**CAHIER DES CHARGES**

**DU MARCHE PUBLIC DE**

**FOURNITURES**

**CENTRALE D’ACHAT AYANT POUR OBJET**

**“FOURNITURE ET MAINTENANCE DE MATÉRIELS ET LOGICIELS RELATIFS À LA CYBERSÉCURITÉ”**

**PROCÉDURE OUVERTE**

**Pouvoir adjudicateur**

**IMIO**

**Auteur de projet**

**IMIO, Frédéric Rasic**

**Rue Léon Morel, 1 à 5032 Isnes**

**Table des matières**

[I. Dispositions administratives 5](#_Toc137024124)

[I.1 Description du marché 5](#_Toc137024125)

[I.2 Contexte de ce marché 6](#_Toc137024126)

[I.3 Identité de l’adjudicateur initial 7](#_Toc137024127)

[I.4 Procédure de passation 7](#_Toc137024128)

[I.5 Fixation des prix 7](#_Toc137024129)

[I.6 Motifs d’exclusion et sélection qualitative 8](#_Toc137024130)

[I.7 Questions et informations préalables au dépôt des offres 13](#_Toc137024131)

[I.8 Forme et contenu des offres 14](#_Toc137024132)

[I.9 Dépôt des offres 14](#_Toc137024133)

[I.10 Ouverture des offres 15](#_Toc137024134)

[I.11 Délai de validité 15](#_Toc137024135)

[I.12 Critères d’attribution 16](#_Toc137024136)

[I.13 Options et Variantes 16](#_Toc137024137)

[I.13.1 Variantes 17](#_Toc137024138)

[I.13.2 Options 17](#_Toc137024139)

[I.14 Choix de l’offre 17](#_Toc137024140)

[I.15 Limites de la centrale d’achats 17](#_Toc137024141)

[II. Dispositions contractuelles 18](#_Toc137024142)

[II.1 Fonctionnaire dirigeant 18](#_Toc137024143)

[II.2 Sous-traitants 19](#_Toc137024144)

[II.3 Assurances 20](#_Toc137024145)

[II.4 Cautionnement 20](#_Toc137024146)

[II.5 CV Vitrines 20](#_Toc137024147)

[II.6 Clause de réexamen : Révisions de experts proposés 20](#_Toc137024148)

[II.7 Clause de réexamen : Révisions de prix 20](#_Toc137024149)

[II.8 Durée et délai d’exécution 21](#_Toc137024150)

[II.9 Sanctions 21](#_Toc137024151)

[II.10 Procédure de commande 21](#_Toc137024152)

[II.11 Procédure de facturation et Délai de paiement 21](#_Toc137024153)

[II.12 Délai de garantie 22](#_Toc137024154)

[II.13 Réception 22](#_Toc137024155)

[II.14 Ressortissants d’un pays tiers en séjour illégal 22](#_Toc137024156)

[II.15 Rémunération due à ses travailleurs 23](#_Toc137024157)

[II.16 Protection des données 23](#_Toc137024158)

[II.17 Devoir de réserve et confidentialité 24](#_Toc137024159)

[II.18 Pénalités 24](#_Toc137024160)

[II.19 Compétence juridictionnelle et législation applicable 24](#_Toc137024161)

[II.20 Règlement Général de Protection des Données 24](#_Toc137024162)

[II.20.1 Protection des données 24](#_Toc137024163)

[II.20.2 Obligations de l’adjudicataire en tant que sous-traitant du Pouvoir adjudicateur dans le cadre des traitements de données 25](#_Toc137024164)

[II.20.3 Sécurité 26](#_Toc137024165)

[II.21 Centrale d’achats 26](#_Toc137024166)

[II.21.1 Limites de la centrale d’achat 27](#_Toc137024167)

[II.21.2 Conditions d’accès 27](#_Toc137024168)

[II.21.3 Procédure de commande 28](#_Toc137024169)

[II.21.4 Procédure de réception des livraisons, implémentations et prestations 28](#_Toc137024170)

[II.21.5 Moyen de contrôles 28](#_Toc137024171)

[II.21.6 Fonctionnaire dirigeant 28](#_Toc137024172)

[II.21.7 Accord de non-divulgation 29](#_Toc137024173)

[III. Description des exigences techniques 30](#_Toc137024174)

[III.1 Introduction 30](#_Toc137024175)

[III.1.1 Rôles et responsabilités 30](#_Toc137024176)

[III.1.2 Contexte 30](#_Toc137024177)

[III.1.3 Domaines d’expertises 31](#_Toc137024178)

[III.1.4 Glossaire 32](#_Toc137024179)

[III.2 Axe Matériel 33](#_Toc137024180)

[III.2.1 Lot M1 : Produit MFA 34](#_Toc137024181)

[III.2.2 Lot M2 : Pare-feu 38](#_Toc137024182)

[III.2.3 Lot M3 : Sauvegardes sécurisées de données 44](#_Toc137024183)

[III.3 Axe Logiciel 48](#_Toc137024184)

[III.3.1 Lot L1 : Journalisation des événements 49](#_Toc137024185)

[III.3.2 Lot L2 : Gestion de l’authentification et identification numérique 53](#_Toc137024186)

[III.3.3 Lot L3 : Filtrage des messages électroniques 57](#_Toc137024187)

[III.3.4 Lot L4 : Antivirus/antimalware/EDR/XDR 61](#_Toc137024188)

[III.3.5 Lot L5 : Gestion des mots de passe 64](#_Toc137024189)

[III.4 Dispositions de fin de marché et de réversibilité 69](#_Toc137024190)

[III.4.1 Clause de réversibilité 69](#_Toc137024191)

[III.4.2 Clause de transférabilité 70](#_Toc137024192)

**Auteur de projet**

Nom : IMIO

Adresse : Rue Léon Morel, 1 à 5032 Isnes

Personne de contact : M. Frédéric Rasic

Téléphone : 081/586.100

Fax : 081/586.129

E-mail : marche.public@imio.be

**Réglementation en vigueur**

1. Loi du 17 juin 2016 relative aux marchés publics et ses modifications ultérieures.

2. Arrêté royal du 18 avril 2017 relatif à la passation des marchés publics dans les secteurs classiques, et ses modifications ultérieures.

3. Arrêté royal du 14 janvier 2013 établissant les règles générales d'exécution des marchés publics, et ses modifications ultérieures.

4. Loi du 17 juin 2013 relative à la motivation, à l’information et aux voies de recours en matière de marchés publics, de certains marchés de travaux, de fournitures et de services et de concessions, et ses modifications ultérieures.

5. Règlement général pour la protection du travail (RGPT), Loi sur le bien-être et Code du bien-être au travail.

6. Loi du 11 février 2013 prévoyant des sanctions et des mesures à l’encontre des employeurs de ressortissants de pays tiers en séjour illégal.

7. Le règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE.

**Dérogations, précisions et commentaires**

L’article 7 de l’arrêté royal du 14 janvier 2013 établissant les règles générales d’exécution des marchés publics dispose que *« Le présent chapitre et les articles 12, § 4, 37 à 38/19 et 61 à 63 sont applicables à l'accord-cadre. En ce qui concerne les marchés conclus sur la base de l’accord-cadre, l’ensemble des dispositions, sans préjudice des articles 5 et 6, sont d’application, sauf disposition contraire dans les documents du marché. Pour les marchés visés, il ne peut cependant être dérogé aux dispositions des articles 9, §§ 2 et 3, 12/1, 37 à 38/6, 38/8, 38/9, § 4, 38/10, § 4, 38/11 à 38/19, 62, alinéa 1er, 1°, et alinéa 2, 62/1 et 69* ».

En d’autres termes, l’arrêté royal du 14 janvier 2013 précité s’applique à l’accord-cadre et aux marchés fondés sur l’accord-cadre, sauf disposition contraire dans le cadre du présent cahier et sauf les dispositions expressément précitées.

En l’espèce, il est précisé que l’article 25 de l’arrêté royal du 14 janvier 2013 ne trouvera pas à s’appliquer : Il est dérogé à l'article 25 § 1er, 2°, h) de l'arrêté royal du 14 janvier 2013 établissant les règles générales d'exécution des marchés publics afin d'éviter les lourdeurs administratives rendues inutiles par le montant de certaines commandes, le cautionnement de 5% n'est exigé que pour les commandes, subséquentes à ce marché (passées par les PAB), supérieures au montant de 50.000 €.

**Modifications apportées à ce document dans le cadre de l’erratum**

Page 131-133 – Annexe D – correction marque d’intérêt (Onhaye 🡺 Olne) + Ajout Hamois

# Dispositions administratives

Cette première partie se rapporte à la réglementation relative à la passation d'un marché public jusqu'à la désignation de l'adjudicataire.

Les dispositions contenues dans cette partie se rapportent à la loi du 17 juin 2016 et à l’arrêté royal du 18 avril 2017 et leurs modifications ultérieures.

## Description du marché

iMio a pour objectif de promouvoir et de coordonner la mutualisation de solutions métiers, de produits et services pour les Pouvoirs locaux.

iMio est articulée autour de trois activités principales :

* Produire des logiciels Open source répondant aux besoins des Pouvoirs locaux. Le modèle Open source permet à iMio d'avoir la maîtrise des outils et d'avoir le choix du prestataire pour la réalisation de développements. Une partie des développements peut aussi être assurée en interne, ce qui garantit une plus grande autonomie d'action ;
* Acheter des solutions en centrale d'achat/marché pour permettre aux communes de bénéficier de solutions du marché à moindre coût et offrir un service d'accompagnement à leur utilisation et leur évolution ;
* Accompagner les membres et formaliser les projets informatiques des Pouvoirs locaux (organisationnel).

La philosophie proposée reste celle de la mutualisation dans la logique « bottom-up » et efforts partagés pour réduire les coûts pour les membres, tout en produisant des solutions en permanence mieux adaptées aux réalités des Pouvoirs locaux, puisque ce sont eux qui les produisent ou les font produire. Il est fondamental que les soumissionnaires adhèrent à ce mode de fonctionnement afin de garantir une adoption massive du projet grâce à l’adéquation fonctionnelle existant entre la réalité des services et leurs outils informatiques.

Les candidats soumissionnaires doivent prendre ceci pour acquis et soumissionner dans cet état d’esprit et vision future.

**Objet du présent marché :** Établir une centrale d’achats en matière de cybersécurité

Ce marché a pour objet d’établir une centrale d’achat en vue de fournir aux communes et CPAS de Wallonie une offre complète de logiciels et de matériels de cybersécurité pour renforcer leur résilience face aux menaces en ligne.

Ce marché se compose de lots distincts couvrant un éventail de domaines de la cybersécurité, comprenant :

* M1 - Produit MFA (authentification multi facteurs)
* M2 - Pare-feu
* M3 - Sauvegarde des données sécurisées
* L1 - Journalisation des événements
* L2 - Projets liés au management de l’authentification et à l’identification numérique
* L3 - Filtrage des messages électroniques
* L4 - Antivirus/antimalware/EDR/XDR
* L5 - Gestion des mots de passe

Le paysage des menaces en matière de cybersécurité étant en constante évolution, les Pouvoirs locaux se doivent d'être en mesure de faire face à ces défis pour garantir leur résilience et protéger leurs intérêts et ceux de leurs citoyens. Ce marché est le résultat de la grande campagne d'audit menée ces derniers mois avec pour objectif de mettre en place un socle commun de défense pour la Wallonie. L'objectif de ce marché est de fournir aux communes et CPAS de Wallonie une solution de cybersécurité complète et personnalisée qui répondra à leurs besoins spécifiques en matière de protection contre les cybermenaces.

**Lieu de livraison** : Pouvoirs locaux wallons ayant adhéré à la centrale d’achat. La liste est reprise en annexe D au présent cahier spécial des charges.

**Codes CPV :**

* 48710000-8 Logiciels de copie de sécurité ou de récupération.
* 48730000-4 Logiciels de sécurité
* 48731000-1 Logiciels de sécurité des fichiers
* 48732000-8 Logiciels de sécurité des données
* 72212710-9 Services de développement de logiciels de copie de sécurité ou de récupération.
* 72212730-5 Services de développement de logiciels de sécurité.
* 72212731-2 Services de développement de logiciels de sécurité des fichiers.
* 72212732-9 Services de développement de logiciels de sécurité des données.

## Contexte de ce marché

Ce marché fait suite à l’établissement d’un état des lieux des Pouvoirs locaux concernant leur infrastructure, les mesures prises pour lutter contre la cybercriminalité et leur gouvernance réalisé entre septembre 2022 et mars 2023. L’objectif de ce marché est de répondre aux constats de l’exercice précédent par une offre pertinente d’équipements et logiciels aux Pouvoirs locaux afin de leur permettre de préserver la continuité de service de leurs missions et la protection des données de leurs citoyens. Ce présent marché vise à répondre aux constats issus de l'état des lieux que nous avons réalisé concernant l'infrastructure, les mesures de lutte contre la cybercriminalité et la gouvernance des Pouvoirs locaux en matière de sécurité de l’information.

Le gouvernement wallon a confié à iMio le rôle de pouvoir adjudicateur pour plusieurs projets visant à soutenir les Pouvoirs locaux dans leur lutte contre la cybercriminalité et la protection de leur cybersécurité. Ce projet de mutualisation et de valorisation des ressources liées à la cybersécurité vise à créer une base commune de cyberdéfense en Wallonie, afin de renforcer la protection de tous les Pouvoirs locaux face aux menaces en ligne en matière de cybercriminalité.

La mise en place d'une structure centralisée disposant de moyens d'action est devenue indispensable pour assurer la sécurité de l'ensemble des Pouvoirs locaux face à la croissance constante des risques en ligne. Ce projet de mutualisation et de valorisation des actifs liés à la cybersécurité a pour vocation de mener à l’émergence d’un « socle commun » de cyberdéfense en Wallonie. Avoir une structure centralisatrice disposant de moyens d’action est désormais indispensable tant la menace pèse sur l’ensemble des pouvoirs locaux.

Cette stratégie a été construite en collaboration totale avec les administrations compétentes sur les sujets de cybersécurité et s’énonce comme ceci :

1. Mettre en place des solutions de cybersécurité à destination des communes de Wallonie, quelle que soit leur taille ;
2. Développer la connaissance des agents des Pouvoirs locaux wallons à la réalité des menaces en matière de cybercriminalité et les sensibiliser aux bonnes pratiques en la matière pour qu’ils puissent s’en protéger ;
3. Soutenir l’action du Gouvernement wallon dans la transition numérique des Pouvoirs locaux ;
4. Créer un cadre numériquement sain pour aider les collectivités à travailler dans un environnement où disponibilité, intégrité et confidentialité seront les maîtres-mots ;
5. Créer une centrale d’achats dédiée à la cybersécurité pour optimiser les investissements publics par le regroupement des communes de Wallonie et d’autres administrations.

La démarche de cyber-résilience vise à protéger les Pouvoirs locaux contre les cyberattaques en mettant en place une approche globale comprenant deux étapes. La première étape a consisté à évaluer la maturité de chaque Pouvoir local face aux cyberattaques en utilisant les résultats des audits de sécurité réalisés précédemment.

L’étape suivante couvre les besoins en équipements, logiciels et matériels, ainsi que les accompagnements et formations nécessaires pour renforcer la protection des Pouvoirs locaux. Ces besoins sont évalués en fonction des catégories de Pouvoirs locaux. Notre marché vise à fournir une solution globale pour cette seconde étape dans une démarche de cyber-résilience.

Ces outils regrouperont les cinq piliers de la cybersécurité :

* Anticiper
* Prévenir
* Protéger
* Détecter et répondre
* Restaurer

La démarche de cyber résilience a pour but de garantir la confidentialité, l’intégrité et la disponibilité de l’information au sein des Pouvoirs locaux wallons.

La démarche s’inscrira également dans une logique cyclique d’amélioration continue en adéquation avec les bonnes pratiques en la matière, de type : planifier (Plan), développer ou réaliser (Do), contrôler (Check) et agir ou ajuster (Act), Cfr Roue de Deming.

## Identité de l’adjudicateur initial

IMIO

Rue Léon Morel, 1

5032 Isnes

Le pouvoir adjudicateur agit comme **centrale d’achat** au sens de l’article 2, 6°, a) de la Loi du 17 juin 2016 relative aux marchés publics, via la technique de l’accord-cadre.

IMIO agit comme pouvoir adjudicateur qui établit la centrale d’achat des services visés par le présent accord-cadre, au bénéfice des pouvoirs adjudicataires bénéficiaires (PAB).

Les pouvoirs adjudicateurs bénéficiaires de la présente centrale sont listés en annexe D du présent cahier spécial des charges.

Le déroulement des procédures subséquentes à ce marché initial est explicité dans la section « Accord cadre » de la deuxième section « II. Dispositions contractuelles » du présent cahier spécial des charges.

## Procédure de passation

Le marché est passé par procédure ouverte.

## Fixation des prix

Le présent marché consiste en un marché à bordereau de prix.

Le marché à bordereau de prix est celui dans lequel les prix unitaires des différents postes sont forfaitaires et les quantités, pour autant que des quantités soient déterminées pour les postes, sont présumées ou exprimées dans une fourchette. Les postes sont portés en compte sur la base des quantités effectivement commandées et mises en œuvre.

Le marché est attribué sur base des prix unitaires mentionnés dans l'offre. Au moment de la rédaction des conditions du présent marché, le pouvoir adjudicateur n'est pas en mesure de définir avec précision les quantités de services dont il aura besoin. En conséquence, les quantités présumées indiquées au cahier des charges régissant le présent marché sont à titre purement indicatif, elles n'engagent nullement l'administration. Dès lors, les adjudicataires ne pourront réclamer aucune indemnité dans le cas où les quantités présumées ne seraient pas atteintes.

## Motifs d’exclusion et sélection qualitative

L'opérateur économique produit le Document unique de marché européen, qui consiste en une déclaration sur l'honneur propre actualisée et qui est accepté par le pouvoir adjudicateur à titre de preuve a priori en lieu et place des documents ou certificats délivrés par des autorités publiques ou des tiers pour confirmer que l'opérateur économique concerné :

1° ne se trouve pas dans l'une des situations d'exclusion visées aux articles 67 à 69 de la loi du 17 juin 2016 ;

2° répond aux critères de sélection applicables qui ont été établis conformément à l'article 71 de la loi du 17 juin 2016 ;

Marche à suivre pour compléter le DUME :

- Rendez-vous sur le site https://dume.publicprocurement.be, et choisissez votre langue.

- A la question ‘Qui êtes-vous’, répondez ‘Je suis un opérateur économique’.

- A la question ‘Quelle action souhaitez-vous effectuer ?’, répondez ‘Générer réponse’.

- Complétez votre pays et cliquez sur suivant. ‘Exclusions’.

- Pour la partie ‘Sélection’, à la question ‘Souhaitez-vous utiliser les critères de sélection A à D ?’ répondez non. Dans ce cas, il vous est demandé une indication globale pour les critères de sélection.

- Précisez si vous satisfaites à tous les critères de sélection exigés.

- Après avoir complété l’entièreté du formulaire, cliquez sur ‘Aperçu’ en bas de page. Vous arrivez sur votre DUME complété que vous pouvez télécharger au format PDF et/ou xml pour être fourni électroniquement avec votre offre.

Les opérateurs économiques peuvent réutiliser un DUME qui a déjà été utilisé dans une procédure antérieure, à condition qu'ils confirment que les informations qui y figurent sont toujours valables.

**L’attention des soumissionnaires est attirée sur le fait qu'un DUME doit être déposé pour tout sous-traitant, quel que soit son statut (indépendant, freelance, ...) à la compétence duquel il est fait appel en vue de satisfaire aux conditions posées au titre de la sélection qualitative.**

Le pouvoir adjudicateur vérifiera, via l'application Télémarc ou via d'autres applications électroniques équivalentes et accessibles gratuitement dans d'autres États membres, la situation du soumissionnaire sur le plan des dettes sociales et sa situation fiscale dans les 20 jours suivant la date ultime pour l'introduction des offres.

L’extrait de casier judiciaire sera examiné dans le chef des adjudicataires pressentis, ainsi que dans le chef des membres de l'organe administratif, de gestion ou de surveillance desdits adjudicataires pressentis ou détiennent un pouvoir de représentation, de décision ou de contrôle en leur sein.

