SPL DESTINATION LES SABLES D'OLONNE

MARCHE DE FOURNITURE ET DE SERVICES

CAHIER DES CHARGES UNIQUE

VALANT REGLEMENT DE CONSULTATION

Prestation de mise en place d'un système d'infogérance et de sécurité informatique pour l'exploitation des Sables d'Olonne Arena et du domaine SPL

Pouvoir adjudicateur

SPL Destination les Sables d'Olonne

Adresse **: 1 promenade Wilson – 85100 LES SABLES D'OLONNE**

Date limite de réception des offres : jeudi 5 juin 2025 - Heure : 12h00

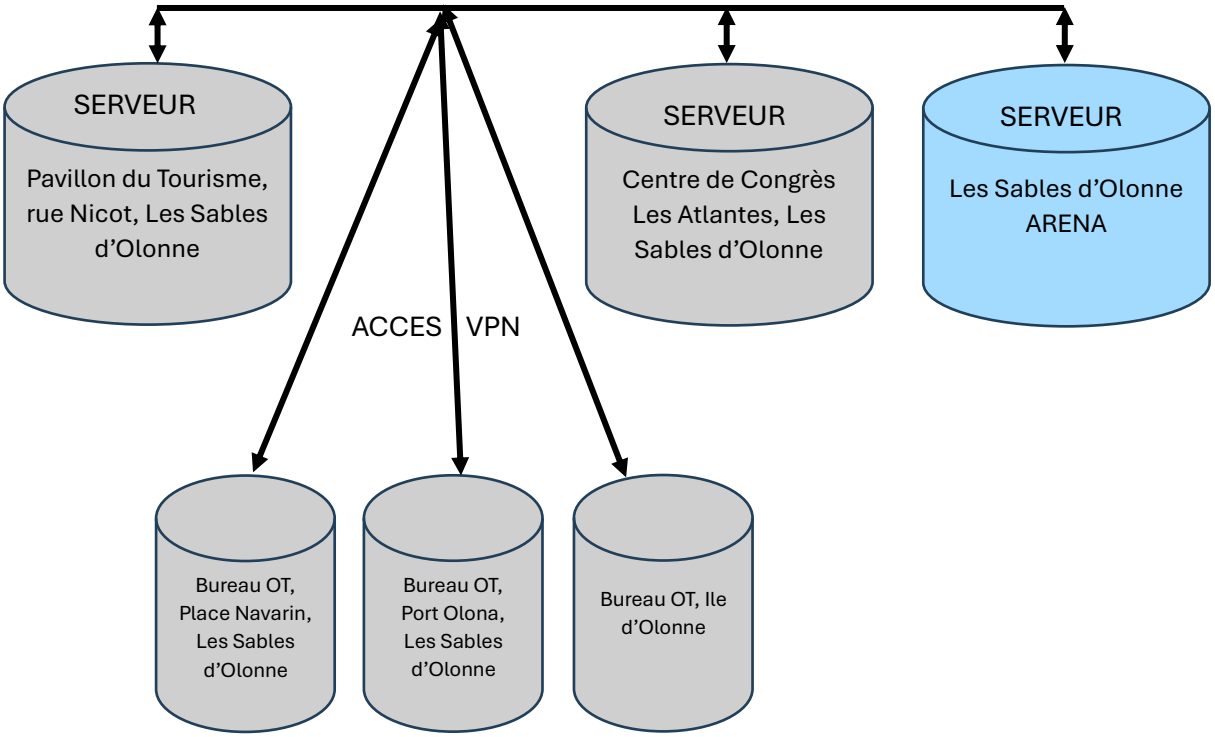
1. Principes généraux de fonctionnement

1.1. Environnement du domaine IT de la SPL Destination Les Sables d'Olonne

La SPL Destination Les Sables d'Olonne exploite plusieurs établissements. Ces établissements sont équipés informatiquement et forment un même domaine.

Tous les établissements sont dotés d'un accès à l'Internet. La téléphonie est gérée en voix sur IP (outil 3Cx). Les serveurs de data des sites Pavillon du Tourisme et Centre de Congrès Les Atlantes communiquent (dont sauvegarde en miroir).

L'organisation de ce domaine est schématiquement décrite ci-dessous :



Les Sables d'Olonne Arena intègre cet environnement de travail au même niveau que le Pavillon du Tourisme et le Centre de Congrès Les Atlantes.

