaux sur différents sites		
L'offre inclut 01 an de support éditeur		

Remarque:

- Le soumissionnaire doit fournir en détail les caractéristiques techniques de la solution proposée avec notamment la fourniture d'un schéma global d'architecture.
- Le soumissionnaire pourra proposer d'autres fonctionnalités supplémentaires **(Toute proposition sera prise en considération dans la note de jugement des offres)**.

6. OBLIGATION DU TITULAIRE

Le titulaire est tenu de présenter auprès du maitre d'ouvrage les pièces suivantes :

- Les Curriculums Vitae, détaillés et portant le cachet de l'entreprise, des personnes que le prestataire s'engage à affecter pour la réalisation du présent projet. L'implémentation des différentes composantes de l'infrastructure proposée devra être assurée par une équipe spécialisée et certifiée constructeur. Les membres de l'équipe doivent avoir au minimum les spécialités suivantes :

- Un Ingénieur ou équivalent **responsable de la gestion du projet** est indispensable, ayant au moins 5 ans d'expérience justifié autant que chef de projet de même grandeur ou plus.
- Un Ingénieur ou équivalent **certifié sur la solution proposée** dans le cadre de cet appel d'offres, ayant au moins 3 ans d'expérience et un niveau de certification expert.

- Une liste nominative du personnel affecté au projet doit faire l'objet d'un tableau récapitulatif selon le format suivant :

Nom & prénom	Rôle dans le projet	Diplômes	Certificats obtenus	Années d'expériences

Les membres de l'équipe projet proposée par le titulaire ne peuvent être remplacés par de nouveaux membres qu'après accord écrit du Maitre d'Ouvrage. Si pour des raisons, indépendantes de la volonté du Titulaire (justifiables), il s'avère nécessaire de remplacer un des membres de l'équipe projet, le Titulaire fournira immédiatement une personne de qualification égale ou supérieure qui doit recevoir l'approbation du Maître d'ouvrage.

REDAL garde le droit de remplacer à tout moment un membre de l'équipe, si il n'est pas satisfait de sa performance ou de ses compétences, ou découvre qu'il s'est rendu coupable de vulgarisation des données de la REDAL, le Titulaire devra, sur demande du Maître d'ouvrage, fournir dans un délai de cinq jours au maximum, un remplaçant dont les qualifications et l'expérience seront soumises à l'approbation du Maître d'ouvrage.

Le Titulaire ne pourra pas soumettre des demandes de paiements au titre des coûts supplémentaires résultant du retrait ou remplacement du personnel.

Représentation du Titulaire et Gestion du Projet

- Le Titulaire désignera un représentant auprès du Maître d'ouvrage muni des pouvoirs nécessaires pour assurer tout le suivi du projet.
- Le Titulaire participera à une réunion de démarrage qui sera organisée dès l'entrée en vigueur du marché à la demande du maître d'ouvrage. La réunion aura pour objet la finalisation des diverses composantes du projet (prérequis, étapes, jalons, livrables, intervenants et organisation des prestations), la vérification des interfaces et la coordination des plannings (élaborer le planning d'exécution du présent marché).
- Le Titulaire s'engage à donner suite à toute demande d'information permettant au Maître d'ouvrage d'assurer le contrôle du projet.
- Le Titulaire doit valider préalablement le plan de chaque livrable avec le Maître d'ouvrage.
- Le Titulaire assurera le pilotage et le suivi de la maîtrise d'œuvre du projet et, à ce titre, devra :
    - Gérer l'avancement du projet, en veillant au respect des plannings
    - Assurer le Reporting dans un tableau de bord hebdomadaire
    - Assurer la coordination des équipes.

Le titulaire du projet doit communiquer chaque vendredi au maitre d'ouvrage, le bilan d'avancement des travaux. Il doit présenter toutes les actions qui devront être menées. Ces actions doivent être priorisées selon l'urgence et selon le degré de gain en qualité et en performance.

Des réunions périodiques doivent être prévues pour la présentation de l'état d'avancement des travaux.

Dans ce cadre, un tableau détaillé d'avancement devra être tenu à jour par le Titulaire et communiqué au maître d'ouvrage.

Le Titulaire devra mobiliser le personnel nécessaire pour mener le projet dans les délais prévus. Si des retards ou des écarts sont constatés, il devra fournir les ressources nécessaires et de qualité pour les rattraper. Il devra faire appel, chaque fois que nécessaire, à des experts du domaine (même non prévus au début de sa mission) afin de dépasser d'éventuelles difficultés qui viendraient à survenir.

Il devra aussi, dans le cadre de l'exécution du présent marché :

- Mettre en place les outils et les documents méthodologiques liés à l'objet contractuel de la mission ;
- Élaborer les procès-verbaux des réunions tenues au cours du déroulement de sa mission;
- Mobiliser toutes les ressources humaines et matérielles qui lui seront nécessaires à la bonne exécution du marché dans les meilleurs délais.

Le Titulaire s'engage à respecter les exigences de la charte de sécurité des prestataires ainsi que la politique de sécurité du système d'information en vigueur à REDAL.