**Situation juridique du soumissionnaire (motifs d'exclusion)**

Le DUME, par lequel l'opérateur économique déclare qu’il ne se trouve pas dans une des situations d’exclusion visées aux articles 67 à 69 de la loi du 17 juin 2016.

**L’attention des soumissionnaires est attirée sur le fait qu'un DUME doit être déposé pour tout sous-traitant, quel que soit son statut (indépendant, freelance, ...) à la compétence duquel il est fait appel en vue de satisfaire aux conditions posées au titre de la sélection qualitative.**

**Les soumissionnaires fourniront d’initiative les éventuelles mesures correctrices tant aux clauses d’exclusion obligatoire qu’aux clauses d’exclusion facultative.**

**Capacité technique et professionnelle du soumissionnaire (critères de sélection)**

Le DUME de l'opérateur économique et/ou éventuellement d’un ou plusieurs sous-traitants auquel il est fait appel, par le/lesquels le soumissionnaire déclare qu'il satisfait aux critères de sélection suivants :

Pour le lot M1 : Produits MFA

|  |  |  |
| --- | --- | --- |
| N° | Critères de sélection | Exigences minimales |
| 1 | Références | Depuis le 1/1/2020, le soumissionnaire doit pouvoir démontrer au minimum :   * 5 installations dans des organisation de moins de 50 personnes * 10 installation dans des organisation de 50 à 500 personnes * 10 installation dans des organisation de 500 personnes et +   Pour qu’une référence soit valable, il faut que la taille de l’organisation soit respectée, et qu’au minimum 2 facteurs d’authentification (login/Mdp + 1 facteur externe au choix) aient été mis en place et être en ordre de maintenance/support par le soumissionnaire/fabricant. Au minimum la moitié de ces références doivent avoir été installées (nouvellement commandées) après cette échéance (1/1/2020), l’autre moitié des références peut être le maintien d’un client préexistant. |
| 2 | Équipe projet | L’équipe chargée des livraisons et implémentations/mises en œuvre doit être composée au minimum de 3 personnes. Ce personnel technique doit faire l’objet d’une certification technique par le fabricant, ou bénéficier d’un processus d’auto-certification interne pour connaître et maîtriser le matériel proposé si le fabricant ne propose pas de certification. |

Pour le lot M2 : Pare-feu

|  |  |  |
| --- | --- | --- |
| N° | Critères de sélection | Exigences minimales |
| 1 | Références | Depuis le 1/1/2020, le soumissionnaire doit pouvoir démontrer au minimum 30 installations valables, dont au minimum :   * 5 avec de l’IP Filtering * 5 avec mise en place de VLAN * 5 avec mise en place de connexions à distance * 5 avec vérification de la validité des paquets et l’adéquation au protocole attendu * 5 avec détection et combat des logiciels espions * 5 avec mise en oeuvre de pare-feu(s) virtuel(s) * 5 avec mise en place de NAT * 5 avec mise en place d’IDS/IPS et mesure de prévention   Une installation peut combiner plusieurs des critères minimums cités ci-dessus.  Pour qu’une installation soit valable, elle doit concerner une entité de plus de 50 postes et être en ordre de maintenance/support par le soumissionnaire/fabricant. Au minimum la moitié de ces références doivent avoir été installées (nouvellement commandées) après cette échéance (1/1/2020), l’autre moitié des références peut être le maintien d’un client préexistant. |
| 2 | Équipe projet | L’équipe chargée des livraisons et implémentations/mises en œuvre doit être composée au minimum de 3 personnes. Ce personnel technique doit faire l’objet de certifications :   * Technique par le fabricant, ou bénéficier d’un processus d’auto-certification interne pour connaître et maîtriser le matériel proposé si le fabricant ne propose pas de certification. |

Pour le lot M3 : Sauvegarde sécurisée de données

|  |  |  |
| --- | --- | --- |
| N° | Critères de sélection | Exigences minimales |
| 1 | Références | Depuis le 1/1/2020, le soumissionnaire doit pouvoir démontrer au minimum 10 installation présentant les caractéristiques suivantes:   * 5 TB de stockage. * 10 machines virtuelles (Windows, Linux, etc). * 3 tâches de sauvegarde automatique. * Connecté au système de virtualisation en place. * Redirection des sauvegardes vers au minimum 2 supports différents (NAS, tape, etc). * Compression et déduplication des systèmes sauvegardés. * Configuration de l’alerting vers des adresses mail. * Tests de restauration réalisés avec succès. * Encryption des sauvegardes.   Pour qu’une référence soit valable, il faut que la taille de l’organisation soit respectée, et qu’au minimum 2 politiques de sauvegardes aient été mises en œuvre (sauvegarde totale (ou full backup), incrémentale (ou incremental backup), différentielle (ou differential backup) et qu’un test régulier de récupération ait été mis en place lors de l’installation. Au minimum la moitié de ces références doivent avoir été installées (nouvellement commandées) après cette échéance (1/1/2020), l’autre moitié des références peut être le maintien d’un client préexistant. |
| 2 | Équipe projet | L’équipe chargée des livraisons et implémentations/mises en œuvre doit être composée au minimum de 3 personnes. Ce personnel technique doit faire l’objet d’une certification technique par le fabricant, ou bénéficier d’un processus d’auto-certification interne pour connaître et maîtriser le matériel proposé si le fabricant ne propose pas de certification. |

Pour le lot L1 : Journalisation des événements

|  |  |  |
| --- | --- | --- |
| N° | Critères de sélection | Exigences minimales |
| 1 | Références | Depuis le 1/1/2020, le soumissionnaire doit pouvoir démontrer au minimum 10 installations valables, dont au minimum :   * 5 par collecte avec agent * 5 par collecte sans agent * 5 avec mise en place de règles d’alertes selon des spécifications fonctionnelles * 5 avec une mise en place d’une politique d’analyse des événements * 5 avec une analyse forensique des journaux * 5 avec un archivage des journaux d’événements   Une installation peut combiner plusieurs des critères minimums cités ci-dessus.  Pour qu’une installation soit valable, elle doit concerner une entité de plus de 50 postes et être en ordre de maintenance/support par le soumissionnaire/éditeur. Au minimum la moitié de ces références doivent avoir été installées (nouvellement commandées) après cette échéance (1/1/2020), l’autre moitié des références peut être le maintien d’un client préexistant. |
| 2 | Équipe projet | L’équipe chargée des livraisons et implémentations/mises en œuvre doit être composée au minimum de 3 personnes. Ce personnel technique doit faire l’objet d’une certification technique par l’éditeur, ou bénéficier d’un processus d’auto-certification interne pour connaître et maîtriser le logiciel proposé si l’éditeur ne propose pas de certification. |

Pour le lot L2 : Gestion de l’authentification et identification numérique

|  |  |  |
| --- | --- | --- |
| N° | Critères de sélection | Exigences minimales |
| 1 | Références | Depuis le 1/1/2020, le soumissionnaire doit pouvoir démontrer au minimum 20 installations valables, dont au minimum :   * 10 installations liées à un annuaire d’entreprises ; * 5 installations liées à une base de données d’utilisateurs * 5 installations permettant le SSO (OAuth ou SAML ou OpenID)   Une installation peut combiner plusieurs des critères minimums cités ci-dessus.  Pour qu’une installation soit valable, elle doit concerner une entité de plus de 100 personnes et être en ordre de maintenance/support par le soumissionnaire/éditeur. Au minimum la moitié de ces références doivent avoir été installées (nouvellement commandées) après cette échéance (1/1/2020), l’autre moitié des références peut être le maintien d’un client préexistant. |
| 2 | Équipe projet | L’équipe chargée des livraisons et implémentations/mises en œuvre doit être composée au minimum de 3 personnes. Ce personnel technique doit faire l’objet d’une certification technique par l’éditeur, ou bénéficier d’un processus d’auto-certification interne pour connaître et maîtriser le logiciel proposé si l’éditeur ne propose pas de certification |

Pour le lot L3 : Filtrage des messages numériques

|  |  |  |
| --- | --- | --- |
| N° | Critères de sélection | Exigences minimales |
| 1 | Références | Depuis le 1/1/2020, le soumissionnaire doit pouvoir au minimum 50 installations valables, dont au minimum :   * 50 installations contenant le filtrage des messages contenant des liens et des pièces jointes nuisibles * 30 installations contenant le filtrage des spams * 20 installations incluant des expressions régulières, des services personnalisés et des analyses statistiques ; * 20 installations incluant différents types de vérifications de contenu basées sur des messages, des textes, des en-têtes, etc., tels que des hachages flous, le filtrage d'expressions régulières, DCC, etc. * 20 installations prévenant le phishing * 10 installations effectuées via une API connectant le système de filtrage au serveur de messagerie   Une installation peut combiner plusieurs des critères minimums cités ci-dessus.  Pour qu’une installation soit valable, elle doit concerner une entité de plus de 100 adresses mail et être en ordre de maintenance/support par le soumissionnaire/éditeur. Au minimum la moitié de ces références doivent avoir été installées (nouvellement commandées) après cette échéance (1/1/2020), l’autre moitié des références peut être le maintien d’un client préexistant. |
| 2 | Équipe projet | L’équipe chargée des livraisons et implémentations/mises en œuvre doit être composée au minimum de 3 personnes. Ce personnel technique doit faire l’objet d’une certification technique par l’éditeur, ou bénéficier d’un processus d’auto-certification interne pour connaître et maîtriser le logiciel proposé si l’éditeur ne propose pas de certification. |

Pour le lot L4 : Antivirus/antimalware/EDR/XDR

|  |  |  |
| --- | --- | --- |
| N° | Critères de sélection | Exigences minimales |
| 1 | Références | Depuis le 1/1/2020, le soumissionnaire doit pouvoir démontrer au minimum 50 installations valables, dont au minimum :   * 50 installations antivirus * 30 installations EDR * 20 installations XDR * 10 avec détection avancée des menaces * 10 avec détection comportementale * 10 avec collecte et analyse des données en temps réel * 10 avec réponse automatique aux incidents * 10 avec analyse des chaînes d’attaques * 10 avec protection contre les ransomware * 10 avec gestion et déploiement automatisé * 5 avec sandboxing   Une installation peut combiner plusieurs des critères minimums cités ci-dessus.  Pour qu’une installation soit valable, elle doit concerner une entité de plus de 100 postes de travail et être en ordre de maintenance/support par le soumissionnaire/éditeur. Au minimum la moitié de ces références doivent avoir été installées (nouvellement commandées) après cette échéance (1/1/2020), l’autre moitié des références peut être le maintien d’un client préexistant |
| 2 | Équipe projet | L’équipe chargée des livraisons et implémentations/mises en œuvre doit être composée au minimum de 3 personnes. Ce personnel technique doit faire l’objet d’une certification technique par l’éditeur, ou bénéficier d’un processus d’auto-certification interne pour connaître et maîtriser le logiciel proposé si l’éditeur ne propose pas de certification. |

Pour le lot L5 : Gestion des mots de passe

|  |  |  |
| --- | --- | --- |
| N° | Critères de sélection | Exigences minimales |
| 1 | Références | Depuis le 1/1/2020, le soumissionnaire doit pouvoir démontrer au minimum 50 installations valables, dont au minimum :   * 50 installations avec sauvegarde et remplissage automatique * 50 installations avec génération de mots de passe complexes * 50 installations avec détection des mots de passe faibles et vieux * 30 installations avec analyse de fuites de données * 30 installations avec synchronisation automatique entre les appareils * 20 installations avec intégration à une authentification multifacteur * 20 installations avec mécanismes de récupération de mots de passe en cas d'oubli ou de perte   Une installation peut combiner plusieurs des critères minimums cités ci-dessus.  Pour qu’une installation soit valable, elle doit concerner une entité de plus de 100 utilisateurs et être en ordre de maintenance/support par le soumissionnaire/éditeur. Au minimum la moitié de ces références doivent avoir été installées (nouvellement commandées) après cette échéance (1/1/2020), l’autre moitié des références peut être le maintien d’un client préexistant. |
| 2 | Équipe projet | L’équipe chargée des livraisons et implémentations/mises en œuvre doit être composée au minimum de 3 personnes. Ce personnel technique doit faire l’objet d’une certification technique par l’éditeur, ou bénéficier d’un processus d’auto-certification interne pour connaître et maîtriser le logiciel proposé si l’éditeur ne propose pas de certification. |

Pour simplifier le travail de complétion et d’analyse du bordereau de sélection qualitative, iMio a préparé le présent document, librement téléchargeable et utilisable par les candidats soumissionnaires : <https://docs.google.com/spreadsheets/d/1n53ohgKR2ArSozpAbtW3Acaxrfl9roa_NuXbtW8XJbc/edit?usp=sharing>

## Questions et informations préalables au dépôt des offres

**Questions**

Jusqu’au 5/7/2023 à 10h00, les candidats-soumissionnaires peuvent adresser leurs questions relatives à cette procédure de marché à iMio :

* Adresse : IMIO, Rue Léon Morel 1, 5032 Isnes
* E-mail : [marche.public@iMio.be](mailto:marche.public@imio.be)

Au-delà de cette échéance, les questions ne seront plus recevables.

Les questions doivent être identifiées par :

* Un numéro de question
* Le nom du candidat-soumissionnaire
* La section du cahier spécial des charges faisant l’objet du questionnement
* Le numéro de page faisant l’objet du questionnement

Aucune question ne pouvant être contextualisée au cahier spécial des charges ne sera traitée.

Afin de simplifier le travail de questionnement et réponse, nous vous invitons à utiliser le document (libre de téléchargement) suivant pour poser vos questions sur le marché public : <https://docs.google.com/document/d/1DRnxBa0rnGjxXRhKzF_ysgDyJZEj3PHhoOuFUtPhh68/edit?usp=sharing>

**Séance d’information**

Sur base des questions posées et des réponses préparées par le pouvoir adjudicateur, une séance d’information sera organisée le 12/7/2023 à 15h30 par le biais d’une visioconférence. Cette information aura pour but de récapituler les éléments principaux du présent marché public ainsi que parcourir les questions-réponses posées par les soumissionnaires.

Pour participer à la séance d’information, le soumissionnaire doit s’inscrire préalablement par mail :

* Adresse mail : [marche.public@imio.be](mailto:marche.public@imio.be)
* Contenu du mail :
  + Sujet : Marché Cybersécurité iMio – « Nom du soumissionnaire »
  + Contenu du mail : coordonnées des participants (nom, prénom, numéro de portable et adresse mail)

Seuls les soumissionnaires peuvent participer à la séance d’information, le pouvoir adjudicateur rappelle que cette séance d’information se fait sur base volontaire, il ne s’agit pas d’une obligation légale, qu’il est donc attendu des participants une attitude correcte et une participation active dans le cadre autorisé par la procédure ouverte. Ne s’agissant pas d’une procédure négociée, aucun terme du cahier spécial des charges ne peut être adapté/modifié.

Les soumissionnaires peuvent poser des questions complémentaires durant la séance d’information, le pouvoir adjudicateur se réserve le droit de ne pas répondre directement en séance et de fournir la réponse par le biais de la publication via Public Procurement (Cfr ci-dessous).

Les questions relevantes, leurs réponses et les documents de la séance d’information seront mis à disposition par l’intermédiaire de Public Procurement au plus tard le 19/7/2023.

## Forme et contenu des offres

Le soumissionnaire établit son offre en français et complète l'inventaire sur le modèle annexé au cahier des charges le cas échéant. Les soumissionnaires ne sont pas autorisés à établir leur offre sur d'autres documents que le formulaire prévu quand bien même il supporte l'entière responsabilité de la parfaite concordance entre les documents qu'il a utilisés et le formulaire.

Les offres étant transmises par des moyens électroniques, le rapport de dépôt de l'offre doit être revêtu d'une signature électronique qualifiée.

Lorsque le rapport de dépôt est signé par un mandataire, celui-ci mentionne clairement son (ses) mandant(s). Le mandataire joint l'acte authentique ou sous seing privé qui lui accorde ses pouvoirs ou une copie scannée de la procuration.

**L’attention du soumissionnaire est attirée sur le fait que la signature du rapport de dépôt par une personne (physique ou morale) non compétente pour engager celui-ci entrainera l'irrégularité de l’offre.**

Les prix doivent toujours être exprimés en euro.

**Pour qu’une offre soit valable, elle doit contenir les éléments suivants présentés :**

Le DUME ainsi que pour les lots soumissionnés :

* Annexe A : formulaire d’offre
* Annexe B : Inventaire
* Annexe C : Bordereau(x) de réponse technique
* Annexe G : Engagements sur l’Obligation de résultats
* Un document récapitulatif de l’offre de service proposée ainsi qu’une présentation de la société ;
* Les curriculums vitae des personnes les identifiant de manière unique
* Les fiches produits/logiciels des fabricants/éditeurs proposés
* Toute(s) autre(s) annexe(s) nécessaire(s) à la bonne complétion du dossier

**Modification des quantités présumées**

Le pouvoir adjudicateur demande aux soumissionnaires de compléter le double bordereau de prix par lot. D’une part, le premier bordereau est la liste des équipements (matériels et logiciels) et des prestations qu’il prévoit de fournir dans le cadre de cette procédure ouverte, les quantités doivent être à 1. Dans le second tableau, il duplique les lignes du premier, en conservant les prix unitaires, et adapte les quantités au regard du scénario à compléter pour l’inventaire du lot soumissionné, voir la description technique de chaque lot.

**Sous-traitance**

Le soumissionnaire indique dans son offre la part du marché qu'il a l'intention de sous-traiter ainsi que les sous-traitants proposés, si connus.

**Soumission à plusieurs lots**

Si le soumissionnaire répond à plusieurs lots, il ne peut pas proposer de rabais, ni d’améliorations.

## Dépôt des offres

Seules les offres qui sont envoyées au plus tard avant l’ouverture des offres via le site internet e-Tendering https://eten.publicprocurement.be/ seront acceptées par le pouvoir adjudicateur. Le site internet e-Tendering garantit le respect des conditions établies par l'article 14 §7 de la loi du 17 juin 2016.

Il y a lieu de remarquer que l'envoi d'une offre par e-mail ne répond pas à ces conditions. Dès lors, il n'est pas autorisé d'introduire une offre par ce moyen.

Par le seul fait de présenter une offre totalement ou partiellement par des moyens électroniques, le soumissionnaire accepte que les données découlant du fonctionnement du dispositif de réception de son offre soient enregistrées.

Plus d'informations peuvent être obtenues sur le site : http://www.publicprocurement.be ou via le numéro de téléphone du helpdesk du service e-procurement : +32 (0)2 740 80 00.

**L'offre ne peut pas être introduite sur papier.**

Par l’introduction d’une offre, les soumissionnaires acceptent sans condition le contenu du cahier des charges et des autres documents relatifs au marché, ainsi que le respect de la procédure de passation telle que décrite dans le cahier des charges et acceptent d’être liés par ces dispositions.

Lorsqu’un soumissionnaire formule une objection à ce sujet ou lorsqu'il découvre des erreurs ou des omissions dans les documents du marché, telles qu’elles rendent impossible l’établissement de son prix ou la comparaison des offres, il les signale immédiatement par écrit et par courrier recommandé, et ce, au plus tard 10 jours avant la date et l'heure limites d'introduction des offres.

Le soumissionnaire est tenu de signaler tout problème de légalité immédiatement apparent à l’égard de la procédure ou du présent cahier spécial des charges, afin qu’il puisse, si nécessaire, encore y être rectifié en ayant le moins de répercussions possibles sur le déroulement de la procédure d’attribution. À défaut de l’avoir fait au plus tard dans les 10 jours de la date ultime de dépôt des offres, le soumissionnaire n’est plus fondé à s’en prévaloir ultérieurement.

## Ouverture des offres

Le : 21/8/2023 à 10h00.

Les offres sont introduites électroniquement, il n'y a pas d'ouverture des offres en séance publique.

## Délai de validité

Le soumissionnaire reste lié par son offre pendant un délai de 120 jours de calendrier, à compter de la date limite de réception des offres.