Le déploiement de la solution retenue devra être opérante (a minima pour un fonctionnement des outils téléphoniques de sécurité réglementaire (voix sur IP)) à la date d'exploitation prévisionnelle du 11 juin 2025 pour les équipements de l'Arena.

1.2. Objectifs généraux

Le programme IT de la SPL Destination Les Sables d'Olonne vise à établir une infrastructure technologique complète et évolutive, répondant aux besoins des différents espaces exploités. Les objectifs principaux sont les suivants :

- Interconnexion et infrastructure réseau : Assurer une connectivité fluide et sécurisée entre tous les bâtiments du domaine avec une redondance optimale pour éviter toute interruption de service.
- Performance et accessibilité : Déployer une infrastructure IT capable de supporter des évènements a forte affluence et garantir une navigation fluide pour les visiteurs, les organisateurs et les exploitants.
- Sécurité des données et cybersécurité : Mettre en place des protocoles de protection des données, incluant la gestion des accès, la surveillance en temps réel et la résilience aux cyberattaques.
- Solutions audiovisuelles et multimédia : Intégrer des systèmes de captation, de diffusion et d'interactivité adaptes aux divers usages (spectacles, conférences, retransmissions sportives, etc.).
- Expérience utilisateur améliorée : Développer des solutions digitales pour fluidifier l'accès aux évènements (billetterie en ligne, contrôle d'accès intelligent, signalétique interactive, etc.).
- Smart Building et IoT : Exploiter l'Internet des objets pour optimiser la gestion énergétique, la maintenance prédictive, le confort des usagers ainsi que la gestion des différents bâtiments pour une organisation plus légère.
- Mobilité et logistique : Optimiser la gestion des parkings, des transports et de la logistique des évènements grâce a des solutions numériques intelligentes.
- Evolutivité et pérennité : Concevoir une architecture flexible, raisonnablement et justement dimensionnée et pouvant s'adapter aux évolutions technologiques et aux besoins futurs du site.

1.3. Schéma directeur et principes

L'architecture réseau du projet Les Sables d'Olonne est un élément garantissant la connectivité et la performance des infrastructures technologiques. Elle doit permettre la gestion fluide des flux de données, l'interconnexion des bâtiments, la sécurisation des communications et l'évolutivité des services. Le réseau sera conçu pour répondre aux besoins des utilisateurs internes (gestionnaires, personnel technique, artistes, sportifs), des visiteurs (spectateurs, touristes, journalistes) ainsi que des infrastructures (capteurs IoT, caméras de surveillance, systèmes de billetterie, plateformes multimédias).

Disponibilité élevée (HA - High Availability) :

- Redondance des équipements critiques (Routeurs, Switch, Firewall).
- Multiplication des liaisons fibre optique pour éviter les points de défaillance uniques.
- Mise en place de protocoles de basculement automatique en cas de panne (HSRP, VRRP).

Sécurité et cloisonnement des flux :

- Isolation des différents usages via des VLANs (administration, visiteurs, IoT, streaming).

- Filtrage du trafic avec des firewalls nouvelle génération (NGFW).
- Protection contre les attaques *DDoS* avec des systèmes IDS/IPS.

Evolutivité et compatibilité :

- Conception ouverte permettant l'intégration de nouvelles technologies.
- Intégration d'un réseau défini par logiciel (SDN) pour une gestion dynamique.

Optimisation des performances et de la latence :

- Utilisation de technologies a faible latence pour le streaming et la vidéoconférence.
- Priorisation des flux critiques via la QoS (Quality of Service).

Interopérabilité avec les infrastructures existantes :

- Compatibilité avec les équipements audiovisuels, les systèmes de billetterie, les dispositifs IoT.
- Centralisation de la gestion a travers un Network Operations Center (NOC).

1.4. Sécurité et gestion du réseau

L'architecture de sécurité et de gestion du réseau devra répondre aux exigences suivantes :

- Protection contre les cybermenaces : Attaques DDoS, ransomware, phishing, etc.
- Segmentation et isolation des flux : Séparer les réseaux visiteurs, exploitation, IoT et sécurité.
- Haute disponibilité et redondance : Minimiser les interruptions en cas de panne ou d'incident.
- Conformité aux recommandations de l'ANSSI.
- Gestion optimisée : Automatisation des taches critiques pour améliorer la réactivité et réduire les couts d'exploitation.