7. ADD-ON

Les soumissionnaires s'engagent obligatoirement sur le prix maximal des add-ons communiqués dans leurs offres pour les 5 années à venir. Ils doivent préciser dans leurs offres le coût de l'extension suivante :

- Licence pour 128 adresses IP supplémentaires
- Licence de scan applicatif pour 10 applications
- Licence Pentest pour un utilisateur supplémentaire

8. FORMATION ET TRANSFERT DE COMPETENCES

➢ Formation

Les concurrents doivent proposer des formations pour former deux administrateurs techniques sur l'ensemble des modules proposés, afin de leur permettre d'acquérir les compétences nécessaires pour gérer et prendre en charge la solution proposée. Les frais des formations proposées seront à la charge des soumissionnaires.

Les formations doivent être dispensées obligatoirement avant le commencement des travaux d'installation et de configuration sur site.

Les soumissionnaires sont tenus de :

- Présenter les justificatifs des compétences, certificats et références d'un instructeur **Francophone** du constructeur, attestant d'un niveau d'expertise technique sur le logiciel objet de l'appel d'offres et d'une méthodologie pédagogique éprouvée. Des copies de certificats sont à fournir dans l'offre ;
- Justifier dans leurs offres techniques que les sessions de formation seront déroulées dans un centre de formation permettant aux participants de bien assimiler le thème de la formation.
- Lesdits centres doivent être spécialisés dans le métier de la formation aux nouvelles technologies de l'information. Les salles de formation doivent être équipées de matériels pédagogiques et techniques récents, adaptés aux formations dispensées ;
- Un manuel de formation est à fournir à chaque participant bénéficiant de la formation (en langue française de préférence).
- Garantir tout au long de la formation, une alternance de l'aspect théorique avec des ateliers pratiques (50% théorie - 50% pratique), l'objectif étant de permettre aux participants de valider leurs acquis ;
- Délivrer des attestations de suivi des formations dispensées au profit des participants ;
- Délivrer un support de cours qui constitue une véritable référence pour les administrateurs, édité par l'éditeur officiel et utilisable pendant et après la formation ;

➢ Transfert de compétences :

Le Prestataire s'engagera à transmettre aux équipes techniques du Client les compétences nécessaires à la maîtrise du projet, depuis l'installation, l'administration, le paramétrage, les tests fonctionnels, la mise en marche, la configuration, l'exploitation, la maintenance des logiciels et toutes les technologies employées dans le cadre de la solution proposée.
Ce transfert de compétence se fera de manière continue, au cours de la réalisation de la prestation.
Le Prestataire assistera le Client durant toutes les phases du projet : étude, test, et réalisation.

9. GARANTIE ET MAINTENANCE

Le Titulaire garantit que tous les équipements et logiciels livrés en exécution du marché sont neufs. Il garantit en outre que le matériel et logiciels livrés en exécution du marché n'auront aucune défectuosité quant à leur conception, aux matériaux utilisés ou à leur mise en œuvre ou à tout acte ou omission du Titulaire.

Cette garantie s'étend à tous les équipements et logiciels sans aucune exception sur une période de **Douze (12) mois**. Ce délai de garantie commence à courir à partir du lendemain de la date de la réception provisoire prononcée par le Maître d'Ouvrage.

Le(s) éditeur(s) des solutions proposées devra disposer d'une équipe de support locale prête à intervenir sur site en cas d'incident.

Tous les logiciels proposés doivent être souscrits au support officiel de leurs éditeurs avec attestation de l'éditeur à l'appui.

Le titulaire doit fournir au préalable les informations nécessaires du support : Téléphone, Fax et Email.

Le Titulaire doit fournir à la livraison une attestation de garantie finale des éditeurs des différents composants de la solution proposée pour une durée minimale de 1 an.

Pendant cette période de garantie, le Titulaire dispensera au Maître d'ouvrage le service suivant :

- Le rétablissement de la conformité des solutions et des services aux spécifications annoncées dans le présent CPS et dans l'offre du titulaire;
- Intervenir sur appel de l'Administration pour remettre en état de fonctionnement la solution et les services défectueux :

Le TITULAIRE doit prendre en charge la demande d'intervention du maître d'ouvrage objet de ce marché dans un délai maximum d'une (1) heure à partir de la demande (Téléphone, fax ou Email) sur une base de 24hx7j. Le système de production doit être remis dans son état normal dans les quatre heures qui suivent la demande d'intervention.

- Informer par écrit le maître d'ouvrage des mises à jour parues et les installer à la demande de ce dernier.

L'entretien préventif comprend les mises au point nécessaires :

- Mise à jour des solutions proposées;

10. CONTRAT DE MAINTENANCE

Le concurrent doit proposer dans son offre un contrat de maintenance qui prendrait effet à la fin de la période de garantie pour résoudre les incidents /difficultés rencontrées par REDAL lors de l'exploitation du logiciel mis en œuvre dans le cadre de cet AO avec un niveau de service équivalent à celui dispensé durant la période de garantie.

En cas de non-respect des délais de résolution des incidents stipulés dans le contrat de maintenance, sauf cas de force majeure, le titulaire sera soumis à une pénalité de retard qui sera calculée selon la formule suivante :

$$P = (V * R) / 364$$

P = le montant de la pénalité ;

V = la valeur de la rémunération annuelle versée au titre de la maintenance ;

R = le nombre de jours de retard.

Lu et approuvé par le soumissionnaire

Cachet et signature du soumissionnaire