## Critères d’attribution

Les critères suivants sont d'application lors de l'attribution du marché pour l’ensemble des lots :

| **N°** | **Description** | **Pondération** |
| --- | --- | --- |
| 1 | Prix | 50 |
|  | *Score offre = (prix de l’offre la plus basse / prix de l’offre) \* pondération du critère « Prix » le prix analysé sera celui de la simulation, Cfr « Forme et contenu des offres »* | |
| 2 | Maîtrise des domaines d'expertise liés à ce lot | 15 |
|  | *Les domaines d’expertise confirmés seront cotés à 1, le résultat de chaque expert sera obtenu par la sommes des côtes individuelles des domaines d’expertise (annexe D), le niveau du soumissionnaire sera obtenu par la moyenne arithmétique des experts présentés par celui-ci.  Les résultats seront comparés entre eux par une règle de 3.*  *Score offre = (résultat du soumissionnaire / résultat maximal) \* pondération du critère « Maîtrise des domaines d’expertise »* | |
| 3 | *Méthodologie d’analyse et d’implémentation* | *10* |
|  | *Chaque réponse aux questions posées sera évaluée par une note allant de 1 à 10. Les résultats individuels seront sommés et comparés entre eux par une règle de 3.*  *Score offre = (résultat du soumissionnaire / résultat maximal) \* pondération du critère « Méthodologie d’analyse et d’implémentation »* | |
| 4 | *Qualité de la documentation (analyse, installation, projet)* | *5* |
|  | *Chaque réponse aux questions posées sera évaluée par une note allant de 1 à 10. Les résultats individuels seront sommés et comparés entre eux par une règle de 3.*  *Score offre = (résultat du soumissionnaire / résultat maximal) \* pondération du critère « Qualité de la documentation »* | |
| 5 | *Qualité technique* | *15* |
|  | *Chaque réponse aux questions posées sera évaluée par une note allant de 1 à 10. Les résultats individuels seront sommés et comparés entre eux par une règle de 3.*  *Score offre = (résultat du soumissionnaire / résultat maximal) \* pondération du critère « Qualité technique »* | |
| 6 | *Licence libre* | *5* |
|  | *Si le matériel ou le logiciel proposé est basé et reste lui-même sous licence libre, ce soumissionnaire obtient le résultat de 5. Si le matériel ou le logiciel proposé est basé et reste lui-même sous licence propriétaire, ce soumissionnaire obtient le résultat de 0.* | |
| Pondération totale des critères d'attribution : | | 100 |

Une certaine valeur a été attribuée à chaque critère. Sur base de l'évaluation de tous ces critères, tenant compte de la valeur attribuée à chacun, le marché sera attribué au soumissionnaire présentant l'offre régulière économiquement la plus avantageuse du point de vue du pouvoir adjudicateur.

## Options et Variantes

La distinction qui est faite entre option et variante se décrit comme suit :

* Une variante est un élément encadré par le pouvoir adjudicateur et proposé à l’initiative de l’adjudicataire, qui remplace en partie la demande du pouvoir adjudicateur ;
* Une option est un élément qui vient compléter un équipement/service, sans le remplacer.

### Variantes

Aucune variante (libre ou facultative) n’est prévue ou autorisée.

### Options

Les options autorisées sont liées aux éléments (matériels ou logiciels) permettant de définir la réponse à apporter à un besoin, en ce compris la granularité financière du bordereau de prix.

## Choix de l’offre

Le pouvoir adjudicateur choisit l'offre économiquement la plus avantageuse, déterminée en se fondant sur le meilleur rapport qualité / prix.

Par la présentation de son offre, le soumissionnaire accepte toutes les clauses du Cahier des Charges et renonce à toutes les autres conditions. Si le pouvoir adjudicateur constate, lors de l’analyse des offres, que le soumissionnaire a ajouté des conditions qui rendent l’offre imprécise ou si le soumissionnaire émet des réserves quant aux conditions du Cahier des Charges, le pouvoir adjudicateur se réserve le droit de considérer l’offre comme substantiellement irrégulière.

Le pouvoir adjudicateur rectifie les erreurs dans les opérations arithmétiques et les erreurs purement matérielles dans les offres, sans que sa responsabilité soit engagée pour les erreurs qui n’auraient pas été décelées. Pour ce faire il peut, dans le délai qu’il détermine, inviter le soumissionnaire à préciser et à compléter la teneur de son offre sans la modifier, afin de rechercher l’intention réelle.

**Marché divisé en lots**

Le pouvoir adjudicateur a le droit de n'attribuer que certains lots et, éventuellement, de décider que les autres lots feront l'objet d'un ou plusieurs nouveaux marchés, au besoin selon un autre mode.

Le soumissionnaire peut présenter une offre pour tous les lots.

Il est interdit de compléter l'offre en mentionnant une proposition d'amélioration consentie par le soumissionnaire sur chaque lot en cas de réunion de certains lots pour lesquels il remet offre.

## Limites de la centrale d’achats

La présente centrale d’achat est limitée aux pouvoirs adjudicateurs bénéficiaires (PAB), à savoir, des pouvoirs locaux wallons ayant marqué un intérêt préalablement au lancement du présent marché et listés en annexe D du présent cahier spécial des charges.

Les marchés subséquents sont commandés par les PAB au fur et à mesure des besoins de ses membres. Ces données ne sont pas un engagement ferme de commande de la part du pouvoir adjudicateur et de ses membres. Ces données constituent une information à l’attention des soumissionnaires.

Le montant cumulé maximal qui pourra être attribué dans le cadre de marchés subséquents fondés sur cette centrale d’achat est de 4.000.000 € TVAC. Une fois ce maximum atteint, aucun nouveau marché ne pourra plus être attribué via la centrale d’achat. La fin de la centrale d’achats ne porte pas préjudice à la poursuite de l’exécution des marchés subséquents en cours.

L’attention des soumissionnaires est attirée sur le fait que la conclusion de l’accord cadre n’entraîne aucune exclusivité dans leurs chefs, iMio se réservant donc le droit de satisfaire les besoins de ce présent marché par d’autres moyens (cfr absence d’exclusivité).

# Dispositions contractuelles

Cette deuxième partie fixe la procédure relative à l’exécution du marché.

Pour autant qu’il n’y soit pas dérogé, l'arrêté royal du 14 janvier 2013 et ses modifications ultérieures établissant les règles générales d'exécution des marchés publics est d’application.

## Fonctionnaire dirigeant

Le contrôle de la procédure initiale ainsi que d’éventuelles inspections des marchés subséquents se déroulent sous l’autorité du conseil d’administration d’iMio représenté par :

Nom : Mr Frédéric Rasic

Adresse : IMIO, Rue Léon Morel, 1 à 5032 Isnes

Téléphone : 081/586.100

Fax : 081/586.129

E-mail : marche.public@imio.be

Le conseil d’administration d’iMio est le seul compétent pour prendre des décisions dans le cadre de la procédure initiale. La personne désignée ci-avant est le représentant désigné par le fonctionnaire dirigeant permettant un contact entre le pouvoir adjudicateur et l’adjudicataire. Elle n’a pas autorité de décision.

Le fonctionnaire dirigeant peut se faire représenter par une personne physique. Dans ce cas, cette personne doit être désignée par le fonctionnaire dirigeant préalablement à l’attribution du marché subséquent.

Le fonctionnaire dirigeant est le seul compétent pour prendre des décisions en matière d’exécution. La personne désignée pour représentation permet un contact entre le pouvoir adjudicateur et l’adjudicataire. Elle n’a pas pouvoir de décision.

Mandats du fonctionnaire dirigeant et son représentant :

* Le fonctionnaire dirigeant est mandaté pour prendre toutes les décisions nécessaires, dans les limites imposées par le présent cahier spécial des charges, afin de veiller à la bonne exécution du contrat ;
* Toute promesse, modification ou accord qui diverge des conditions de ce Cahier spécial des Charges et qui n’est pas notifié par le pouvoir adjudicateur est à considérer comme nul par les deux parties ;
* Le fonctionnaire dirigeant peut déléguer tout ou partie de ses fonctions à un de ses délégués moyennant communication écrite aux participants concernés ;
* Le représentant du fonctionnaire dirigeant ne peut prescrire des services modificatifs ou supplémentaires quelconques sans l’accord écrit du Pouvoir adjudicateur.

Toutes communications et notifications que l’adjudicataire estime devoir faire concernant son marché sont faites, par écrit, au fonctionnaire dirigeant.

L’adjudicataire ne pourra se prévaloir du fait qu’une surveillance ou un contrôle a été exercé par le pouvoir adjudicateur ou son fonctionnaire dirigeant pour prétendre être dégagé de sa responsabilité si les travaux venaient à être refusés ultérieurement.

L’exécution des marchés subséquents se déroulera sous le contrôle de l’organe exécutif du pouvoir adjudicateur bénéficiaire.

## Sous-traitants

Le soumissionnaire peut faire valoir les capacités de sous-traitants ou d'autres entités. Dans ce cas, il joint à son offre les documents utiles desquels ressort l'engagement de ces sous-traitants ou entités de mettre les moyens nécessaires à la disposition du soumissionnaire. **Le sous-traitant déposera son DUME.**

Si un opérateur économique souhaite recourir aux capacités d'autres entités pour sa sélection qualitative en ce qui concerne les critères relatifs aux titres d'études et professionnels ou à l'expérience professionnelle pertinente, l’opérateur économique est tenu de travailler avec ces sous-traitants désignés lors de l'exécution du marché. Le recours à d'autres sous-traitants est soumis à l'accord préalable du pouvoir adjudicateur.

En application de l'article 74 de l'AR du 18 avril 2017, le soumissionnaire indique dans son offre la part du marché qu'il a éventuellement l'intention de sous-traiter ainsi que les sous-traitants proposés.

Le pouvoir adjudicateur transmet, au plus tard au début de l’exécution du marché, les informations suivantes à l’adjudicateur : le nom, les coordonnées et les représentants légaux de tous les sous-traitants, quelle que soit la mesure dans laquelle ils participent à la chaîne de sous-traitance et quelle que soit leur place dans cette chaîne, participant à l'exécution du marché, dans la mesure où ces informations sont connues à ce stade.

Le pouvoir adjudicateur est, pendant toute la durée du marché, tenu de porter sans délai à la connaissance de l’adjudicateur de tout changement relatif à ces informations ainsi que des informations requises pour tout nouveau sous-traitant qui participera ultérieurement à ces travaux ou à la prestation de ces services.

Les adjudicataires demeurent responsables envers le pouvoir adjudicateur lorsqu'ils confient tout ou partie de leurs engagements à des sous-traitants.

Le pouvoir adjudicateur ne lie aucun lien contractuel avec ces sous-traitants.

Ces sous-traitants ne peuvent se trouver dans un des cas d'exclusion visés à l'article 67 de la loi du 17 juin 2016, hormis le cas où l'entrepreneur, le fournisseur ou le prestataire de services concerné, conformément à l'article 70 de la loi, démontre vis-à-vis de du pouvoir adjudicateur avoir pris les mesures suffisantes afin de prouver sa fiabilité.

En application de l'article 12/4 de l'AR du 14 janvier 2013, ces sous-traitants satisfont, proportionnellement à la partie du marché qu'ils exécutent, aux exigences minimales en matière de capacité technique et professionnelle imposées par les documents du marché.

**Sous-traitants**  
Dans le cadre de ce marché, la sous-traitance est autorisée au maximum d’un seul niveau :

* Adjudicataire du marché
  + Sous-traitant de niveau 1 : acceptable
    - Sous-traitant de niveau 2 : Interdit

Le candidat soumissionnaire doit joindre à son offre une déclaration de sous-traitance signée par le sous-traitant déclaré. À défaut de déclaration signée, l’offre du candidat soumissionnaire sera déclarée irrégulière.

## Assurances

L'adjudicataire contracte les assurances couvrant sa responsabilité en matière d'accidents de travail et sa responsabilité civile vis-à-vis des tiers lors de l'exécution du marché.

Dans un délai de trente jours à compter de la conclusion du marché, l'adjudicataire justifie qu'il a souscrit ces contrats d'assurances, au moyen d'une attestation établissant l'étendue de la responsabilité garantie requise par les documents du marché.

À tout moment durant l'exécution du marché, l'adjudicataire produit cette attestation, dans un délai de quinze jours à compter de la réception de la demande du pouvoir adjudicateur.

## Cautionnement

Aucun cautionnement ne sera exigé pour ce marché initial.

**Article 25 de l'arrêté royal du 14 janvier 2013**

Aucun cautionnement n'est exigé alors qu'il est légalement obligatoire.

Justification : Il est dérogé à l'article 25 § 1er, 2°, h) de l'arrêté royal du 14 janvier 2013 établissant les règles générales d'exécution des marchés publics afin d'éviter les lourdeurs administratives rendues inutiles par le montant de certaines commandes, le cautionnement de 5% n'est exigé que pour les commandes, passées par les PAB et subséquentes à ce marché, supérieures au montant de 50.000 €. Les cautionnements seront donc constitués dans le cadre des marchés subséquents effectués par les pouvoirs adjudicateurs bénéficiaires de la centrale d’achat.

## CV Vitrines

Le soumissionnaire est tenu de faire participer aux missions les personnes qui ont été proposées en réponse à cet accord cadre. Le pouvoir adjudicateur entend ainsi interdire la pratique des CV-Vitrines. Les sanctions sont définies dans les dispositions contractuelles relatives à l’exécution (II.9 Sanctions).

## Clause de réexamen : Révisions de experts proposés

La pratique des CV Vitrine étant interdite, et vu les évolutions professionnelles possibles au cours de la durée de vie de la centrale d’achat, le remplacement des experts chargés des mission est autorisé, à condition qu’il ait été :

* Sollicité au fonctionnaire dirigeant du pouvoir adjudicateur de ce marché ;
* Autorisé par ce dernier.

Ce processus ne peut pas être réalisé auprès du PAB.

## Clause de réexamen : Révisions de prix

Une révision des prix sera autorisée, à fréquence annuelle. Elle est autorisée à la hausse et à la baisse mais sera plafonnée à une augmentation maximum équivalente à l’indexation annuelle de l’ipc lissé publié sur statbel.fgov.be.

Le soumissionnaire n’est pas autorisé à cumuler les augmentations non-réclamées pour justifier une révision dépassant le taux fixé.

La révision des prix demandée par le soumissionnaire doit être basée sur des paramètres objectifs et contrôlables, elle doit utiliser des coefficients de pondération appropriés, elle reflète ainsi la structure réelle des coûts.

Les motifs pouvant être invoqués sont :

* Licences :
  + Prix d’achat
  + Taux de change
* Matériel :
  + Prix d’achat
  + Taux de change
* Fournitures/énergies :
  + Prix d’achat
  + Taux de change
* Prestations :
  + Indice salaire

Les demande de révision des prix doivent être introduites par courrier, à l’attention du fonctionnaire dirigeant, au plus tard 2 mois avant la date échéance. La date échéance est l’anniversaire de l’attribution du marché (en pratique, si l’attribution du marché est décidée par le fonctionnaire dirigeant d’iMio le 1 juillet 2023, les demandes de révision des prix pour l’année suivante doivent être introduites au plus tard le 1 mai des années suivantes). À défaut de respecter le délai d’introduction, la demande de révision des prix sera ignorée, il sera interdit aux adjudicataires concernés d’adapter leur prix.

## Durée et délai d’exécution

Durée totale de ce marché : 48 mois

Le marché prend cours le premier jour calendrier qui suit le jour où les adjudicataires ont reçu la notification de la conclusion du marché.

Lorsque le marché est résilié en application d’une mesure d’office ou en application de l’article II.9 du présent cahier, la résiliation du marché est limitée au seul adjudicataire à l’encontre de qui la mesure a été prise.

Délai d’exécution des marchés subséquents est à convenir lors de la commande

Le marché subséquent prend cours le premier jour calendrier qui suit le jour où iMio a reçu l’accusé de réception du bon de commande. Les marchés subséquents conclus avant la date d’échéance de la centrale d’achat demeurent exécutables jusqu’à leur terme.

## Sanctions

Lorsqu’un adjudicataire est 2 fois d’affilée dans l’incapacité d’exécuter correctement la mission, ou lorsqu’un de ses experts expert délivre à 2 reprises un travail incomplet ou incorrect (cfr. Vérification des prestations, description des exigences techniques et annexes du présent cahier des charges), l’adjudicataire peut être exclu de la centrale d’achat et entraîner la fermeture du lot concerné.

## Procédure de commande

Les informations relatives à la méthodologie de commande(s) subséquente(s) sont présentées dans la section « Centrale d’achat ».

## Procédure de facturation et Délai de paiement

Les modalités de facturation sont à définir par les pouvoirs adjudicateurs bénéficiaires, dans le cadre de leur(s) marché(s) subséquent(s).

**Facturation électronique**

Le pouvoir adjudicateur accepte la transmission des factures sous un format électronique (au format XML selon le standard PEPPOL bis), conformément à l'article 192/1 de la loi du 17/06/2016.

Les factures pourront être soumises directement via https://digital.belgium.be/e-invoicing/ ou via votre outil comptable (connecté au réseau PEPPOL).

La facture électronique doit obligatoirement comporter les mentions suivantes :

1° les identifiants de processus et de facture ;

2° la période de facturation ;

3° les renseignements concernant le vendeur ;

4° les renseignements concernant l’acheteur ;

5° les renseignements concernant le bénéficiaire du paiement ;

6° les renseignements concernant le représentant fiscal du vendeur ;

7° la référence du contrat ;

8° les détails concernant la fourniture ;

9° les instructions relatives au paiement ;

10° les renseignements concernant les déductions ou frais supplémentaires ;

11° les renseignements concernant les postes figurant sur la facture ;

12° les montants totaux de la facture ;

13° la répartition par taux de TVA.

## Délai de garantie

Les matériels et logiciels doivent être garantis pour une durée identique à celle du marché et prolongés par la souscription aux contrats de maintenance et support.

## Réception

Les modalités de réception sont à définir par les pouvoirs adjudicateurs bénéficiaires, dans le cadre de leur(s) marché(s) subséquent(s), une procédure minimale est toutefois définie dans le cadre de la centrale d’achat (Cfr section Centrale d’achat).

## Ressortissants d’un pays tiers en séjour illégal

Lorsque l’adjudicataire ou sous-traitant reçoit copie de la notification visée à l’article 49/2, alinéa 4, du Code pénal social, dans laquelle il est informé qu’il occupe en Belgique un ou plusieurs ressortissants d’un pays tiers en séjour illégal, cet adjudicataire ou sous-traitant s’abstient, avec effet immédiat, de se rendre encore au lieu d’exécution du marché ou de poursuivre l’exécution du marché, et ce jusqu’à ce que l’autorité adjudicatrice donne un ordre contraire.

Il en va de même lorsque l’adjudicataire ou sous-traitant est informé :

- soit par l’adjudicataire ou par l’autorité adjudicatrice selon le cas de ce qu’ils ont reçu la notification, visée à l’article 49/2, alinéas 1er et 2, du Code pénal social, concernant cette entreprise ;

- soit via l’affichage prévu par l’article 35/12 de la loi du 12 avril 1965 relative à la protection de la rémunération des travailleurs, qu’il occupe en Belgique un ou plusieurs ressortissants d’un pays tiers en séjour illégal.

Par ailleurs, l’adjudicataire ou sous-traitant est tenu d’insérer, dans les contrats de sous-traitance qu’il conclurait éventuellement, une clause stipulant que :

1° le sous-traitant s’abstient de se rendre encore au lieu d’exécution du marché ou de poursuivre l’exécution du marché, lorsqu’une notification établie en exécution de l’article 49/2 du Code pénal social révèle que ce sous-traitant occupe un ressortissant d’un pays tiers en séjour illégal ;

2° le non-respect de l’obligation visée au point 1° est considéré comme un manquement grave dans le chef du sous-traitant, à la suite duquel l’entreprise est habilitée à résilier le contrat ;

3° le sous-traitant est tenu d’insérer, dans les contrats de sous-traitance, une clause analogue à celle visée aux points 1° et 2° et d’assurer que de telles clauses soient également insérées dans les contrats de sous-traitance ultérieurs.

## Rémunération due à ses travailleurs

Lorsque l’adjudicataire ou sous-traitant reçoit copie de la notification visée à l’article 49/1, alinéa 3, du Code pénal social, par laquelle il est informé d’un manquement grave à son obligation de payer dans les délais, à ses travailleurs, la rémunération à laquelle ceux-ci ont droit, cet adjudicataire ou sous-traitant s’abstient, avec effet immédiat, de se rendre encore au lieu d’exécution du marché ou de poursuivre l’exécution du marché, et ce jusqu’à ce qu’il présente la preuve à l’autorité adjudicatrice que les travailleurs concernés ont reçu l’intégralité de leur rémunération.