> Architecture de sécurité réseau

La stratégie de sécurité repose sur une approche Zéro Trust, ou chaque connexion et chaque utilisateur sont authentifiés avant d'accéder aux ressources du réseau.

- Pare-feu et filtrage avancé
    - Firewalls) intégrant la détection d'intrusions (IPS/IDS).
    - Filtrage URL & DNS pour bloquer les sites malveillants et prévenir les attaques.
    - Inspection SSL/TLS pour identifier les menaces cachées dans le trafic chiffre.
    - Segmentation des réseaux (micro-segmentation) pour cloisonner les différents flux (staff, visiteurs, IoT, sécurité).

- Gestion des accès et authentification
    - Contrôle d'accès base sur les rôles (RBAC) pour restreindre les permissions.
    - Authentification multi-facteurs (MFA) sur tous les accès critiques.
    - Intégration du 802.1X pour sécuriser l'accès aux ressources réseau filaires et Wi-Fi.

    - Gestion centralisée des identités (IAM) pour une administration simplifiée et sécurisée.

- Protection contre les cyberattaques
    - Systèmes anti-DDoS pour détecter et atténuer les attaques volumétriques.
    - Supervision et analyse en temps réel des incidents de sécurité.
    - Plans de réponse aux incidents avec des protocoles clairs en cas de brèche de sécurité.

> Supervision et gestion du réseau

Une gestion proactive du réseau est essentielle pour garantir la disponibilité et la performance des infrastructures IT.

- Monitoring et détection des anomalies
    - Solutions NMS (Network Monitoring System) pour surveiller les équipements en temps réel.
    - Tableaux de bord et alertes en temps réel pour anticiper les dégradations de performance.

- Automatisation et gestion centralisée
    - Orchestration et automatisation via des plateformes.
    - Mise à jour automatisée des firmwares pour éviter les failles de sécurité.
    - Gestion des configurations et des politiques réseau via un SDN (Software Defined Network).

- Redondance et haute disponibilité
    - Topologie réseau redondante avec des liens multiples entre les sites exploités par la SPL pour éviter les points de défaillance.
    - Protocoles de basculement automatique (Failover) en cas de panne d'un équipement critique.
    - Plans de reprise d'activité (PRA) et de continuité d'activité (PCA) pour assurer un fonctionnement ininterrompu en cas de sinistre.

- Conformité et bonnes pratiques
    - Inventaire et cartographie : Maintenir un suivi précis des équipements connectés et des interconnexions pour une meilleure gestion des risques.
    - Sécurisation des systèmes critiques : Isoler les infrastructures sensibles (contrôle d'accès, vidéoprotection) pour limiter les impacts en cas d'incident.
    - Plan de reprise d'activité : Assurer des sauvegardes régulières et un mode dégradé pour garantir la continuité des services en cas de panne ou d'attaque.
    - Protection renforcée lors des évènements : Déployer une surveillance accrue et des mesures spécifiques pour prévenir les cybermenaces ciblant les grands rassemblements.

Le réseau IT devra respecter les normes de cybersécurité et de protection des données (RGPD notamment).

Des audits de sécurité réguliers seront effectués pour évaluer la conformité et tester la résilience du réseau face aux cyberattaques.

Le programme IT inclura une évolution continue de la sécurité réseau, avec notamment :

- Intégration de l'IA pour la détection comportementale des menaces.
- Cloud Security Posture Management (CSPM) pour sécuriser les infrastructures cloud hybrides.
- Zéro Trust Network Access (ZTNA) pour un accès sécurise aux applications distantes.
- Formation continue des équipes pour renforcer la sensibilisation à la cybersécurité.

Pour information, l'infrastructure IT sera construite autour d'une architecture virtualisée et hybride pour maximiser la flexibilité et la scalabilité du système.

- Infrastructure virtualisée
    - Hyperviseurs : type Proxmox, selon les besoins.
    - Virtualisation des serveurs : Consolidation des services IT sur des serveurs virtualises pour réduire l'empreinte matérielle et améliorer la tolérance aux pannes.
    - Infrastructure hyperconvergée (HCI) : Optimisation des ressources CPU, stockage et réseau.
    - Basculement automatique des VM en cas de panne matérielle (High Availability - HA).

L'objectif est d'assurer une flexibilité maximale, tout en garantissant une réduction des couts d'exploitation grâce à la mutualisation des ressources.

La gestion et la supervision des infrastructures IT et du réseau global de la SPL doivent garantir une disponibilité optimale, une réactivité en cas d'incident et une anticipation proactive des pannes. Pour cela, une approche centralisée et automatisée sera mise en place, combinant monitoring avance, gestion des configurations, supervision en temps réel et automatisation des taches de maintenance.

- Supervision centralisée et monitoring

  Un centre de supervision IT (NOC – Network Operations Center) sera mis en place pour surveiller en temps réel l'état des infrastructures.

    - Un tableau de bord unifié, accessible via une plateforme centralisée, permettra de suivre l'état du réseau, des serveurs, des systèmes de stockage et des applications critiques.
    - Surveillance en temps réel de la performance des équipements, avec génération d'alertes en cas de dysfonctionnement ou de seuil critique atteint (CPU, RAM, bande passante, température, etc.).

- Gestion des incidents et maintenance prédictive

  La gestion proactive des incidents repose sur un ITSM (IT Service Management) performant et une maintenance optimisée :

- Automatisation du traitement des incidents via un système ITSM (ServiceNow, GLPI, Zendesk), permettant de catégoriser automatiquement les demandes et de prioriser les interventions.
- Gestion des tickets avec SLA définissant des délais d'intervention selon l'impact métier des incidents.
- Maintenance prédictive basée sur des analyses de données et des tendances, permettant d'anticiper les pannes avant qu'elles ne surviennent.
- Tests en environnement isolé avant tout déploiement d'un correctif pour éviter tout impact sur la production.
- Mise à jour et application des correctifs critiques en mode automatique.

- Sauvegarde et plan de continuité

Pour assurer la résilience des infrastructures, une politique de sauvegarde et de récupération robuste sera mise en place :

- Sauvegarde automatique et externalisée des configurations et des données sur un site distant.
- Tests réguliers des procédures de restauration, garantissant la disponibilité des données en cas d'incident.
- Mise en place d'un PRA (Plan de Reprise d'Activité) et d'un PCA (Plan de Continuité d'Activité), assurant une reprise rapide après une panne ou une cyberattaque.
- Infrastructure de secours en mode miroir, synchronisée en temps réel avec le datacenter principal.

1.5. Stockage et gestion des données

Le datacenter proposera une infrastructure de stockage hybride pour répondre aux besoins de performance et de sécurité.

- Stockage principal : NAS/SAN (50 To) hybride combinant disques SSD NVMe pour les charges critiques et disques classiques pour l'archivage.
- Capacité de stockage initiale : 12 To, avec possibilité d'extension.
- Sauvegarde automatisée et réplication en temps réel sur un site distant pour garantir la résilience en cas de sinistre.
- Intégration de solutions de compression et de déduplication pour optimiser l'espace de stockage.

1.6. Suivi et évolution de la segmentation des réseaux et VLAN existants

Les flux seront séparés en plusieurs VLANs pour garantir une isolation et une sécurité optimales, exemples :

- VLAN 10 : Administration (gestion IT, support technique).
- VLAN 20 : Evènements et production audiovisuelle.
- VLAN 30 : WiFi public pour visiteurs et spectateurs.
- VLAN 40 : Systèmes de billetterie et contrôle d'accès.
- VLAN 50 : IoT (capteurs, éclairage, gestion énergétique).

- VLAN 60 : Vidéosurveillance

Chaque VLAN bénéficiera d'un filtrage spécifique à l'aide de listes de contrôle d'accès (ACL) et de firewalls afin de garantir une isolation stricte des flux de données et d'éviter toute intrusion. Les ACL fonctionnent comme un ensemble de règles définissant quels types de trafic sont autorisés ou bloqués entre les différents segments du réseau.

Elles permettent ainsi de restreindre l'accès aux ressources sensibles en fonction des adresses IP, des protocoles ou des ports utilisés, renforçant ainsi la sécurité globale du réseau.

La définition précises des besoins fera l'objet d'une réunion de lancement entre le candidat retenu et la SPL.