Il en va de même lorsque l’adjudicataire ou sous-traitant est informé :

- soit par l’adjudicataire ou par l’autorité adjudicatrice selon le cas de ce qu’ils ont reçu la notification visée à l’article 49/1, alinéa 1er, du Code pénal social, concernant cette entreprise ;

- soit via l’affichage prévu par l’article 35/4 de la loi du 12 avril 1965 relative à la protection de la rémunération des travailleurs.

Par ailleurs, l’adjudicataire ou sous-traitant est tenu d’insérer, dans les contrats de sous-traitance qu’il conclurait éventuellement, une clause stipulant que :

1° le sous-traitant s’abstient de se rendre encore au lieu d’exécution du marché ou de poursuivre l’exécution du marché, lorsqu’une notification établie en exécution de l’article 49/1 du Code pénal social révèle que ce sous-traitant manque gravement à son obligation de payer dans les délais, à ses travailleurs, la rémunération à laquelle ceux-ci ont droit ;

2° le non-respect de l’obligation visée au point 1° est considéré comme un manquement grave dans le chef du sous-traitant, à la suite duquel l’adjudicataire est habilité à résilier le contrat ;

3° le sous-traitant est tenu d’insérer, dans les contrats de sous-traitance, une clause analogue à celle visée aux points 1° et 2° et d’assurer que de telles clauses soient également insérées dans les contrats de sous-traitance ultérieurs.

## Protection des données

Les données personnelles collectées dans le cadre du marché public par l'adjudicataire du marché, ainsi que par ses sous-traitants, agissant en tant que responsables du traitement doivent être traitées conformément au Règlement général sur la protection des données (Règlement (UE) 2016/679 du Parlement Européen et Du Conseil du 27 avril 2016).

Dans ce cadre, l’adjudicataire et ses sous-traitants s’engagent à ce que les informations personnelles collectées soient utilisées uniquement pour l'exécution du marché, ou en exécution d'une obligation légale, ou avec l'accord explicite de l'adjudicateur.

## Devoir de réserve et confidentialité

L’adjudicataire s’abstiendra, en toutes circonstances, de révéler le moindre renseignement concernant le marché ou IMIO et les bénéficiaires, sans l’approbation de IMIO. Cette obligation s’applique également à toute personne à laquelle on fait appel dans le cadre du présent marché. Les personnes mobilisées pour l’exécution du marché seront tenues de signer un engagement de confidentialité séparé à la demande de IMIO.

Il est renvoyé pour le surplus aux articles 19 à 23 de l’arrêté royal du 14 janvier 2013.

## Pénalités

Conformément à l’article 45, §1er de l’arrêté royal du 14 janvier 2013 établissant les règles générales d’exécution dans les marchés publics, le pouvoir adjudicateur est en mesure de réclamer une pénalité.

Les modalités de pénalités sont à définir par les pouvoirs adjudicateurs bénéficiaires, dans le cadre de leur(s) marché(s) subséquent(s).

## Compétence juridictionnelle et législation applicable

Le présent marché est exclusivement soumis au droit belge.

Tous les litiges relatifs à l’exécution de ce marché établissant la centrale d’achat et des marchés subséquents sont exclusivement tranchés par les tribunaux compétents de l’arrondissement judiciaire de Namur. La langue véhiculaire est le français.

IMIO n’est en aucun cas responsable des dommages causés à des personnes ou à des biens qui sont la conséquence directe ou indirecte des activités nécessaires à l’exécution de ce marché. L’adjudicataire garantit IMIO contre toute action en dommages et intérêts par des tiers à cet égard.

## Règlement Général de Protection des Données

### Protection des données

Informations relatives aux droits des soumissionnaires et adjudicataires en tant que personne concernée par le traitement des données personnelles dans le cadre du présent marché

En application du Règlement (UE) 2016/679 du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre

Circulation de ces données (le « RGPD »), l’intercommunale iMio, en tant que Pouvoir adjudicateur, est responsable du traitement des données des soumissionnaires au présent marché.

Les coordonnées du Pouvoir adjudicateur sont :

* IMIO
* Rue Léon Morel, 1,
* 5032 Isnes

Les coordonnées du Délégué à la protection des données du Pouvoir adjudicateur sont :

* iMio
* Jessie Maloteau
* vieprivee@imio.be

Dans le cadre du présent marché, les données du soumissionnaire ne sont traitées qu’aux fins de la gestion de la procédure d’attribution du présent marché et les données de l’adjudicateur sont traitées aux fins de la mise en œuvre du présent marché. En aucun cas, vos données ne sont traitées par le Pouvoir adjudicateur à des fins commerciales ou publicitaires ni transférées à des tiers qui utiliseraient ces données à de telles fins.

La durée de conservation de vos données n’excède pas la durée nécessaire au regard des finalités pour lesquelles les données sont traitées.

La passation du présent marché est conditionnée, en partie, à la transmission des données du soumissionnaire au pouvoir adjudicataire. La non-transmission de ces données peut avoir pour conséquence l’exclusion de la candidature du soumissionnaire en cause.

Dans le cadre de l’exécution du présent marché (en ce compris la phase précontractuelle), le Pouvoir adjudicateur peut être amené à recevoir ou à communiquer vos données à caractère personnel notamment aux destinataires suivants :

* Vous-même ;
* Des Pouvoirs locaux, Services publics fédéraux ou régionaux ;
* Des parties à une procédure administrative ou judiciaire qui implique l’intercommunale IMIO ;
* Des tiers dans le cadre d’obligations contractuelles.

Les données du soumissionnaire ne sont transmises à un pays tiers (hors UE) que dans la

Stricte nécessité de l’exercice des missions du pouvoir adjudicateur en tant qu’autorité publique ou lorsque une obligation légale ou conventionnelle l’impose.

Le soumissionnaire a les droits suivants, applicables dans les limites du RGPD :

* Droit d’accès à ses données ;
* Droit de rectifier ses données ;
* Droit à l’effacement de ses données ;
* Droit à la limitation du traitement de ses données ;
* Droit à la portabilité de ses données ;
* Droit de s’opposer au traitement de ses données.

Afin d’exercer ses droits, le soumissionnaire peut contacter le pouvoir adjudicataire en prenant directement contact avec notre Délégué à la protection des données.

Si le soumissionnaire estime que le pouvoir adjudicataire n’a pas respecté ses droits en matière de vie privée, il a la possibilité d’introduire une plainte auprès de l’autorité de protection des données belge :

* Autorité de protection des données
* Rue de la Presse, 35
* 1000 Bruxelles
* +32 274 48 00
* [Https://www.autoriteprotectiondonnees.be/](https://www.autoriteprotectiondonnees.be/)

### Obligations de l’adjudicataire en tant que sous-traitant du Pouvoir adjudicateur dans le cadre des traitements de données

En application du Règlement (UE) 2016/679 du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (le « RGPD »), l’adjudicataire doit/peut être considéré comme sous-traitant pour le compte du Pouvoir adjudicateur.

Il en découle que l’adjudicataire s’engage à mettre en place toutes les garanties suffisantes quant à la mise en œuvre de mesures techniques et organisationnelles appropriées de manière à ce que les traitements (éventuels) de données répondent aux exigences du RGPD et garantissent la protection des droits des personnes concernées par lesdits traitements.

À cet égard, l’adjudicataire s’engage à :

* Ne traiter les données à caractère personnel que sur instruction documentée du responsable du traitement, y compris en ce qui concerne les transferts de données à caractère personnel vers un pays tiers ou à une organisation internationale, à moins qu'il ne soit tenu d'y procéder en vertu du droit de l'Union ou du droit de l'État membre auquel l’adjudicataire est soumis; dans ce cas, l’adjudicataire informe le Pouvoir adjudicateur de cette obligation juridique avant le traitement, sauf si le droit concerné interdit une telle information pour des motifs importants d'intérêt public ;
* Veiller à ce que les personnes autorisées à traiter les données à caractère personnel s'engagent à respecter la confidentialité ou soient soumises à une obligation légale appropriée de confidentialité ;
* Prendre toutes les mesures appropriées afin de garantir la sécurité des traitements de données ;
* En tenant compte de la nature du traitement, aider le Pouvoir adjudicateur, par des mesures techniques et organisationnelles appropriées, dans toute la mesure du possible, à s'acquitter de son obligation de donner suite aux demandes dont les personnes concernées le saisissent en vue d'exercer leurs droits prévus ;
* Aider le Pouvoir adjudicateur à garantir le respect des obligations prévues par le RGPD (notamment en matière de sécurisation des données, d’analyse d’impact et de fuites de données) compte tenu de la nature du traitement et des informations à la disposition du sous-traitant ;
* Selon le choix du responsable du traitement, supprimer toutes les données à caractère personnel ou les renvoyer au responsable du traitement au terme de la prestation de services relatifs au présent marché, et à détruire les copies existantes, à moins que le droit de l'Union ou le droit de l'État membre n'exige la conservation des données à caractère personnel ; et
* À mettre à la disposition du responsable du traitement toutes les informations nécessaires pour démontrer le respect des obligations prévues au présent article et pour permettre la réalisation d'audits, y compris des inspections, par le Pouvoir adjudicateur ou un autre auditeur qu'il a mandaté, et contribuer à ces audits.

A cet égard, l’adjudicataire informe immédiatement le Pouvoir adjudicateur si, selon lui, une instruction constitue une violation du présent règlement ou d'autres dispositions du droit de l'Union ou du droit des États membres relatives à la protection des données.

### Sécurité

Il est demandé que le plus grand soin soit apporté par l’adjudicataire à la gestion de la sécurité informatique, tant matérielle (hardware) qu’immatérielle (software). La gestion de la sécurité informatique porte sur l’intégrité, la disponibilité et la confidentialité des données transportées mais aussi sur la protection contre les failles de sécurité et les infections de logiciels malveillants, tels que les virus, vers, portes dérobées, chevaux de Troie, logiciels espions et autres formes de logiciels malicieux.

L’adjudicataire prend toutes les mesures nécessaires, notamment de sécurité matérielle, afin d’éviter tout virus ou toute contamination de la structure informatique du Pouvoir adjudicateur tout au long de la durée du présent marché, qui seraient liés aux matériels et/ou aux prestations fournies par l’adjudicataire dans le cadre du présent marché.

En cas d’incident de sécurité (lui étant imputable ou non), l’adjudicataire s’engage à intervenir et à coopérer avec le Pouvoir adjudicateur pour rétablir le niveau de sécurité initial attendu, et à entreprendre tout ce qui est en son pouvoir pour éviter qu’un tel événement ne se reproduise dans le futur. Si l’incident de sécurité est imputable à l’adjudicataire ou à son matériel (y compris par le biais de ses sous-traitants), son intervention conformément au présent paragraphe est intégralement à sa charge.

## Centrale d’achats

Le présent marché est passé sous forme d’une centrale d’achat, passant des activités d’achats centralisées sous la forme de marché, conformément aux articles 2, 6° et 7° b) et 47 de la loi du 17 juin 2016 sur les marchés publics. Dans ce cadre, IMIO intervient en tant que pouvoir adjudicateur organisateur du marché. Chaque membre d’iMio est un pouvoir adjudicateur bénéficiaire du marché. Chaque « administration cliente » bénéficiaire du marché agira comme pouvoir adjudicateur.

Pour pouvoir bénéficier des marchés d’IMIO, « l’administration cliente » doit impérativement avoir marqué son intérêt et valablement décidé d’adhérer à la centrale d’achat. La liste des bénéficiaires ayant signé la convention à la date de la publication du présent Cahier spécial des charges est reprise en annexe D de ce cahier des charges. Cette liste de membres est disponible pour l’adjudicataire du marché sur demande auprès d’iMio, tout au long de l’exécution du marché.

Le prestataire s’engage à faire bénéficier, pendant toute la durée du marché, les adhérents à IMIO, des clauses et conditions reprises dans les documents du présent marché et, pour le surplus, dans l’offre de l’adjudicataire telle qu’approuvée par le pouvoir adjudicateur (prix, conditions de livraison, ...).

L’adhésion à la centrale d’achat « Cybersécurité » permet à « l’administration cliente » de commander des fournitures, logiciels et services en bénéficiant des conditions remises par les adjudicataires.

« L’administration cliente » bénéficie des marchés d’IMIO par simple commande.

D’un point de vue juridique, IMIO garantit à « l’administration cliente » que les dispositions prévues par la législation sur les marchés publics ont été respectées et que IMIO est un pouvoir adjudicateur agissant sous forme de centrale au sens de l’article 2,6° de la loi 17 juin 2016.

La responsabilité de la sélection dans le catalogue de l’adjudicataire des fournitures ou services par commande est du ressort des membres bénéficiaires. IMIO agit en tant qu’intermédiaire via sa centrale de marché et n’est pas responsable d’une erreur de sélection dans les choix faits par le membre bénéficiaire. Les membres bénéficiaires seront responsables des contrats qu’ils concluront avec l’adjudicataire retenu. Imio ne supporte aucune responsabilité pour cette phase, cela n’empêche pas iMio de vérifier que les services et fournitures délivrées sont conformes aux services et fournitures fixés par ce marché public. Lors d’une demande d’offre ou à la commande, l’adjudicataire devra vérifier que les configurations souhaitées sont cohérentes et adéquates aux attentes et situations propres de l’« administration cliente ».

La facturation des commandes de fournitures, logiciels ou services dans le cadre du présent marché seront facturés au « membre bénéficiaire » par l’adjudicataire.

### Limites de la centrale d’achat

La présente centrale d’achat est limitée aux pouvoirs adjudicateurs bénéficiaires (PAB), à savoir, des pouvoirs locaux wallons ayant marqué un intérêt préalablement au lancement du présent marché et listés en annexe D du présent cahier spécial des charges.

Les marchés subséquents sont commandés par les PAB au fur et à mesure des besoins de ses membres. Ces données ne sont pas un engagement ferme de commande de la part du pouvoir adjudicateur et de ses membres. Ces données constituent une information à l’attention des soumissionnaires.

Le montant cumulé maximal qui pourra être attribué dans le cadre de marchés subséquents fondés sur cette procédure ouverte (tous lots confondus) est de 4.000.000 € TVAC. Une fois ce maximum atteint, aucun nouveau marché ne pourra plus être attribué via la centrale d’achat. La fin de la centrale d’achats ne porte pas préjudice à la poursuite de l’exécution des marchés subséquents en cours. La limite de la centrale d’achat est définie par les commandes des axes matériels, logiciels et services.

L’attention des soumissionnaires est attirée sur le fait que la conclusion de l’accord cadre n’entraîne aucune exclusivité dans leurs chefs, le PA se réservant donc le droit de satisfaire les besoins de ce présent marché par d’autres moyens (cfr absence d’exclusivité).

### Conditions d’accès

Pour pouvoir recourir à la centrale d’achat découlant de ce marché, le Pouvoir local doit remplir 2 conditions :

* Avoir marqué son intérêt pour la centrale d’achat (Cfr Annexe D du présent cahier spécial des charges) ;
* Avoir décidé d’adhérer à la centrale d’achat (Cfr Annexe F du présent cahier spécial des charges). Sauf délégation, cette décision relève de l’organe législatif du pouvoir adjudicateur bénéficiaire (Conseil communal pour les Administrations Communales, Conseil de l’action sociale pour les CPAS, etc.) ;
* Avoir décidé de recourir à la centrale d’achat pour leur marché subséquent.

Les adjudicataires doivent s’assurer du respect de ces conditions pour établir une offre de prix basée sur cette centrale d’achat.

### Procédure de commande

La procédure de commande sera précisée lors du lancement de la centrale d’achat, toutefois, voici la procédure pressentie.

Pour chaque demande de devis, l’adjudicataire du marché doit :

* Vérifier l’adhésion du PAB à la centrale d’achat, pour ce faire, il obtient de la part du PAB la décision d’adhésion à la centrale d’achat Cybersécurité (modèle fourni en annexe F au présent cahier spécial des charges) ;
* Rencontrer le PAB et définir avec lui les éléments nécessaires à la réalisation du projet (par éléments nécessaires, on entend toutes les prestations, logiciels et matériels nécessaires) ;
* Informer iMio des :
  + Informations relatives au PAB (identification du PAB et délibération d’adhésion) ;
  + Nature de la mission demandée ;
  + Copie de l’offre réalisée en réponse à l’expression des besoins, cette offre doit spécifiquement faire référence à la centrale d’achat, et le lot correspondant.
* Transmettre au PAB l’offre réalisée en réponse à l’expression des besoins ;
* Obtenir la délibération d’attribution du marché subséquent, cette décision doit être basée sur la central d’achat.
* Transmettre cette délibération d’attribution à iMio.

Toute commande qui n’aura pas été obtenue en respectant ces étapes sera de facto considérée comme nulle et non-avenue.

### Procédure de réception des livraisons, implémentations et prestations

Lorsque l’adjudicataire du marché a terminé le travail tel que défini dans son offre de prix (Cfr procédure de commande), il doit :

* Obtenir le rapport de livraison signé par le pouvoir adjudicateur bénéficiaire (Annexe E du présent CSC) ;
* Facturer les services et équipements fournis ;
* Contrôler le paiement de la facture ;
* Transmettre à iMio ces éléments (rapport de livraison, facture émise et preuve de paiement)

### Moyen de contrôles

Ces éléments (liés à la commande et les facture/paiement) seront utilisés comme moyen de contrôle du respect des livrables et conditions de la centrale d’achat, et également pour l’octroi du subside régional relatif à la cybersécurité, il est donc fondamental que les fournisseurs respectent ces procédures et étapes. Un reporting général sera donc mis en œuvre, l’adjudicataire devra s’y conformer.

Tout soumissionnaire qui ne s’engage pas à respecter la procédure de commande et le reporting verra son offre déclarée irrégulière.

### Fonctionnaire dirigeant

L’exécution et la surveillance des fournitures et/ou services des marchés subséquents se déroulent sous le contrôle et la responsabilité du fonctionnaire dirigeant du pouvoir adjudicateur désigné par le membre bénéficiaire. Le fonctionnaire dirigeant peut se faire représenter par une personne physique. Dans ce cas, cette personne doit être désignée par le fonctionnaire dirigeant préalablement à l’attribution du marché subséquent.

Le fonctionnaire dirigeant est le seul compétent pour prendre des décisions en matière d’exécution. La personne désignée pour représentation permet un contact entre le pouvoir adjudicateur et l’adjudicataire. Elle n’a pas pouvoir de décision.

Mandats du fonctionnaire dirigeant et son représentant :

* Le fonctionnaire dirigeant est mandaté pour prendre toutes les décisions nécessaires, dans les limites imposées par le présent cahier spécial des charges, afin de veiller à la bonne exécution du contrat ;
* Toute promesse, modification ou accord qui diverge des conditions de ce Cahier spécial des Charges et qui n’est pas notifié par le pouvoir adjudicateur est à considérer comme nul par les deux parties ;
* Le fonctionnaire dirigeant peut déléguer tout ou partie de ses fonctions à un de ses délégués moyennant communication écrite aux participants concernés ;
* Le représentant du fonctionnaire dirigeant ne peut prescrire des services modificatifs ou supplémentaires quelconques sans l’accord écrit du Pouvoir adjudicateur.

Toutes communications et notifications que l’adjudicataire estime devoir faire concernant son marché sont faites, par écrit, au fonctionnaire dirigeant.

L’adjudicataire ne pourra se prévaloir du fait qu’une surveillance ou un contrôle a été exercé par le pouvoir adjudicateur ou son fonctionnaire dirigeant pour prétendre être dégagé de sa responsabilité si les travaux venaient à être refusés ultérieurement.

### Accord de non-divulgation

Il est essentiel que les soumissionnaires soient assurés du respect de la confidentialité entourant ce type d’information.

Le pouvoir adjudicateur s’engage à :

* Recevoir, à traiter et à conserver les informations confidentielles de manière confidentielle ;
* Ne pas utiliser les informations confidentielles, directement ou indirectement, pour un autre but que l’objet ou pour une éventuelle coopération entre les Parties (Pouvoir adjudicateur / Adjudicataire) ;
* Limiter la divulgation des informations confidentielles aux membres de son personnel et à ses partenaires qui ont véritablement besoin de les connaître et qui sont liés par une obligation de garder le secret par rapport aux Informations Confidentielles ;
* Nonobstant ce qui précède, le pouvoir adjudicateur peut divulguer, après autorisation écrite préalable de l’adjudicataire, des informations confidentielles à ses membres, mais uniquement dans la mesure où ces membres ont véritablement besoin de connaître ces informations confidentielles et seront, ainsi que leur personnel, tenus de maintenir ces informations confidentielles. Le pouvoir adjudicateur est responsable du respect du présent contrat par ses membres ;
* Ne pas divulguer ces informations, en dehors des personnes autorisées et nécessitant l’accès à ces informations pour permettre le contrôle de la révision des prix.