L'infrastructure IT sera construite autour d'une architecture virtualisée et hybride pour maximiser la flexibilité et la scalabilité du système.

- Infrastructure virtualisée
  - Hyperviseurs : type Proxmox, selon les besoins.
  - Virtualisation des serveurs : Consolidation des services IT sur des serveurs virtualises pour réduire l'empreinte matérielle et améliorer la tolérance aux pannes.
  - Infrastructure hyperconvergée (HCI) : Optimisation des ressources CPU, stockage et réseau.
  - Basculement automatique des VM en cas de panne matérielle (High Availability - HA).

L'objectif est d'assurer une flexibilité maximale, tout en garantissant une réduction des couts d'exploitation grâce à la mutualisation des ressources.

La gestion et la supervision des infrastructures IT et du réseau global de la SPL doivent garantir une disponibilité optimale, une réactivité en cas d'incident et une anticipation proactive des pannes. Pour cela, une approche centralisée et automatisée sera mise en place, combinant monitoring avance, gestion des configurations, supervision en temps réel et automatisation des taches de maintenance.

1.7. Réseau sans-fil Wifi

- <u>Sécurité et qualité de service (QoS)</u>

Pour garantir la sécurité et la performance du réseau Wi-Fi, plusieurs mesures seront mises en place :

- Authentification WPA3 pour un chiffrement renforcé.
- Portails captifs avec authentification unique (SSO) et intégration aux services du complexe.
- Détection et prévention des intrusions (WIDS/WIPS) pour eviter les attaques (man-in-the-middle, rogue AP).
- Priorisation des flux vidéo et VoIP via des mécanismes de qualité de service (QoS).

- Allocation dynamique de bande passante pour éviter la saturation du réseau.
- Gestion des accès invités avec limitation du débit et isolation des sessions.
- Une plateforme centralisée de gestion du Wi-Fi sera mise en place pour :
    - Surveiller en temps réel les performances et l'usage du réseau.
    - Optimiser la couverture en ajustant dynamiquement la puissance des points d'accès.
    - Produire des rapports d'analyse sur la fréquentation et les usages du Wi-Fi.

Des outils comme Cisco DNA Center, Aruba AirWave ou Mist AI pourront être utilisés pour optimiser et automatiser la gestion du réseau.

Un réseau WIFI est présent sur le centre de Congés Les Atlantes.

Un prochain réseau sera déployé sur Les Sables d'Olonne Arena.

2. Les prestations attendues : fourniture de services

Le candidat devra soumettre une offre détaillée intégrant :

- La description des services et de équipements requis selon le cahier des charges. Si les quantités diffèrent avec la demande, le candidat devra en expliquer les motifs ;
- Le coût des services ;
- Les modalités techniques de mise en œuvre, de suivi et de gestion du système d'infogérance et de sécurité informatique.

Matériels et prestations	**Localisation**	**Quantité prévisionnelle**	**Prix unitaire (en € HT)**	**TOTAL (en € HT)**
Firewall IDS/IPS (domaine SPL)	Ensemble domaine SPL	1	- €	- €
EDR 100 utilisateurs	Ensemble domaine SPL	1	- €	- €
Schéma d'adressage des équipements IT de l'Arena et mise en œuvre technique + interconnexion avec les sites exploités par la SPL (contrat prévisionnel entre le 1er juin 2025 et le 31/12/2026)	Ensemble domaine SPL	1	- €	- €
Infogérance et monitoring des serveurs, des NAS Backup et des sauvegardes, des switch, gestion des routeurs, **GTI (pour panne bloquante) requise 1 HEURE** jours ouvrés (variantes possibles), contrat prévisionnel entre le 1er juin 2025 et le 31/12/2026	Ensemble domaine SPL	1	- €	- €
Infogérance (dont portails, multi SSID, conformité légale) et monitoring des réseaux WIFI, contrat prévisionnel entre le 1er juin 2025 et le 31/12/2026	Ensemble domaine SPL	1	- €	- €
TOTAL HT				**- €**
TOTAL TTC (taux de TVA en vigueur : ..... %)				**- €**

3. Règlement de consultation

Nature et étendue des prestations

Nature et étendue des prestations : les prestations sont décrites au Cahier des charges.