# Description des exigences techniques

## Introduction

### Rôles et responsabilités

Dans le cadre de ce marché, l’équipe cyber d’iMio a eu la charge de la préparation du texte décrivant les objectifs, le contexte ainsi que les thématiques dont chaque lot est présenté ultérieurement.

Le deuxième rôle de l’équipe cyber d’iMio sera d’analyser les offres et d’instruire le dossier auprès du CA d’iMio qui attribuera les lots aux soumissionnaires.

Le troisième rôle de l’équipe cyber d’iMio sera le suivi des commandes effectuées sur la plate-forme d’achat dédiée, en concertation avec l’ensemble des parties prenantes.

Enfin, iMio jouera un rôle de conseil auprès des Pouvoirs locaux dans le cadre de ce marché à propos de la pertinence des choix posés. Cela étant, les Pouvoirs locaux restent bien entendu autonomes quant à leur décision finale.

Du fait de sa qualité, le soumissionnaire devra couvrir l’ensemble des aspects des services soumissionnés selon le lot pour soutenir le Pouvoir local dans son action.

Les exemples incluent mais ne se limite pas à :

* L’analyse des besoins et exigences potentielles spécifiques des Pouvoirs locaux ;
* L’installation et la mise en service de produits et d’applications ;
* L’assistance et la maintenance, sur site, comme en distanciel, des services fournis auprès des Pouvoirs locaux ;
* Le développement de processus et de procédures pertinents dans le cadre d’ajouts des services soumissionnés.

### Contexte

Le gouvernement wallon a lancé un projet pour soutenir les Pouvoirs locaux dans leur volonté de se protéger contre les enjeux de la cybersécurité et de la cybercriminalité. Pour répondre à cet appel, le rôle de pouvoir adjudicateur pour différents marchés liés à cet enjeu a été confié à iMio. Le projet de mutualisation et de valorisation des actifs liés à la cybersécurité vise à mettre en place un "socle commun" de cyberdéfense en Wallonie, afin de permettre aux Pouvoirs locaux de préserver la continuité de leurs missions et la protection des données de leurs citoyens. Pour atteindre cet objectif, il est nécessaire de mettre en œuvre une approche globale qui inclut des solutions de matériel, de logiciel, et d'accompagnement adaptées aux besoins des Pouvoirs locaux. Ce marché vise à sélectionner les fournisseurs qui proposeront les offres les plus adaptées et les plus compétitives pour répondre à ces enjeux.

Pour ce faire, iMio établit une central d’achat, qui comporte trois axes définis sur les caractéristiques des outils et services disponibles :

* Axe 1 : Accompagnement & formation
* Axe 2 : Matériel
* Axe 3 : Logiciel

Ce marché concerne les axes 2 (Matériel) et 3 (Logiciel).

L'évolution rapide du paysage des menaces, notamment l'augmentation du nombre de cyberattaques, exige des capacités solides dans le domaine de la cybersécurité pour garantir la résilience et la défense des Pouvoirs locaux wallons. L’expression des exigences techniques a pour objectif de définir les critères techniques et fonctionnels que les produits et services proposés doivent respecter pour être retenus dans le cadre de ce marché. Ces exigences sont essentielles pour garantir que les offres proposées répondent aux besoins et aux attentes des Pouvoirs locaux en matière de sécurité. Elles doivent donc être précises et détaillées afin de permettre aux soumissionnaires de présenter une offre qui réponde aux critères fixés.

Il est important de noter que ces exigences sont une condition sine qua non pour être retenu dans le cadre de ce marché. Toute offre qui ne respecte pas ces exigences sera rejetée. Par conséquent, il est important de prendre le temps de bien comprendre et de respecter ces exigences afin de maximiser les chances de succès de votre offre.

Dans cette section, nous détaillerons les exigences techniques et fonctionnelles qui s'appliquent à chaque lot proposé dans ce marché. Nous vous invitons donc à prendre le temps de lire attentivement ces exigences afin de vous assurer que votre offre répond aux critères fixés.

L’axe Matériel est l'ensemble des équipements, des logiciels et des matériels proposés par le soumissionnaire aux Pouvoirs locaux afin de renforcer la sécurité de leur infrastructure. Il peut inclure des équipements de sécurité tels que des pare-feu, des antivirus ou des outils de gestion de mots de passe, ainsi que des équipements de réseau et de stockage. L'objectif du matériel est de permettre aux Pouvoirs locaux de disposer de solutions adaptées pour protéger leurs systèmes et leurs données.

L’axe Logiciel est l'ensemble des programmes et des applications proposés par le soumissionnaire aux Pouvoirs locaux afin de renforcer la sécurité de leur infrastructure. Il peut inclure des logiciels de sécurité tels que des antivirus, des outils de gestion de mots de passe ou des solutions de filtrage de courriels, ainsi que des logiciels de gestion et de supervision. La sauvegarde de données fait également partie de cet axe. L'objectif du logiciel est de permettre aux Pouvoirs locaux de disposer de solutions adaptées pour protéger leurs systèmes et leurs données, et de les gérer de manière efficace. Les logiciels proposés doivent être adaptés aux besoins et aux exigences des Pouvoirs locaux et être faciles à utiliser. Le cas échéant, ils devront être compatibles avec les équipements et les matériels proposés dans les autres lots. Enfin, ils doivent être fournis avec les licences et les documents de support nécessaires pour leur utilisation et leur maintenance.

### Domaines d’expertises

Le niveau d'expertise attendu des experts est défini en fonction des spécificités techniques de chaque lot. Le profil qui n'atteint pas 75% des points d'expertise sera considéré comme irrégulière et sera exclue du marché, l’offre globale pourrait être exclue du marché si cette dernière ne rencontre plus les critères de sélection qualitative (nombre minimal d’experts).

Les experts doivent démontrer une solide formation académique dans le domaine de la cybersécurité, ainsi qu'une expérience pratique pertinente acquise lors de projets ou de stages. Ils doivent être capables de travailler en équipe et de s'adapter rapidement pour acquérir de nouvelles compétences techniques. Les connaissances et l'expérience des experts juniors seront évaluées en fonction des domaines d'expertise spécifiques à chaque lot.

Les experts seniors doivent justifier d'une expérience professionnelle approfondie d'au moins 7 ans dans le domaine de la cybersécurité, avec une expertise spécifique correspondant au lot concerné. Ils doivent démontrer leur maîtrise des normes et des meilleures pratiques, telles que l'ISO 27001, le NIS2 et le RGPD, ainsi que leur capacité à gérer des projets complexes et à fournir des conseils stratégiques en matière de cybersécurité. Les compétences et l'expérience des experts seniors seront également évaluées en fonction des domaines d'expertise spécifiques à chaque lot.

Il est essentiel que les soumissionnaires vérifient que les experts proposés possèdent les compétences techniques et l'expérience requises correspondant aux spécificités de chaque lot. Cela garantira la qualité et l'efficacité des services fournis dans le cadre du marché. Les détails des domaines d'expertise, ainsi que les critères d'évaluation, sont disponibles dans chaque lot du présent cahier spécial des charges.

La sélection des experts se fera en fonction des compétences démontrées dans leur curriculum vitae, qui devra attester de leur maîtrise des domaines d'expertise revendiqués. Les soumissionnaires sont invités à utiliser le tableau fourni dans l'Annexe C – Bordereau de réponse technique pour indiquer l'expérience professionnelle relative à chaque domaine d'expertise.

La combinaison de profils d'experts juniors et seniors est essentielle pour répondre aux exigences techniques spécifiques de chaque lot et assurer la qualité des services rendus.

### Glossaire

|  |  |
| --- | --- |
| Terme | Définition |
| ANSSI | L'Agence nationale de la sécurité des systèmes d'information est un service français. |
| ASD | Australian Signals Directorate |
| Audit de cybersécurité | Un audit de cybersécurité est un audit sur le niveau de sécurité de l'information dans une organisation afin de juger de la maturité de l’organisation. |
| CIS BENCHMARK | Normes de sécurité reconnues au niveau international pour la défense des systèmes et des données informatiques contre les cyberattaques. |
| CISSP | Certified Information Systems Security Professional |
| CSIRT | Une équipe d'intervention en cas d'incident de sécurité informatique (en anglais, Computer Security Incident Response Team ou CSIRT). |
| EBIOS | La méthode EBIOS (Expression des Besoins et Identification des Objectifs de Sécurité) est un outil complet de gestion des risques. |
| ICS | Information & Communication Services. |
| IOT | L'Internet des objets ou IdO (en anglais (the) Internet of Things ou IoT) |
| ISO | International Organization for Standardization (Organisation internationale de normalisation) |
| ISO 27001 | L'ISO/CEI 27001 est une norme internationale de sécurité des systèmes d'information de l'ISO et la CEI. |
| ISO 27002 | La norme ISO/CEI 27002 est une norme internationale concernant la sécurité de l'information. |
| ISO 27005 | La norme ISO/CEI 27005 décrit les grandes lignes d'une gestion des risques dans une perspective de mise en place d'un SMSI. |
| JIRA | Jira est un système de suivi de bugs, de gestion des incidents et de gestion de projets. |
| NIS | Directive “Network and Information System Security”. |
| NIS2 | Nouvelle directive “Network and Information System Security”. |
| NIST | National Institute of Standards and Technology |
| Pouvoir Locaux | Entités politiques subordonnées à l'Autorité fédérale et aux Régions, organisées sur le plan d'une province, d'une commune ou d'un district communal. |
| RGS | Le référentiel général de sécurité (RGS) est le cadre réglementaire permettant d’instaurer la confiance dans les échanges au sein de l’administration et avec les citoyens. |
| RSSI | Le responsable de la sécurité des systèmes d'information définit et développe la politique de sécurité de l'information de son entreprise. |
| SMSI | système de management de la sécurité de l'information. |
| TIC | Technologies de l'Information et de la Communication. |
| Vulnérabilités | Une vulnérabilité ou faille est une faiblesse dans un système informatique permettant à un attaquant de porter atteinte à l'intégrité de ce système. |

## Axe Matériel

### Exigences générales

L'axe "matériel" vise à fournir du matériel de haute qualité et performant, ainsi que tous les accessoires et licences de gestion nécessaires, pour assurer la protection des systèmes et données des Pouvoirs locaux contre les menaces de la cybersécurité.

#### Objectifs

Cet axe soutient l’ensemble des services cybersécurité liés aux matériels informatiques et aux Pouvoirs locaux.

Ce marché vise à agrémenter la centrale d’achat de matériels informatiques et de cybersécurité pour aider les Pouvoirs locaux à se protéger contre les cybermenaces.

Les objectifs sont les suivants :

* Permettre aux Pouvoirs locaux de disposer de matériel de qualité supérieure et de leur offrir les moyens de le mettre en œuvre de manière efficace pour protéger leurs systèmes et leurs données contre les menaces en ligne.
* Permettre aux Pouvoirs locaux de bénéficier d’une expérience de qualité pour gérer et entretenir leur matériel de manière adéquate en jouissant d’une assistance technique à distance, sur site, et d’une formation continue sur les matériels informatiques.
* Permettre aux Pouvoirs locaux de bénéficier d’une documentation claire et précise sur l’ensemble du matériel installé permettant ainsi une meilleure gestion et une maintenance efficace à long terme.

#### Principales caractéristiques de l’Axe

Le soumissionnaire doit être en mesure de soutenir les capacités des Pouvoirs locaux pour tous les services soumissionnés auquel il prendra part. Le soutien à ces services doit être fourni selon les normes les plus élevées, de manière efficace et en temps voulu. Le soumissionnaire potentiel doit également être en mesure de soutenir les Pouvoirs locaux dans la préparation et la gestion de ces services.

Le soumissionnaire doit être capable de s'intégrer dans la procédure de fourniture de services des Pouvoirs locaux et de soutenir le flux de travail de fourniture de services de Pouvoirs locaux si nécessaire.

Le soumissionnaire doit être capable de se conformer aux exigences et obligations des Pouvoirs locaux en matière de traitement et de protection de l'information, ainsi qu'en matière de responsabilité et de non-divulgation de l'information.

Le soumissionnaire doit être en mesure de fournir une équipe d'experts capables de fournir le niveau de soutien nécessaire pour le service demandé. Il est considéré comme obligatoire que les membres de l'équipe possèdent des certifications applicables au service demandé. Le soumissionnaire doit fournir les CVs des membres de l'équipe proposée en mentionnant l'expérience antérieure pertinente.

Le soumissionnaire doit également être en mesure de fournir l'équipement technique nécessaire pour assurer le soutien du ou des services demandés (y compris le matériel et les logiciels nécessaires, le cas échéant).

Le soumissionnaire doit être en mesure de satisfaire aux exigences spécifiques concernant la non-divulgation d'informations, si cela est requis dans une demande particulière.

Le contractant doit être capable de travailler ensemble (avec les conseils d’iMio et toute partie prenante jugée nécessaire) avec d'autres partenaires pertinents pour des demandes spécifiques (y compris d'autres soumissionnaires, des Pouvoirs locaux, etc.).

#### Installation

Dans le cas où le lot concerné nécessiterait une installation et configuration logicielle, celle-ci ne pourra être soumise à une facturation additionnelle. Ainsi, le soumissionnaire devra inclure dans son offre l’installation et la configuration et aucune correction en ce sens ne pourra être acceptée.

Un volet spécifique lié à l’installation devra être fourni par le soumissionnaire afin de jauger de la charge de travail ainsi que des attentes envers le Pouvoir local. Dans le cas d’une installation logicielle, le soumissionnaire devra mentionner si le serveur applicatif est hébergé au sein de l’infrastructure du Pouvoir local ou s’il sera disponible sous le format « SaaS ». Dans le cas d’un hébergement au sein du Pouvoir local, le soumissionnaire devra inclure dans son prix les spécificités matérielles nécessaires et inclure l’achat du matériel dans le prix remis lors de la remise d’offre.

#### Maintenance et Support

Les soumissionnaires fourniront dans leur devis les services de garantie, d'assistance et de maintenance de type premium.

La qualité de service de garantie/assistance et options de maintenance, y compris la mise à disposition d'un seul point de contact seront des éléments pris en compte lors de l’attribution.

Le soumissionnaire devra indiquer à iMio lors de la soumission de son offre, les différentes possibilités de prises en charge des demandes et incidents, la méthode de contact ainsi que les objectifs de résolution des incidents et requêtes.

Outre l’explication de la prise de contact et de la procédure d’introduction des incidents, un rapport mensuel ou trimestriel devra être fourni au Pouvoir local afin d’assurer le suivi des incidents.

Dans le cas où le soumissionnaire ne saurait garantir un service tel que décrit dans son offre, des pénalités pourraient s’appliquer. En ce sens, le soumissionnaire renseignera dans l’offre, la grille qu’il considère juste pour ce marché.

#### Documentation

Les soumissionnaires fourniront dans leur devis les services de garantie, d'assistance et de maintenance de type premium.

La qualité de service de garantie/assistance et options de maintenance, y compris la mise à disposition d'un seul point de contact seront des éléments pris en compte lors de l’attribution.

Le soumissionnaire devra indiquer à iMio lors de la soumission de son offre, les différentes possibilités de prises en charge des demandes et incidents, la méthode de contact ainsi que les objectifs de résolution des incidents et requêtes.

Outre l’explication de la prise de contact et de la procédure d’introduction des incidents, un rapport mensuel ou trimestriel devra être fourni au Pouvoir local afin d’assurer le suivi des incidents.

#### Canal d’acquisition

L’adjudicataire doit acquérir les équipements (matériels et logiciels) via le canal officiel et européen du fabricant/éditeur.

### Lot M1 : Produit MFA

#### Objectif du lot

Le lot "Produit MFA physique" vise à fournir des dispositifs de validation à deux facteurs pour renforcer la sécurité des accès aux systèmes d'information des Pouvoirs locaux wallons. Les objectifs de ce lot incluent :

* Fournir des dispositifs de validation à deux facteurs (MFA) pour protéger les comptes utilisateur contre les tentatives d'accès non autorisées ;
* Fournir des dispositifs MFA faciles à utiliser et à déployer pour les employés des Pouvoirs locaux ;
* Fournir des dispositifs MFA compatibles avec les systèmes d'exploitation et les applications couramment utilisés par les Pouvoirs locaux ;
* Fournir des options de personnalisation pour s'adapter aux besoins spécifiques des Pouvoirs locaux en matière de sécurité ;
* Fournir des services de support technique pour assister les Pouvoirs locaux dans le déploiement et la gestion des dispositifs MFA.

#### Caractéristiques spécifiques du lot

Les caractéristiques spécifiques attendues des produits MFA physique proposés dans le cadre de ce lot incluent :

* La compatibilité avec les protocoles d'authentification couramment utilisés tels que OAUTH, RADIUS, et SAML ;
* La prise en charge des différents types d'authentification tels que l'authentification à deux facteurs par code d'un temps, jeton physique, carte à puce, etc ;
* La possibilité de personnaliser les paramètres d'authentification en fonction des besoins spécifiques des Pouvoirs locaux ;
* La possibilité de gérer à distance les dispositifs MFA pour faciliter la gestion et l'administration ;
* La possibilité de générer des rapports sur l'utilisation et les tentatives d'accès pour faciliter la surveillance et la détection des anomalies ;
* La prise en charge des différents systèmes d'exploitation et des plates-formes couramment utilisés par les Pouvoirs locaux ;
* La possibilité de se connecter aux systèmes d'authentification en utilisant des protocoles standard tels que RADIUS et LDAP ;
* La possibilité de connecter les dispositifs MFA à des réseaux sans fil pour une utilisation mobile ;
* La possibilité de désactiver temporairement ou de réinitialiser les dispositifs MFA en cas de perte ou de vol ;
* La prise en charge de la récupération de données en cas de panne ou de défaillance du dispositif ;
* La possibilité de générer des alertes en cas de tentatives d'accès non autorisées ou d'utilisation normale ;
* La possibilité de connecter les dispositifs MFA à des systèmes de gestion des identités pour faciliter la gestion des utilisateurs et des autorisations d'accès ;
* La possibilité de mettre à niveau les dispositifs MFA pour prendre en charge les mises à jour de sécurité et les nouvelles fonctionnalités.

#### Spécifications techniques

Les spécificités techniques attendues des produits MFA physique proposés dans le cadre de ce lot incluent :

* La conformité aux normes de sécurité courantes telles que ISO 27001 ;
* La possibilité de chiffrer les données pour protéger les informations sensibles ;
* La possibilité de sécuriser les communications avec les dispositifs MFA en utilisant des protocoles de sécurité courants tels que SSL/TLS ;
* La possibilité de configurer des politiques d'accès pour limiter l'accès aux dispositifs MFA en fonction des besoins spécifiques des Pouvoirs locaux ;
* La possibilité de configurer des politiques de mots de passe pour renforcer la sécurité des dispositifs MFA ;
* La possibilité de gérer les autorisations d'accès et les utilisateurs à distance pour faciliter la gestion et l'administration ;
* La possibilité de configurer des alertes pour détecter les anomalies et les tentatives d'accès non autorisées ;
* La possibilité de prendre en charge les protocoles de sécurité courants tels que RADIUS, TOTP, HOTP pour l'authentification à deux facteurs ;
* La possibilité de prendre en charge les systèmes d'exploitation courants tels que Windows, MacOS, Linux, iOS, Android pour la compatibilité avec les systèmes d'authentification ;
* La possibilité de configurer des politiques de verrouillage automatique et de réinitialisation pour protéger les dispositifs MFA en cas de perte ou de vol ;
* La possibilité de générer des codes d'authentification à un facteur à partir d'un bouton physique sur l'appareil ;
* La possibilité de générer des codes d'authentification à un facteur à partir d'un écran tactile sur l'appareil ;
* La possibilité de stocker des clés privées sur l'appareil pour une utilisation avec des protocoles de sécurité tels que SSH et SSL/TLS ;
* La possibilité de prendre en charge des protocoles de chiffrements courants pour les données stockées sur l'appareil ;
* La possibilité de prendre en charge des protocoles de communication courants pour la communication entre l'appareil et les systèmes d'authentification tels que NFC, Bluetooth, USB ;
* La possibilité de connecter l'appareil à un ordinateur pour la configuration et la gestion ;
* La possibilité de prendre en charge des protocoles de gestion de clés courants tels que PKI pour renforcer la sécurité des communications entre l'appareil et les systèmes d'authentification.