Lieu d'exécution : les Sables d'Olonne Arena

Durée et reconduction

La durée du marché est comprise entre le 1er juin 2025 et le 31 décembre 2026. Le marché ne sera pas reconduit

Procédure de passation mise en œuvre

La présente consultation est passée selon une procédure adaptée librement définie par le pouvoir adjudicateur, dans le respect des dispositions de l'article L.2123-1 du code de la commande publique, et selon les modalités particulières suivantes :

Le pouvoir adjudicateur éliminera les candidats dont la candidature sera jugée irrecevable ou dont les capacités seront jugées insuffisantes. Il procédera ensuite à l'analyse des offres remises par les candidats retenus. Il se réserve toutefois la possibilité de procéder à l'analyse des candidatures après analyse et classement des offres.

Le pouvoir adjudicateur éliminera les offres inappropriées et décidera d'engager ou non les négociations, le pouvoir adjudicateur pouvant en toute hypothèse décider d'attribuer le marché sur la base des offres initiales sans négociation.

Dans l'affirmative, le pouvoir adjudicateur négociera avec tous les candidats. Dans le cas où le pouvoir adjudicateur aura admis à la négociation les offres irrégulières ou inacceptables, il devra, à l'issue des négociations, rejeter, sans les classer, les offres qui demeureraient irrégulières ou inacceptables.

Le pouvoir adjudicateur pourra cependant autoriser les soumissionnaires concernés à régulariser les offres irrégulières, à condition qu'elles ne soient pas anormalement basses.

Dans le cas où le pouvoir adjudicateur aura admis à la négociation les offres irrégulières ou inacceptables, il devra, à l'issue des négociations, rejeter, sans les classer, les offres qui demeureraient irrégulières ou inacceptables.

Le pouvoir adjudicateur pourra cependant autoriser les soumissionnaires concernés à régulariser les offres irrégulières, à condition qu'elles ne soient pas anormalement basses.

La négociation aura un caractère écrit et pourra porter sur un, plusieurs ou l'ensembles des éléments de l'offre.

À l'issue de ces négociations, il retiendra l'offre économiquement la plus avantageuse sur la base des critères de choix des offres définis dans l'avis et/ou dans le présent règlement de la consultation.

Contenu du dossier de consultation

Le présent cahier des charges.

Variante

Aucune variante.

Délai de validité des offres

Le délai de validité des offres est fixé à 120 jours à compter de la date limite de remise des offres.

Modifications de détail au dossier de consultation

Le pouvoir adjudicateur se réserve le droit d'apporter au plus tard 5 jours avant la date limite fixée pour la réception des offres, des modifications de détail au dossier de consultation. Les candidats devront alors répondre sur la base du dossier modifié sans pouvoir élever aucune réclamation à ce sujet.

Si pendant l'étude du dossier par les candidats la date limite ci-dessus est reportée, la disposition précédente est applicable en fonction de cette nouvelle date.

Retrait du dossier

Le pouvoir adjudicateur informe les candidats que le dossier de consultation des entreprises est dématérialisé. Il ne pourra en aucun cas être remis sur support papier ou sur support physique électronique.

Les candidats téléchargeront les documents dématérialisés du dossier de consultation des entreprises, documents et renseignements complémentaires ainsi que l'avis d'appel public à la concurrence via le profil d'acheteur http://www.marches-securises.fr.

Afin de pouvoir décompresser et lire les documents mis à disposition par le pouvoir adjudicateur, les soumissionnaires devront disposer des logiciels permettant de lire les formats suivants :

- Fichiers compressés au standard .zip (lisibles par les logiciels Winzip, Quickzip ou winrar par exemple)
- Adobe® Acrobat® .pdf (lisibles par le logiciel Acrobat Reader)
- Rich Text Format .rtf (lisibles par l'ensemble des traitements de texte : word de Microsoft, Wordpercfect, Openoffice, ou encore la visionneuse de Microsoft....)
- .docx ou .xlsx ou .pptx (lisibles par l'ensemble Microsoft Office, Open office, ou encore la visionneuse de Microsoft....)
- Le cas échéant le format DWF (lisibles par les logiciels Autocad, ou des visionneuses telles que Autodesk DWF viewer, Free DWG Viewer d'Informative Graphics, ...)