#### Rapports et documentations

Afin de garantir que les produits MFA physique proposés répondent aux exigences de qualité requises, il est essentiel de disposer de rapports et de documentations détaillés fournis par les soumissionnaires. Ces documents permettront d'évaluer les caractéristiques techniques, les garanties et les engagements en matière de service après-vente et de support technique, les procédures de test et de validation, les mécanismes de gestion de la qualité et les protocoles de sécurité utilisés.

* Des spécifications détaillées des appareils MFA physique proposés, y compris les caractéristiques techniques, les fonctionnalités, les compatibilités et les certifications obtenues ;
* Des informations sur les garanties et les engagements en matière de service après-vente et de support technique, y compris les délais de réponse et les mécanismes de résolution de problèmes ;
* Des informations sur les procédures de test et de validation des appareils MFA physique, y compris les méthodologies utilisées, les résultats obtenus et les certifications obtenues ;
* Des informations sur les mécanismes de gestion de la qualité utilisés pour assurer la qualité des appareils MFA physique, y compris les procédures de contrôle de qualité, les audits internes, etc. ;
* Des informations sur les protocoles de sécurité utilisés pour protéger les appareils MFA physique contre les menaces potentielles, y compris les méthodologies de cryptographie, les mécanismes d'authentification, les protocoles de mise à jour de sécurité, etc. ;
* Des documents décrivant les caractéristiques techniques des produits MFA physique proposés, tels que les spécifications matérielles, les fonctionnalités, les normes de sécurité, les certifications obtenues, etc. ;
* Des informations sur les garanties et les engagements en matière de service après-vente et de support technique, y compris les procédures de résolution des problèmes, les délais de réponse, les mécanismes de suivi et de reporting, etc. ;
* Des documents décrivant les procédures de test et de validation utilisées pour garantir la qualité des produits MFA physique proposés, y compris les protocoles de test, les résultats obtenus, les éventuelles certifications obtenues, etc. ;
* Des informations sur les mécanismes de gestion de la qualité utilisés pour garantir la conformité des produits MFA physique proposés aux normes et aux réglementations en vigueur, y compris les politiques, les procédures, les protocoles de contrôle de la qualité, etc. ;
* Des informations sur les protocoles de sécurité utilisés pour garantir la confidentialité, l'intégrité et la disponibilité des données traitées par les produits MFA physique proposés, y compris les politiques de sécurité, les procédures d'authentification, les protocoles de chiffrement, etc.

#### Obligation de résultats

Dans le cadre de ce marché, il est important de demander aux soumissionnaires des engagements clairs et précis en termes de résultats pour garantir la protection des Pouvoirs locaux wallons. Les obligations de résultats seront proposées par le soumissionnaire en matière de conformité aux normes et réglementations, de sécurité des données, de délais de mise en service, de disponibilité et qualité de service après-vente, de garantie des produits, de compatibilité avec les systèmes d'information existants et de formation des utilisateurs.

Ces engagements contribueront à garantir que les produits MFA physique proposés répondent aux besoins et aux exigences des Pouvoirs locaux wallons en matière de sécurité de l'information :

* La mise en place d'un système de gestion de la qualité pour garantir la conformité des produits MFA physique proposés aux normes et aux réglementations en vigueur ;
* La mise en place de protocoles de sécurité pour garantir la confidentialité, l'intégrité et la disponibilité des données traitées par les produits MFA physique proposés ;
* Des engagements en termes de délais de mise en service et de mise à disposition des produits MFA physique ;
* Des engagements en termes de disponibilité et de qualité de service après-vente et de support technique pour les produits MFA physique proposés ;
* Des engagements en termes de garantie des produits MFA physique proposés ;
* Des engagements en termes de compatibilité avec les systèmes d'information existants des Pouvoir locaux wallons ;
* Des engagements en termes de formation des utilisateurs pour les produits MFA physique proposés ;
* Garantie de la fiabilité et de la robustesse des produits MFA physique proposés ;
* Capacité des produits à s'intégrer dans les systèmes d'authentification existants et à s'adapter aux évolutions futurs des besoins en matière de sécurité ;
* Possibilité de personnalisation des paramètres de sécurité pour répondre aux exigences spécifiques des Pouvoirs locaux wallons ;
* Engagement en termes de support technique et de maintenance des produits MFA physique proposés ;
* Engagement en termes de protection des données des utilisateurs et de confidentialité des informations transmises par les produits MFA physique ;
* Engagement en termes de respect des normes de sécurité et de conformité réglementaire.

#### Domaines d’expertise à maîtriser

Il est important de s'assurer que les soumissionnaires possèdent les compétences et l'expérience nécessaires pour fournir des appareils MFA physique de qualité supérieure et répondre aux besoins spécifiques de notre organisation. Les domaines d'expertise clés pour ce lot incluent :

* Expérience dans la conception et la fabrication d'appareils MFA physique ;
* Connaissance des protocoles d'authentification à plusieurs facteurs (MFA) tels que TOTP, HOTP, RSA SecurID, etc. ;
* Connaissance des protocoles de communication courants pour la communication entre l'appareil et les systèmes d'authentification tels que NFC, Bluetooth, USB ;
* Connaissance des protocoles de cryptage courants pour chiffrer les données stockées sur l'appareil ;
* Connaissance des protocoles de gestion de clés courants tels que PKI pour renforcer la sécurité des communications entre l'appareil et les systèmes d'authentification ;
* Connaissance des protocoles de communication courants pour la communication entre l'appareil et les systèmes d'authentification tels que RADIUS, TOTP, HOTP ;
* Expérience dans la mise en place et la gestion de solutions MFA physique pour les organisations ;
* Connaissance des normes de sécurité courantes telles que ISO 27001 et NIS 2 ;
* Connaissance des différents types d'appareils MFA physique tels que les tokens, les clés USB, les cartes à puce, les lecteurs d'empreintes digitales, les caméras d'empreintes faciales, etc. ;
* Expérience dans la personnalisation des appareils MFA physique pour répondre aux besoins spécifiques de l'organisation, tels que les exigences de branding, les paramètres de configuration, etc. ;
* Connaissance des différents systèmes d'exploitation couramment utilisés pour les appareils MFA physique, tels que Windows, iOS, Android, etc. ;
* Connaissance des exigences réglementaires et normatives liées à l'utilisation d'appareils MFA physique ;
* Connaissance des meilleures pratiques de sécurité pour la gestion et la maintenance des appareils MFA physique, tels que la gestion des mots de passe, la sauvegarde de données, la gestion des clés de chiffrement, etc ;
* Une connaissance approfondie des meilleures pratiques de sécurité, telles que l'identification et la gestion des vulnérabilités, la protection contre les attaques brute force, la sécurisation des communications, etc.
* Une capacité à mettre en place des mesures de sécurité robustes afin de protéger les dispositifs MFA physiques contre les attaques physiques et logiques, ainsi que pour garantir la confidentialité, l'intégrité et la disponibilité des données traitées.
* Une expertise dans le protocole d’authentification couramment utilisé tel que SAML, Radius, OAUTH. La mise en œuvre de ces protocoles doit se faire de manière sécurisée en utilisant des mécanismes d’échange de clés, de chiffrement et d’authentification forte.

#### Scénario pour compléter l’inventaire

Scénario pour le lot "Produit MFA physique" - Taille administration : 80 utilisateurs/agents :

Volumétrie et quantités nécessaires :

* 80 dispositifs de validation à deux facteurs (MFA) physiques.
* 80 kits de déploiement comprenant les accessoires et les guides d'installation.

Implémentation pratique :

* Chaque utilisateur/agent du pouvoir local recevra un dispositif MFA physique personnel.
* Les dispositifs MFA seront préconfigurés avec les paramètres d'authentification nécessaires et les politiques de sécurité définies par le pouvoir local.
* Un processus de déploiement sera mis en place pour distribuer les dispositifs MFA aux utilisateurs/agents.
* Les utilisateurs/agents seront formés sur l'utilisation des dispositifs MFA et les bonnes pratiques en matière de sécurité.

### Lot M2 : Pare-feu

#### Objectif du lot

Le lot concernant les pares-feux vise à protéger les Pouvoirs locaux de Wallonie contre les risques de sécurité informatique en mettant en place des pares-feux adaptés aux environnements Windows et Linux utilisés par ces derniers. Ces pares-feux permettront de garantir la confidentialité, l'intégrité et la disponibilité des données et des systèmes informatiques des Pouvoirs locaux de Wallonie dans ces environnements. Ils assureront également la conformité aux réglementations et aux normes en matière de sécurité informatique applicables aux Pouvoirs locaux de Wallonie dans ces environnements. Enfin, ils contribueront à améliorer la performance des systèmes informatiques des Pouvoirs locaux de Wallonie en limitant les tentatives de piratage et les attaques informatiques grâce à leur utilisation dans ces environnements.

Le soumissionnaire doit fournir un équipement qui répond aux exigences minimales énoncées ci-dessous. Si le soumissionnaire ne satisfait pas à ces exigences minimales, sa soumission sera automatiquement disqualifiée. Il est important que le soumissionnaire décrive de manière détaillée et précise comment son équipement répond à chaque exigence. Une simple déclaration affirmant que l'équipement répond aux exigences ou une réitération des exigences de ce marché ne suffira pas à cet égard. Il est crucial que le soumissionnaire fournisse des preuves concrètes de la façon dont son équipement répond aux exigences minimales requises. En outre, si le soumissionnaire propose des solutions alternatives pour remplir les exigences minimales, il doit clairement expliquer comment ces solutions répondent aux besoins énoncés et comment elles sont supérieures aux solutions standards.

#### Caractéristiques spécifiques du lot

Pour garantir la qualité et l'efficacité des pares-feux proposés pour les Pouvoirs locaux wallons, nous demandons aux soumissionnaires de s'engager sur les caractéristiques spécifiques du lot suivantes :

Caractéristiques spécifiques du lot :

* Capacité de traitement élevée : le pare-feu doit être capable de gérer un nombre élevé de sessions simultanées et de transactions, en utilisant des technologies d'optimisation de ressources et de traitement parallèle ;
* Technologie de détection de menace avancée : le pare-feu doit être équipé de technologies avancées de détection de menace, comme l'analyse de comportement et l'apprentissage automatique, afin de pouvoir détecter et bloquer efficacement les tentatives d'intrusion et de cyber-attaque ;
* Fonctionnalités de contrôle d'accès granulaires : le pare-feu doit proposer des fonctionnalités de contrôle d'accès granulaires et flexibles, qui permettent de définir des politiques de sécurité précises en fonction des utilisateurs, des groupes, des applications et des protocoles ;
* Prise en charge de différents protocoles de chiffrement et de VPN : le pare-feu doit être capable de prendre en charge différents protocoles de chiffrement et de VPN ;
* Technologie de gestion de bande passante et de QoS : le pare-feu doit être équipé de technologies avancées de gestion de bande passante et de QoS, afin de pouvoir répartir de manière équitable les ressources de réseau entre différents types de trafic et de garantir des performances optimales pour les applications critiques ;
* Prise en charge de différents protocoles de routage : le pare-feu doit être capable de prendre en charge différents protocoles de routage dynamique, comme RIP v2, OSPF, BGP, afin de pouvoir s'intégrer efficacement dans des environnements de réseau complexes et hétérogènes ;
* Outils de gestion et de surveillance avancés : le pare-feu doit proposer des outils de gestion et de surveillance avancés, qui permettent aux administrateurs de surveiller en temps réel l'état et les performances du produit, de diagnostiquer les problèmes et de les résoudre rapidement ;
* Interopérabilité et compatibilité avec d'autres équipements et solutions de sécurité : le pare-feu doit être capable de fonctionner de manière transparente et interopérable avec d'autres équipements et solutions de sécurité, et doit être compatible avec les différents systèmes d'exploitation et environnements de déploiement prévus ;
* Programme d'assistance et d'accompagnement complet : le soumissionnaire doit proposer un programme d'assistance et d'accompagnement complet, qui comprend des services de mise en service, de formation, de maintenance, de support technique et de déploiement. Ces services doivent être adaptés aux besoins et aux contraintes des Pouvoirs locaux wallons, et doivent être fournis par des équipes de professionnels expérimentés et qualifiés ;
* Mises à jour et évolutions logicielles régulières : le soumissionnaire doit s'engager à fournir des mises à jour et évolutions logicielles régulières pour le pare-feu proposé, afin de maintenir la qualité et la performance de l'équipement, et de garantir la conformité aux normes et réglementations en vigueur ;
* Garantie et protection de la confidentialité des données : le soumissionnaire doit s'engager à respecter les exigences de garantie et de protection de la confidentialité des données des Pouvoirs locaux wallons, en mettant en place les mesures de sécurité et de protection adéquates pour protéger les données sensibles transitant sur le réseau ;
* Politique de retour et de remplacement : le soumissionnaire doit prévoir une politique de retour et de remplacement qui garantit la disponibilité et la qualité des équipements proposés, en cas de défaillance ou de défaillance prématurée.

#### Spécifications techniques

##### Pare-feu virtuel

Pour assurer la sécurité de l'environnement en ligne des Pouvoirs locaux de Wallonie, le soumissionnaire doit fournir un pare-feu, potentiellement en grappe, capable de prendre en charge les configurations active/active et active/passive. Le pare-feu doit également disposer de la technologie d'inspection des politiques "Stateful" et d'une intelligence applicative pour les protocoles TCP/IP couramment utilisés tels que Telnet, FTP, etc.

Il est important de noter que le pare-feu doit être doté d'une licence sans restriction de dispositifs ni de connexions. Cela signifie que le nombre de dispositifs ou de connexions protégées par le pare-feu ne doit pas être limité par la licence. Le soumissionnaire doit donc fournir une solution qui permette aux Pouvoirs locaux de Wallonie de protéger l'ensemble de leur environnement en ligne sans limitation de dispositifs ni de connexions.

Pour assurer une performance optimale, le soumissionnaire doit fournir un pare-feu doté de certaines caractéristiques en matière de matériel et d'interface :

* Le pare-feu doit avoir une interface Ethernet pour la gestion hors bande du dispositif ;
* Le pare-feu doit prendre en charge IPv4 et IPv6 ;
* Technologies d'optimisation des ressources, comme l'utilisation de plusieurs cœurs de processeur à un moment donné ;
* Le pare-feu doit équilibrer les décisions de sécurité entre plusieurs cœurs à un moment donné ;
* Doit décharger l'inspection de sécurité vers un module logiciel optimisé en termes de performances ;
* Paires de commutateurs DMS dédiés par interface physique ;
* Montage en rack 19" avec rails standard inclus ;
* Le balisage VLAN doit être pris en charge sur les interfaces pare-feu ;
* Support intégré pour les VPN IPSEC avec support 3DES et AES256 ;
* Prise en charge de > 15 pares-feux virtuels ;
* Haute disponibilité active/active ;
* Détection de la défaillance d'un dispositif, d'un lien et d'un chemin, avec état ;
* Les modules de pare-feu doivent prendre en charge le déploiement en mode routé et en mode transparent ;
* Le pare-feu doit fournir un support de moteur d'état pour tous les protocoles courants de la pile TCP/IP ;
* Prise en charge des protocoles Le pare-feu doit fournir une fonctionnalité NAT, y compris les traductions NAT dynamiques et statiques ;
* Doit permettre l'application de règles de sécurité dans des intervalles de temps à configurer avec une date/heure d'expiration ;
* Le pare-feu doit prendre en charge les méthodes d'authentification des utilisateurs, des clients et des sessions ;
* Le pare-feu doit prendre en charge les protocoles d'authentification RADIUS, LDAP, TACACS et les méthodes PKI ;
* Le pare-feu doit prendre en charge l'authentification ICP avec les normes PCKS#7 et PCKS#10 ;
* Le pare-feu doit prendre en charge la répartition de la charge avec synchronisation de l'état.

##### Pare-feu de l’environnement de back-office

Le soumissionnaire doit fournir des pare-feu qui supportent une configuration active/active et active/passive. Cela garantira une haute disponibilité et une redondance des fonctionnalités de sécurité offertes par les pare-feu. Le pare-feu doit également prendre en charge la technologie d'inspection des politiques "Stateful" et disposer d'une intelligence applicative pour les protocoles TCP/IP couramment utilisés tels que Telnet, FTP, etc.

En outre, le pare-feu doit prendre en charge les protocoles de routage dynamique tels que RIP v2, OSPF et BGP. Cela permettra de gérer efficacement le trafic réseau et d'optimiser les performances du réseau.

Il est important de noter que le pare-feu doit être doté d'une licence sans restriction de dispositifs ni de connexions. Cela signifie que le nombre de dispositifs ou de connexions protégées par le pare-feu ne doit pas être limité par la licence. Le soumissionnaire doit donc fournir une solution qui permette aux Pouvoirs locaux de Wallonie de protéger l'ensemble de leur réseau sans limitation de dispositifs ni de connexions.

Pour assurer une performance optimale, le soumissionnaire doit fournir un pare-feu doté de certaines caractéristiques en matière de matériel et d'interface :

* Le pare-feu doit avoir une interface Ethernet ;
* Les technologies d'optimisation des ressources, comme l'utilisation de plusieurs cœurs d'unité centrale à un moment donné ;
* Le pare-feu doit équilibrer les décisions de sécurité entre plusieurs cœurs à un moment donné ;
* Doit décharger l'inspection de sécurité vers un module logiciel optimisé en termes de performances ;
* Paires de commutateurs DMS dédiés par interface physique ;
* Le balisage VLAN doit être pris en charge sur les interfaces du pare-feu ;
* Support intégré pour les VPN IPSEC avec support 3DES et AES256 ;
* Les modules de pare-feu doivent permettre le déploiement en mode routé et en mode transparent ;
* Le pare-feu doit fournir un support de moteur d'état pour tous les protocoles courants de la pile TCP/IP ;
* Le pare-feu doit prendre en charge tous les protocoles courants de la pile TCP/IP ; Le pare-feu doit fournir une fonctionnalité NAT, y compris les traductions NAT dynamiques et statiques ;
* Doit permettre l'application de règles de sécurité dans des intervalles de temps à configurer avec une date/heure d'expiration ;
* Le pare-feu doit prendre en charge les méthodes d'authentification des utilisateurs, des clients et des sessions ;
* Le pare-feu doit prendre en charge les protocoles d'authentification RADIUS, LDAP, TACACS et les méthodes PKI ;
* Le pare-feu doit prendre en charge l'authentification ICP avec les normes PCKS#7 et PCKS#10 ;
* Le pare-feu doit prendre en charge la répartition de la charge avec synchronisation de l'état ;
* Support pour > 15 pares-feux virtuels ;
* Haute disponibilité active/active ;
* Détection de la défaillance d'un dispositif, d'un lien et d'un chemin, avec état ;
* Sandbox.

##### Administration

Les exigences techniques pour l'administration, la gestion et la journalisation sont les suivantes :

* Gestion centrale des clusters de pare-feu, y compris l'installation de la base de règles, la gestion des changements et la journalisation ;
* Connexions chiffrées et authentifiées utilisées pour toutes les communications de gestion et de passerelle, y compris la collecte des journaux ;
* Génération automatique de vues HTML de la base de règles qui peuvent être stockées en externe et utilisées pour la révision des changements, l'archivage et l'accès simplifié à des fins de révision ;
* Analyse automatisée des politiques de pare-feu mettant en évidence les problèmes de sécurité potentiels, les écarts par rapport aux meilleures pratiques et les règles et éléments de politique obsolètes/testés ;
* Analyse automatisée des journaux, y compris le suivi des occurrences de règles et l'affichage par rapport à la base de règles ;
* Prise en charge de la collecte et du signalement des événements syslog génériques, y compris les formats prédéfinis standard ;
* Prise en charge des tickets d'événement et des alertes ;
* Prise en charge de la collecte et du signalement d'événements syslog génériques, y compris les formats prédéfinis standard ;
* Des vues graphiques complètes des événements, y compris des rapports géographiques ;
* Surveillance et suivi des paramètres clés du système et des services, représentés graphiquement sur 18 mois pour l'analyse des tendances.

Une garantie minimale de 3 ans sur les équipements.