Tous les logiciels requis peuvent être téléchargés gratuitement sur le profil d'acheteur.

Lors du téléchargement du dossier de consultation, le candidat est invité à renseigner le nom de l'organisme soumissionnaire, le nom de la personne physique téléchargeant les documents et une adresse électronique permettant de façon certaine une correspondance électronique, afin qu'il puisse bénéficier de toutes les informations complémentaires diffusées lors du déroulement de la présente consultation, en particulier les éventuelles précisions ou report de délais.

Le candidat ne pourra porter aucune réclamation s'il ne bénéficie pas de toutes les informations complémentaires diffusées par la plateforme de dématérialisation lors du déroulement de la présente consultation en raison d'une erreur qu'il aurait faite dans la saisie de son adresse électronique, en cas de non identification de la personne lors du téléchargement, en cas de non indication de la dite adresse électronique, en cas de suppression de l'adresse ou en cas de téléchargement du cahier des charges ailleurs que sur le profil d'acheteur. Il est recommandé à tout candidat de consulter régulièrement la plateforme afin de s'assurer qu'il bénéficie bien des dernières modifications éventuelles.

En cas de difficulté quant au téléchargement du DCE, le candidat est invité à se rapprocher de la hotline technique au 04 92 90 93 27 mailto: technique@atline.fr.

Contenu des candidatures et des offres

Chaque candidat ou chaque membre de l'équipe candidate devra produire dans un dossier « Candidature » les pièces suivantes :

1/ Une lettre de candidature (DC1 ou équivalent) comportant l'ensemble des indications permettant d'identifier le candidat ou l'ensemble des membres du groupement en cas de réponse en groupement.

2 / Une déclaration sur l'honneur attestant qu'il ne fait pas l'objet d'une des interdictions de soumissionner telles que définies aux articles L.2141-1 à L.2141-5 et L.2141-7 à L.2141-11 du code de la commande publique et qu'il est en règle au regard des articles L.5212-1 à L.5212-11 du code du travail concernant l'emploi des travailleurs handicapés. La remise d'un DC1 ou d'un DUME vaudra remise d'une déclaration sur l'honneur.

Comme la lettre de candidature, la déclaration sur l'honneur n'a pas à être signée par le candidat ou par chacun des membres d'un groupement le cas échéant. Elle sera signée au stade de l'attribution par le seul attributaire (candidat seul ou ensemble des cotraitants en cas de groupement).

L'attention des candidats est attirée sur le fait qu'ils doivent informer sans délai l'acheteur de tout changement de situation, au cours de la procédure de passation ainsi d'ailleurs qu'au cours de l'exécution du marché, qui les placeraient dans un des cas d'interdiction de soumissionner ayant pour effet de les exclure d'un marché public.

3 / Eléments nécessaires au choix de l'offre

- La description des services requis. Si les quantités diffèrent avec la demande, le candidat devra en expliquer les motifs ;
- Le coût d'investissement selon le tableau fourni au point 3 ;
- Un planning d'installation et de mise en œuvre.

Jugement des offres

Critères	Pondération
Prix (noté sur 10)	Pondération 60%
Modalités techniques de mise en œuvre, de suivi et de gestion du système d'infogérance et de sécurité informatique (noté sur 10)	Pondération 40%

Conditions d’envoi et de remise des offres

Les conditions d’envoi et de remise des candidatures et des offres qui suivent s’imposent aux candidats.

Toute remise sous une autre forme que celle imposée au présent règlement de la consultation entraînera l’irrégularité de l’offre. Dans cette hypothèse, le pouvoir adjudicateur pourra néanmoins s’il le souhaite demander aux candidats concernés de régulariser leur offre.

Les candidatures et offres seront remises par la voie électronique via le profil d’acheteur www.marches-securises.fr.

Si le candidat adresse plusieurs offres différentes, seule la dernière offre reçue, dans les conditions du présent règlement, sera examinée.

Renseignements complémentaires

Pour obtenir tous renseignements complémentaires qui leurs seraient nécessaires au cours de leur étude, les candidats devront faire parvenir en temps utile une demande via le profil d’acheteur.

Les demandes doivent parvenir au plus tard 4 jours avant la date limite de réception des offres.

Une réponse sera alors adressée au plus tard 3 jours avant la date limite de réception des offres