##### Spécifications liées à la taille du Pouvoir local

Pour répondre au marché, le soumissionnaire doit décrire de manière détaillée et précise comment son produit proposé répond à chaque spécification énoncée dans le tableau. Il est important de noter que l'équipement proposé doit répondre aux exigences minimales des spécifications techniques. Si le soumissionnaire ne satisfait pas à ces exigences minimales, sa soumission sera automatiquement disqualifiée. Il est donc crucial que le soumissionnaire fournisse des preuves concrètes de la façon dont son produit répond aux exigences minimales requises.

Une simple déclaration affirmant que le produit répond aux exigences ou une réitération des exigences du marché ne suffira pas à cet égard. Le soumissionnaire doit fournir une description détaillée et étayée de la façon dont son produit répond aux spécifications énoncées dans le tableau. Si le soumissionnaire propose des solutions alternatives pour remplir les exigences minimales, il doit clairement expliquer comment ces solutions répondent aux besoins énoncés et comment elles sont supérieures aux solutions standards. Il est important que le soumissionnaire fournisse une description complète et convaincante de la façon dont son produit répond aux exigences minimales requises, afin que les Pouvoirs locaux de Wallonie puissent évaluer pleinement les mérites de sa soumission.

#### Rapports et documentations

Pour assurer la qualité et la fiabilité des pare-feu proposés pour les Pouvoirs locaux wallons, il est important de disposer de documentation et de rapports détaillés sur les caractéristiques et les performances du produit. Les soumissionnaires doivent fournir les éléments suivants :

* Documentation technique du pare-feu proposé, y compris les fonctionnalités, les caractéristiques et les spécifications du produit ;
* Manuel d'utilisation du pare-feu, comprenant les instructions détaillées sur la configuration et la gestion du produit ;
* Rapport d'évaluation des performances du pare-feu, mettant en avant les résultats de tests de charge et de performance réalisés par le soumissionnaire ;
* Liste des certifications et conformités obtenues par le pare-feu, y compris les certifications de sécurité et les normes de qualité ;
* Document de support technique, décrivant les modalités de support proposées par le soumissionnaire, y compris les canaux de support disponibles et les délais de réponse garantis ;
* Rapports de sécurité et de conformité, décrivant les mesures de sécurité mises en place par le soumissionnaire pour protéger les données et les systèmes de ses clients ;
* Documentation sur les mises à jour et les correctifs de sécurité publiés pour le pare-feu, y compris les dates de sortie et les notes de version ;
* Rapport de compatibilité du pare-feu avec d'autres équipements réseau et logiciels, tels que les commutateurs et les routeurs, les systèmes d'exploitation et les logiciels de gestion de réseau ;
* Liste des intégrations et des API disponibles pour le pare-feu, y compris les informations sur les partenaires et les solutions tiers prises en charge ;
* Guides de déploiement et de configuration, fournissant des instructions détaillées sur la manière de mettre en place et de configurer le pare-feu dans différents environnements de déploiement ;
* Documentation sur les options de support avancées proposées par le soumissionnaire, telles que le support de niveau 3 et les services de dépannage à distance ;
* Rapports sur les cas d'utilisation réussis et les retours d'expérience de clients existants utilisant le pare-feu proposé.

#### Obligation de résultats

Pour garantir la qualité et la fiabilité des pares-feux proposés pour les Pouvoirs locaux wallons, nous demandons aux soumissionnaires de s'engager sur les obligations de résultats suivantes :

* Disponibilité du pare-feu : le soumissionnaire doit garantir un taux de disponibilité élevé et durable du pare-feu, en utilisant des technologies de haute disponibilité et de redondance comme le clustering actif/actif et actif/passif ;
* Performances du pare-feu : le soumissionnaire doit fournir des garanties de performance et de débit pour le pare-feu, en prenant en compte les différents usages et charges de travail prévus ;
* Sécurité du pare-feu : le soumissionnaire doit garantir la sécurité du pare-feu et de ses fonctionnalités, en mettant en œuvre des mesures de sécurité avancées comme l'inspection de contenu et l'analyse de comportement ;
* Support technique : le soumissionnaire doit fournir un support technique de qualité aux utilisateurs du pare-feu, en utilisant des canaux de support adaptés et en garantissant des délais de réponse rapides ;
* Mises à jour et correctifs : le soumissionnaire doit fournir régulièrement des mises à jour et des correctifs de sécurité pour le pare-feu, afin de maintenir les performances et la sécurité du produit à jour ;
* Formation et documentation : le soumissionnaire doit proposer des programmes de formation et de documentation pour les utilisateurs du pare-feu, afin de leur permettre de mieux comprendre et d'utiliser le produit ;
* Intégration avec d'autres équipements et solutions : le soumissionnaire doit être capable de démontrer comment son pare-feu peut être intégré et utilisé en conjonction avec d'autres équipements et solutions de sécurité, tels que les systèmes de détection d'intrusion, les logiciels de gestion de réseau, etc. ;
* Gestion et surveillance : le soumissionnaire doit fournir des outils et des fonctionnalités de gestion et de surveillance avancées pour le pare-feu, afin de permettre aux administrateurs de surveiller en temps réel l'état et les performances du produit ;
* Flexibilité et évolutivité : le soumissionnaire doit démontrer comment son pare-feu peut être configuré et adapté à différents environnements de déploiement et à des charges de travail variables, et comment il peut être facilement évolué pour prendre en charge de nouvelles fonctionnalités et de nouvelles exigences de sécurité ;
* Assistance et accompagnement : le soumissionnaire doit proposer des programmes d'assistance et d'accompagnement pour les utilisateurs du pare-feu, afin de les aider à tirer le meilleur parti du produit et à résoudre rapidement les problèmes rencontrés ;
* Engagement de service : le soumissionnaire doit s'engager sur des niveaux de service et de support précis et mesurables pour le pare-feu, afin de garantir une qualité de service constante aux utilisateurs.

#### Domaines d’expertise à maîtriser

Pour assurer la sécurité et la fiabilité du réseau des Pouvoirs locaux wallons, il est crucial de s'assurer que les pares-feux proposés répondent aux exigences les plus élevées en matière de technologie et de performance. Pour cette raison, nous souhaitons que les soumissionnaires mettent en avant leur expertise dans les domaines suivants :

* Connaissance approfondie des technologies de sécurité réseau, notamment des protocoles de sécurité et des technologies de chiffrement ;
* Maîtrise des différents protocoles de routage et de commutation utilisés dans les réseaux locaux et étendus ;
* Connaissance des normes et réglementations en matière de sécurité des réseaux, notamment celles applicables aux Pouvoirs locaux wallons ;
* Expérience de la mise en œuvre et de la gestion de pare-feu dans des environnements de petite et moyenne taille ;
* Capacité à fournir un support technique de qualité et à répondre rapidement aux demandes d’assistance des utilisateurs ;
* Connaissance des outils et des processus de gestion de la sécurité, tels que la gestion des mises à jour de logiciels et de la documentation, la gestion des événements de sécurité et la gestion des alertes de sécurité ;
* Capacité à fournir une évaluation de l'infrastructure réseau existante et à proposer des solutions de mise à niveau ou de mise à jour pour améliorer la sécurité et la performance ;
* Compétences en matière de déploiement et de configuration de pare-feu en grappe, en particulier en mode active/active et active/passive ;
* Connaissance des meilleures pratiques de gestion de la sécurité et de la performance des pares-feux, y compris les processus de monitoring et de rapport ;
* Expérience de la mise en œuvre de règles de sécurité avancées, telles que l'inspection de contenu et l'analyse de comportement ;
* Capacité à fournir une formation et un support technique aux utilisateurs du pare-feu, y compris la mise en place de documents de référence et de guides d'utilisation ;
* Connaissance des technologies de virtualisation et de la manière de déployer et de gérer des pare-feu virtuels dans un environnement de cloud computing.

#### Scénario pour compléter l’inventaire

Scénario pour le lot "Pare-feu" - Débit maximal jusqu'à 1 Gbps :

* Spécifications techniques requises :
* Débit minimal : Jusqu'à 1 Gbps
* Ports LAN : 4 ports Ethernet 1 Gbps
* Ports WAN : 1 port Ethernet 1 Gbps
* Protocoles de sécurité supportés : IPsec, SSL/TLS
* Fonctionnalités de filtrage : Filtrage par adresse IP, port, protocole, URL, application
* Fonctionnalités de VPN : Prise en charge des tunnels VPN IPsec et SSL, jusqu'à 500 tunnels VPN simultanés
* Prise en charge de la haute disponibilité : Non applicable (utilisation en mode autonome)
* Capacité de gestion des utilisateurs distants : Jusqu'à 100 utilisateurs
* Support technique inclus avec mise à jour logicielle pendant la durée de vie du produit.

Implémentation pratique :

* Le pare-feu sera installé au niveau du réseau local du pouvoir local, assurant la sécurité des flux entrants et sortants.
* Les 4 ports Ethernet 1 Gbps seront utilisés pour connecter les différents segments du réseau local.
* Le port Ethernet 1 Gbps connectera le pare-feu au réseau WAN pour permettre l'accès à Internet.
* Les protocoles de sécurité IPsec et SSL/TLS seront activés pour assurer des communications sécurisées.
* Les fonctionnalités de filtrage seront configurées en fonction des politiques de sécurité définies par le pouvoir local, permettant un contrôle granulaire sur les flux réseau.
* Les tunnels VPN IPsec et SSL seront configurés pour permettre aux utilisateurs distants d'accéder au réseau interne de manière sécurisée.
* Le référent informatique du pouvoir local sera formé sur l'utilisation basique du pare-feu afin d’être indépendant pour le support de bas niveau.
* Le support technique et les mises à jour logicielles seront assurés pendant toute la durée de vie du produit, garantissant un fonctionnement optimal et une protection continue contre les menaces émergentes.

### Lot M3 : Sauvegardes sécurisées de données

#### Objectif du lot

L'objectif est de fournir une solution flexible et fiable pour assurer la protection et la restauration des données des Pouvoirs locaux.

La sauvegarde sécurisée, ou autrement appelé le backup, des données est un domaine de plus en plus complexe et important pour les Pouvoirs locaux et les organisations qui opèrent à l'échelle locale car leurs données sont devenues de plus en plus vitales. Le backup des données est essentiel pour assurer la sécurité et la disponibilité des données à tout moment, qu'il s'agisse d'une panne matérielle ou d'une attaque informatique. De plus, le backup permet de préserver la confidentialité des données et de garantir leur intégrité. Il est donc primordial que les pouvoirs locaux disposent des solutions de backup adéquates pour s'assurer que leurs données sont à l'abri des risques et des menaces. Ce lot présentera les technologies et les solutions les plus avancées pour assurer la sécurité, la disponibilité et l'intégrité des données essentielles aux Pouvoirs locaux.

#### Caractéristiques spécifiques du lot

Le système de sauvegarde sécurisée des données doit être capable de sauvegarder et de restaurer les données à partir de différentes sources telles que les serveurs, les postes de travail, les applications, les systèmes de fichiers et les bases de données. Il doit également être capable de sauvegarder les données sur des supports de stockage externes tels que des bandes ou des disques durs. Le système de sauvegarde des données doit être capable de gérer les sauvegardes à des fréquences définies par l'entreprise. Il doit également être capable de gérer la rotation des supports de sauvegarde et de surveiller le bon fonctionnement du système.

Le système de sauvegarde des données doit prendre en charge les principaux systèmes d'exploitation et les principales applications. Il doit également prendre en charge les principaux formats de données et de fichiers. Le système de sauvegarde des données doit être capable de générer des rapports de sauvegarde et de restauration et de fournir des outils d'administration pour gérer le système. Il doit également être capable de fournir une interface utilisateur conviviale. Le système de sauvegarde des données doit être capable de se connecter à des systèmes de stockage distants pour offrir une solution de sauvegarde et de restauration à distance. Le système de sauvegarde des données doit être capable de se connecter à des systèmes de sauvegarde et de restauration en ligne et de gérer la sauvegarde et la restauration des données en ligne. Il est important que le système soit simple à utiliser et à administrer et qu'il offre une fiabilité et une sécurité maximales.

Les prestations liées à ce lot doivent se décomposer en 3 phases :

1. Analyse de la situation du Pouvoir local et définition de la stratégie de sauvegarde sécurisée des données ;
2. Mise en place de la solution adéquate en fonction de l’analyse préalable et de la stratégie définie ;

Entretien et amélioration de la solution mise en place.

#### Spécifications techniques

Pour gérer de manière sécurisée la sauvegarde de leurs données, les pouvoirs locaux belges locaux wallons souhaitent mettre en place une solution conforme aux réglementations et aux normes de sécurité en vigueur en Belgique. Le soumissionnaire doit suivre les spécificités techniques suivantes :

* Proposer une solution de sauvegarde multi-niveaux pour garantir la sauvegarde des données sur différents supports et à différents emplacements ;
* Proposer un chiffrement fort des données pour protéger les données sauvegardées contre les accès non autorisés ;
* Proposer une solution de sauvegarde automatisée pour garantir que les données sont sauvegardées régulièrement et de manière fiable ;
* Proposer une solution de sauvegarde à distance pour protéger les données contre les risques locaux, tels que les incendies ou les inondations ;
* Proposer une solution de sauvegarde de haute disponibilité pour assurer la disponibilité des données en cas de besoin ;
* Proposer une solution de sauvegarde de haute performance pour garantir la rapidité de la sauvegarde et de la restauration des données ;
* Proposer une solution de sauvegarde évolutive pour évoluer avec les besoins grandissants des données des Pouvoirs locaux ;
* Proposer un système de journalisation pour suivre les actions de sauvegarde et de restauration ;
* Définir des stratégies de sauvegarde et de restauration pour toutes les données vitales ;
* Proposer des outils et des logiciels de sauvegarde et de restauration adaptés à l'environnement et à la taille des données ;
* Proposer des solutions de sauvegarde et de restauration fiables et testées en amont ;
* Définir des règles de sauvegarde et de restauration pour chaque type de données ;
* Proposer des solutions de sauvegarde et de restauration redondantes pour assurer la sécurité des données ;
* Proposer des solutions de sauvegarde et de restauration automatiques pour assurer la sécurité et la redondance des données ;
* Planifier des tests de sauvegarde et de restauration réguliers pour vérifier l'intégrité des données.

#### Rapports et documentations

Pour garantir une mise en œuvre efficace et conforme aux exigences de la réglementation, nous attendons des soumissionnaires les éléments suivants :

* Une politique de sauvegarde sécurisée documentée, et mise à jour le cas échéant, basée sur les bonnes pratiques de l’industrie (par exemple : la 3-2-1-0) et établie en bonne intelligence avec le Pouvoir local selon ses spécificités ;
* Des rapports sur la mise en œuvre et la configuration du produit de sauvegarde des données sécurisé ;
* Des documents décrivant les processus de gestion des alertes et des notifications générées par la solution ;
* Des rapports de performance et de disponibilité de la solution ;
* Des documents décrivant les procédures de sauvegarde et de restauration des données ;
* Des documents décrivant les procédures de maintenance préventive et corrective de la solution ;
* Des manuels d'utilisation et de formation destinés aux utilisateurs finaux du produit ;
* Documentation technique décrivant les fonctionnalités et les caractéristiques de la solution proposée ;
* Rapports de test et de validation de la solution proposée, y compris des résultats de tests de performance et de charge ;
* Preuves de conformité aux réglementations et normes industrielles pertinentes ;
* Guides de mise en œuvre et de maintenance de la solution, y compris des procédures de déploiement et de mise à jour ;

Garanties et assurances de qualité de la solution et du support proposé par le soumissionnaire.

#### Obligation de résultats

La sauvegarde sécurisée des données est un élément clé de la sécurité informatique, qui permet d’assurer la sécurité et la disponibilité des données à tout moment, qu'il s'agisse d'une panne matérielle ou d'une attaque informatique. De plus, le backup permet de préserver la confidentialité des données et de garantir leur intégrité. Il est donc important de s'assurer que les soumissionnaires pour ce lot seront en mesure de fournir des solutions de qualité, fiables et efficaces pour la sauvegarde sécurisée des données. Pour cela, voici quelques obligations de résultats que les soumissionnaires pourraient être tenus de respecter :

* Capacité à sauvegarder et restaurer de manière sécurisée les données provenant de différents équipements et sources ;
* Capacité à analyser et à visualiser les rapports de sauvegarde ou de restauration de manière à faciliter la détection et la résolution d’anomalies ou d’incident ;
* Fonctionnalités de rapport et de notification pour informer les responsables de sécurité en cas de problème ou de comportement suspect ;
* Mise à disposition de guides et de documentation pour aider les utilisateurs à configurer et à utiliser les solutions de sauvegarde sécurisée des données de manière optimale ;
* Garantie de disponibilité et de performance des solutions de sauvegarde sécurisée des données, avec un temps de réponse rapide en cas de problème ou de besoin de support ;
* Fournir un système de connexion à un système externe de journalisation qui permettra de suivre et d'analyser les évènements de sécurité de manière centralisée ;
* S'assurer que la solution de sauvegarde sécurisée des données est conforme aux réglementations et aux normes de sécurité en vigueur ;
* Fournir un support technique pour l'installation, la configuration et l'intégration de la solution de sauvegarde sécurisée des données dans l'infrastructure existante des Pouvoirs locaux ;
* Fournir une documentation détaillée sur l'utilisation et la maintenance de la solution de sauvegarde sécurisée des données ;

Fournir des mises à jour régulières de la solution de sauvegarde sécurisée des données pour garantir sa compatibilité avec les évolutions technologiques et les nouvelles réglementations de sécurité.

#### Domaines d’expertise à maîtriser

Pour assurer la mise en œuvre réussie et sécurisée de projets liés à une solution de sauvegarde sécurisée des données pour les pouvoirs locaux wallons, nous recherchons des soumissionnaires possédant une solide expertise dans les domaines suivants :

* Connaissance des réglementations et des normes en matière de sauvegarde et restauration des données en Belgique ;
* Expérience dans la mise en place et le déploiement en matière de sauvegarde et restauration des données ;
* Compétences en matière de sécurité de l'information et de gestion des risques liés à la sauvegarde et restauration des données ;
* Connaissance des normes et des réglementations en matière de sauvegarde et de protection des données (par exemple, RGPD) ;
* Compétences en matière de planification et de mise en place de stratégies de sauvegarde ;
* Connaissance des différents types de sauvegarde (par exemple, incrémentielle, différentielle, complète) et des technologies associées (par exemple, sauvegarde sur bande, sauvegarde sur disque, sauvegarde dans le cloud) ;
* Compétences en matière de sécurité des systèmes pour protéger les données sauvegardées contre les attaques externes et internes ;
* Compétences en matière de surveillance et de gestion des performances des systèmes de sauvegarde pour assurer la disponibilité des données en cas de besoin ;
* Connaissance des outils de sauvegarde et de restauration pour gérer les processus de sauvegarde et de restauration des données ;
* Connaissance de la récupération des données pour pouvoir récupérer les données en cas de besoin. ;
* Connaissance des politiques de RTO et RPO pour garantir la restauration des données en temps voulu et dans les limites de tolérance de perte de données ;
* Compétences en matière de formation et de support technique pour les utilisateurs finaux, afin de garantir que la sauvegarde et la restauration des données sont utilisées de manière efficace et sécurisée ;
* Connaissance des tendances et des innovations dans le domaine de la sauvegarde et la restauration des données, afin de pouvoir conseiller et orienter les Pouvoirs locaux sur les meilleures pratiques et les technologies les plus récentes.

#### Scénario pour compléter l’inventaire

Scénario pour le lot "Sauvegardes sécurisées de données" - Capacité de stockage de 15 To :

Spécifications techniques requises

Fourniture et mise en place de :

* Équipement d'une capacité totale de stockage de 15 To (pour prévoir la croissance future des données) :
  + 12 disques durs de 2 To chacun pour une capacité de stockage totale de 24 To (permettant la mise en place de la redondance et du RAID pour une meilleure protection des données).
  + Licence pour le logiciel afin de couvrir l’ensemble des fonctionnalités demandées
* Prestations nécessaires à la mise en œuvre des fonctionnalités exprimées.

Implémentation pratique :

* L'équipement de sauvegarde sera installé au sein de l'infrastructure du pouvoir local, assurant la protection et la sauvegarde des données critiques.
* Les 12 disques durs de 2 To seront configurés en tant que dispositifs de stockage redondants, permettant la mise en place du RAID pour une meilleure résilience en cas de défaillance d'un disque.
* La capacité totale de stockage de 15 To permettra de répondre aux besoins actuels et de prévoir la croissance future des données.
* La licence du logiciel de sauvegarde sera activée, permettant d'accéder à l'ensemble des fonctionnalités nécessaires pour la sauvegarde sécurisée des données.
* Le référent informatique du pouvoir local sera formé sur l'utilisation logiciel du système de sauvegarde afin d’être indépendant pour le support de bas niveau.
* Les prestations nécessaires, telles que l'installation, la configuration et la mise en œuvre des fonctionnalités demandées, seront réalisées par le fournisseur.
* Les sauvegardes seront planifiées et effectuées régulièrement, assurant la disponibilité des données en cas de perte ou de corruption.

## Axe Logiciel

L'axe "logiciel" vise à fournir des logiciels de sécurité de qualité supérieure pour protéger les systèmes et les données des Pouvoirs locaux contre les menaces de la cybersécurité. Ces logiciels permettront également aux Pouvoirs locaux de gérer efficacement leurs programmes de cybersécurité et de maintenir la conformité avec les exigences réglementaires en matière de sécurité des données.

**Objectifs**

L'objectif de l'axe logiciel de ce marché est de fournir des solutions logicielles robustes et adaptées aux besoins de sécurité des Pouvoirs locaux wallons. Ces solutions doivent être en mesure de protéger les données et les systèmes de ces institutions contre les menaces informatiques, telles que les virus, les ransomwares, les attaques de phishing et autres formes de cyber intrusion, cela inclus les éléments suivants :

* Augmenter les capacités des Pouvoirs locaux en matière de cybersécurité en leur fournissant des outils de gestion de parc de licences, de gestion de sécurité des terminaux et de gestion de la sécurité des données.
* Aider les Pouvoirs locaux à maintenir et à mettre à jour leurs logiciels de cybersécurité afin de garantir leur efficacité contre les menaces en constante évolution.
* Offrir aux Pouvoirs locaux une assistance technique pour l'installation, la configuration et l'utilisation de leurs logiciels de cybersécurité.
* Ces solutions logicielles devront être facilement gérables et maintenables afin de permettre aux équipes informatiques des Pouvoirs locaux de les utiliser efficacement et de les mettre à jour rapidement en cas de besoin. Elles devront également être adaptées aux différentes architectures de réseau et aux environnements de travail existants des Pouvoirs locaux, afin de garantir une intégration facile et une utilisation fluide.



* Ces solutions logicielles devront être accompagnées de formations et de supports de qualité pour aider les utilisateurs à les utiliser de manière optimale et à en tirer le meilleur parti. Elles devront également être conformes aux réglementations et aux standards de sécurité en vigueur, afin de garantir la sécurité des données et des systèmes des Pouvoirs locaux.

**Principales caractéristiques de l’Axe**

Le soumissionnaire doit être en mesure de soutenir les capacités des Pouvoirs locaux pour tous les services soumissionnés auquel il prendra part. Le soutien à ces services doit être fourni selon les normes les plus élevées, de manière efficace et en temps voulu. Le soumissionnaire doit également être en mesure de soutenir les Pouvoirs locaux dans la préparation et la gestion de ces services.

Le soumissionnaire doit être capable de s'intégrer dans la procédure de fourniture de services des Pouvoirs locaux et de soutenir le flux de travail de fourniture de services de Pouvoirs locaux si nécessaire.

Le soumissionnaire doit être capable de se conformer aux exigences et obligations des Pouvoirs locaux en matière de traitement et de protection de l'information, ainsi qu'en matière de responsabilité et de non-divulgation de l'information.

Le soumissionnaire doit être en mesure de fournir une équipe d'experts capables de fournir le niveau de soutien nécessaire pour le service demandé. Il est considéré comme obligatoire que les membres de l'équipe possèdent des certifications applicables au service demandé. Le soumissionnaire doit fournir les CVs des membres de l'équipe proposée en mentionnant l'expérience antérieure pertinente.

Le soumissionnaire doit également être en mesure de fournir l'équipement technique nécessaire pour assurer le soutien du ou des services demandés (y compris le matériel et les logiciels nécessaires, le cas échéant).

Le soumissionnaire doit être en mesure de satisfaire aux exigences spécifiques concernant la non-divulgation d'informations, si cela est requis dans une demande particulière.

Le contractant doit être capable de travailler ensemble (avec les conseils d’iMio et toute partie prenante jugée nécessaire) avec d'autres partenaires pertinents pour des demandes spécifiques (y compris d'autres soumissionnaires, des Pouvoirs locaux, etc.).

**Installation**

Dans le cas où le lot concerné nécessiterait une installation et configuration logicielle, celle-ci ne pourra être soumise à une facturation additionnelle. Ainsi, le soumissionnaire devra inclure dans son offre l’installation et la configuration et aucune correction en ce sens ne pourra être accepté.

Un volet spécifique lié à l’installation devra être fourni par le soumissionnaire afin de jauger de la charge de travail ainsi que des attentes envers le Pouvoir local. Dans le cas d’une installation logicielle, le soumissionnaire devra mentionner si le serveur applicatif est hébergé au sein de l’infrastructure du Pouvoir local ou s’il sera disponible sous le format « SaaS ». Dans le cas d’un hébergement au sein du Pouvoir local, le soumissionnaire devra inclure dans son prix les spécificités matérielles nécessaires et inclure l’achat du matériel dans le prix remis lors du marché dans le cas où il ne pourrait pas utiliser le système actuellement en service pour l’installation du service.

**Maintenance et Support**

Les soumissionnaires fourniront dans leur devis les services de garantie, d'assistance et de maintenance de type premium.

La qualité de service de garantie/assistance et options de maintenance, y compris la mise à disposition d'un seul point de contact seront des éléments pris en compte lors de l’attribution.

Le soumissionnaire devra indiquer à iMio lors de la soumission de son offre, les différentes possibilités de prises en charge des demandes et incidents, la méthode de contact ainsi que les objectifs de résolution des incidents et requêtes.

Outre l’explication de la prise de contact et de la procédure d’introduction des incidents, un rapport mensuel ou trimestriel devra être fourni au Pouvoir local afin d’assurer le suivi des incidents.

Dans le cas le soumissionnaire ne saurait garantir un service endéans les chiffres communiqués dans la remise de l’offre, des pénalités pourraient s’appliquer. En ce sens, le soumissionnaire renseignera dans l’offre, la grille qu’il considère juste pour ce marché.

**Documentations**

Les soumissionnaires fourniront dans leur devis les services de garantie, d'assistance et de maintenance de type premium.

La qualité de service de garantie/assistance et options de maintenance, y compris la mise à disposition d'un seul point de contact seront des éléments pris en compte lors de l’attribution.

Le soumissionnaire devra indiquer à iMio lors de la soumission de son offre, les différentes possibilités de prises en charge des demandes et incidents, la méthode de contact ainsi que les objectifs de résolution des incidents et requêtes.

Outre l’explication de la prise de contact et de la procédure d’introduction des incidents, un rapport mensuel ou trimestriel devra être fourni au Pouvoir local afin d’assurer le suivi des incidents.

Dans le cas où le soumissionnaire ne saurait garantir un service tel que décrit dans son offre, des pénalités pourraient s’appliquer. En ce sens, le soumissionnaire renseignera dans l’offre, la grille qu’il considère juste pour ce marché.

### Lot L1 : Journalisation des événements

#### Objectif du lot

La journalisation des événements est une étape cruciale de la sécurité informatique. Elle consiste à enregistrer tous les évènements qui ont lieu sur un réseau, afin de permettre une meilleure surveillance et une analyse en cas de problème ou de menace.

Les objectifs de ce lot sont multiples :

* Collecter et enregistrer de manière sécurisée les évènements survenus sur le réseau des Pouvoirs locaux wallons ;
* Mettre en place une infrastructure permettant de stocker et de traiter les journaux de manière efficace ;
* Fournir une interface de visualisation et d'analyse des journaux pour les équipes de sécurité ;
* Assurer la conformité aux réglementations en vigueur en matière de journalisation des événements ;
* Mise en place d'un système de journalisation des évènements conforme aux réglementations en vigueur (RGPD, ISO 27001, etc.) ;
* Collecte et archivage des journaux d'événements provenant de différents équipements de l'infrastructure de sécurité (firewalls, IDS/IPS, serveurs, etc.) ;
* Analyse en temps réel des journaux pour détection de menaces et alertes ;
* Possibilité de consultation et de recherche des journaux par les équipes de sécurité ;
* Mise à disposition de fonctionnalités de rapport pour suivi et analyse des événements ;
* Mise en place de règles de rétention adaptées aux besoins et aux exigences réglementaires.

#### Caractéristiques spécifiques du lot

Dans le cadre de notre stratégie de sécurité de l'information, nous recherchons un produit de journalisation des événements qui répondra à nos exigences en matière de collecte, d'analyse et de rapport des données de journalisation. Nous souhaitons être en mesure de suivre et de comprendre les activités qui se déroulent sur notre réseau, afin de pouvoir réagir rapidement en cas d'incident de sécurité. Pour ce faire, nous recherchons un produit qui possède les caractéristiques suivantes :

* Capacité à collecter des journaux de données de différents équipements et systèmes informatiques ;
* Fonctionnalités de filtrage et de recherche avancées pour identifier rapidement les évènements pertinents ;
* Possibilité de configurer des alertes en temps réel pour les évènements critiques ;
* Intégration avec d'autres outils de sécurité, tels que les pares-feux et les systèmes de détection d’intrusion ;
* Facilité d'utilisation pour les administrateurs de système et les responsables de la sécurité ;
* Support technique et documentation détaillée fournis par le fournisseur du produit ;
* Capacité à journaliser tous les évènements de sécurité pertinents de l'ensemble des systèmes et réseaux ;
* Possibilité de configurer des alertes en temps réel en cas d'évènements anormaux ou suspects ;
* Fonctionnalités de recherche avancée permettant de filtrer et d'analyser les journaux de manière efficace ;
* Intégration avec d'autres outils de sécurité tels que les systèmes de détection d'intrusion (IDS) et de prévention d'intrusion (IPS) ;
* Capacité à gérer des volumes importants de journaux sans perturbation des performances du système ;
* Support de plusieurs protocoles de journalisation, tels que Syslog, Windows Event Log et JSON, pour une compatibilité maximale avec les équipements existants ;
* Mise en place d'une stratégie de rotation et de conservation des journaux afin de garantir la disponibilité à long terme des données de journalisation.

#### Spécificités techniques

Pour assurer la sécurité et la protection des données des Pouvoirs locaux wallons, il est crucial de disposer d'un système de journalisation efficace qui permette de suivre et de surveiller tous les événements survenus au sein de l'organisation. Cela nécessite des produits de journalisation de haute qualité, capables de collecter, de traiter et de stocker de grandes quantités de données de manière fiable et sécurisée. Pour ce faire, nous recherchons des soumissionnaires possédant les spécificités techniques suivantes :

* Capacité à enregistrer et stocker des logs de différents évènements (connexions, actions de l'utilisateur, erreurs, etc.) sur l'ensemble des équipements de l'organisation, y compris les serveurs, les ordinateurs de bureau, les terminaux mobiles, les appareils de réseau, etc. ;
* Capacité à collecter, trier et analyser les logs en temps réel et à identifier les évènements anormaux ou suspects ;
* Capacité à mettre en place des alertes automatiques en cas d'évènement important ou de tentative de brèche de sécurité ;
* Capacité à fournir une interface de gestion intuitive et conviviale permettant de visualiser et de gérer les logs de manière centralisée et de faciliter leur utilisation par les équipes de sécurité et de support ;
* Capacité à assurer la confidentialité et l'intégrité des logs et à protéger les données enregistrées contre toute modification ou suppression non autorisée ;
* Capacité à intégrer des fonctionnalités de journalisation avancées telles que la mise en place de règles de filtrage, la création de profils d'utilisateur, la gestion des droits d'accès, etc. ;
* Capacité à collecter et analyser des données de journalisation de différentes sources, notamment les systèmes d'exploitation, les applications et les équipements de réseau ;
* Compétences en matière de sécurité de l'information, notamment en ce qui concerne les réglementations et les normes en vigueur ;
* Connaissance des meilleures pratiques en matière de gestion de la journalisation des événements, y compris la création de politiques et de procédures de journalisation ;
* Expérience de déploiement et de maintenance de solutions de journalisation des évènements dans des environnements complexes ;
* Capacité à fournir une formation et un support technique pour l'utilisation de la solution de journalisation des événements.

#### Rapport et documentations

Pour garantir une mise en œuvre efficace et conforme aux exigences de la réglementation, nous attendons des soumissionnaires les éléments suivants :

* Des rapports sur la mise en œuvre et la configuration du produit de journalisation des événements ;
* Des documents décrivant les processus de gestion des alertes et des notifications générées par le produit ;
* Des rapports de performance et de disponibilité du produit ;
* Des documents décrivant les procédures de sauvegarde et de restauration des données de journalisation ;
* Des documents décrivant les procédures de maintenance préventive et corrective du produit ;
* Des manuels d'utilisation et de formation destinés aux utilisateurs finaux du produit ;
* Documentation technique décrivant les fonctionnalités et les caractéristiques du produit proposé ;
* Rapports de test et de validation du produit, y compris des résultats de tests de performance et de charge ;
* Preuves de conformité aux réglementations et normes industrielles pertinentes ;
* Références de clients ayant déjà mis en œuvre le produit et témoignages de leur satisfaction ;
* Guides de mise en œuvre et de maintenance du produit, y compris des procédures de déploiement et de mise à jour ;
* Garanties et assurances de qualité du produit et du support proposé par le soumissionnaire.

#### Obligation de résultats

La journalisation des événements est un élément clé de la sécurité informatique, permettant de suivre et d'analyser les activités et les incidents sur les réseaux et les systèmes. Il est donc important de s'assurer que les soumissionnaires pour ce lot seront en mesure de fournir des produits de qualité, fiables et efficaces pour la journalisation des événements. Pour cela, voici quelques obligations de résultats que les soumissionnaires pourraient être tenus de respecter :

* Capacité à collecter et à stocker de manière sécurisée les journaux d'évènements provenant de différents équipements et sources ;
* Capacité à analyser et à visualiser les journaux d'évènements de manière à faciliter la détection et la résolution des incidents ;
* Fonctionnalités de rapport et de notification pour informer les responsables de sécurité en cas de problème ou de comportement suspect ;
* Mise à disposition de guides et de documentation pour aider les utilisateurs à configurer et à utiliser les produits de journalisation des évènements de manière optimale ;
* Garantie de disponibilité et de performance des produits de journalisation des évènements, avec un temps de réponse rapide en cas de problème ou de besoin de support ;
* Fournir un système de journalisation fiable et efficace qui permettra de suivre et d'analyser les événements de sécurité de manière centralisée ;
* S'assurer que le système de journalisation est conforme aux réglementations et aux normes de sécurité en vigueur ;
* Fournir un support technique pour l'installation, la configuration et l'intégration du système de journalisation dans l'infrastructure existante des Pouvoirs locaux ;
* Fournir une documentation détaillée sur l'utilisation et la maintenance du système de journalisation ;
* Fournir des mises à jour régulières du système de journalisation pour garantir sa compatibilité avec les évolutions technologiques et les nouvelles réglementations de sécurité.

#### Domaines d’expertise à maîtriser

La journalisation des évènements est un élément clé de la sécurité de l'information pour les Pouvoirs locaux. Elle permet de surveiller et de suivre les activités de l'organisation, de détecter les anomalies et les incidents de sécurité, et de fournir une preuve lors d'enquêtes ou de litiges. Afin de s'assurer que les Pouvoirs locaux disposent d'une journalisation efficace et fiable, il est important de mettre en place des produits et des services de qualité qui répondent à leurs besoins spécifiques. Les soumissionnaires doivent donc être en mesure de démontrer leur expertise dans ce domaine et de proposer des solutions adaptées aux exigences des Pouvoirs locaux :

* Connaissance des règlementations et normes en matière de journalisation des évènements (par exemple, PCI DSS, GDPR, ISO 27001) ;
* Expérience dans l'implémentation de solutions de journalisation des évènements dans des environnements de taille similaire à celui des Pouvoirs locaux wallons ;
* Maîtrise des technologies et protocoles utilisés dans les solutions de journalisation des évènements (par exemple, Syslog, CEF, JSON) ;
* Capacité à intégrer des solutions de journalisation des évènements dans des architectures de sécurité existantes ;
* Expérience dans la gestion de grandes quantités de données de journalisation et dans l'analyse de ces données pour identifier des anomalies et des menaces potentielles ;
* Capacité à configurer et à personnaliser les règles de journalisation et les alertes en fonction des besoins spécifiques du client ;
* Expérience en matière de gestion et d'analyse des journaux d'événements, notamment en utilisant des outils de visualisation de données et de corrélation d’événements ;
* Bonne compréhension des architectures de réseau et des protocoles de communication courants, ainsi que des enjeux de sécurité associés ;
* Capacité à travailler en étroite collaboration avec les équipes de sécurité et de réseau pour définir les besoins en matière de journalisation et mettre en œuvre des solutions adaptées.

#### Scénario pour compléter l’inventaire

Scénario pour le lot "Journalisation des événements" - 2Go de données quotidienne :

Volumétrie et quantités nécessaires :

* Fourniture et mise en place de :
  + Équipement d'une capacité totale de stockage de 4 To (pour prévoir le stockage longue durée des données) :
  + 2 disques durs de 2 To chacun pour une capacité de stockage totale de 4 To (permettant la mise en place de la redondance et du RAID pour une meilleure protection des données).
* Licence pour le logiciel afin de couvrir l’ensemble des fonctionnalités demandées
* Capacité d’ingérer 400 event par seconde.
* Prestations nécessaires à la mise en œuvre des fonctionnalités exprimées.

Implémentation pratique :

* La solution de journalisation des événements sera déployée au sein de l'infrastructure du pouvoir local pour collecter les logs provenant de différents systèmes et équipements.
* Elle sera configurée pour collecter les logs des serveurs, des équipements réseau, des applications et des dispositifs de sécurité, permettant une vue d'ensemble des activités de l'environnement informatique.
* Les logs collectés seront stockés de manière sécurisée et fiable, garantissant l'intégrité et la confidentialité des données.
* La solution offrira des fonctionnalités avancées d'analyse des logs, permettant de détecter les incidents de sécurité, les comportements anormaux et les indicateurs de compromission.
* Elle fournira également des options de génération de rapports personnalisés et d'exportation des données, offrant une flexibilité dans l'analyse des logs.

### Lot L2 : Gestion de l’authentification et identification numérique

#### Objectif du lot

Le management de l'authentification et de l'identification est un enjeu de sécurité majeur pour les Pouvoirs locaux wallons. Il est essentiel de garantir l'accès aux ressources et aux informations de manière sécurisée et contrôlée, tout en assurant la confidentialité et l'intégrité des données. Les projets liés au management de l'authentification et à l'identification visent à mettre en place des solutions adaptées et efficaces pour répondre à ces enjeux, en tenant compte des besoins et des contraintes de chaque organisation. L'objectif de ce lot est de sélectionner des soumissionnaires capables de proposer et de mettre en œuvre des projets de management de l'authentification et de l'identification répondant aux exigences de sécurité et de qualité requises.

#### Caractéristiques spécifiques du lot

Pour assurer la sécurité de l'identification et de l'authentification numérique de l'ensemble des utilisateurs et de leurs données, il est crucial de mettre en place des projets de management de l'authentification et de l'identification numérique de haute qualité. Les soumissionnaires doivent être en mesure de proposer des solutions adaptées aux besoins spécifiques des Pouvoirs locaux wallons et de garantir leur efficacité à long terme :

* Gestion avancée des identités et des accès ;
* Intégration avec les systèmes de gestion de l'identité existants ;
* Support multi-facteur d’authentification ;
* Gestion des politiques d'accès et des processus de vérification ;
* Fonctionnalités de rapport et de surveillance des activités d'authentification et d’identification ;
* Compatibilité avec les normes et réglementations en matière de sécurité de l'identité et de l'authentification numérique (par exemple, GDPR, ISO 27001) ;
* Capacité à fournir un système de gestion de l'authentification et de l'identification qui respecte les normes de sécurité les plus récentes et les plus strictes, telles que les recommandations de l'Agence nationale de la sécurité des systèmes d'information (ANSSI) ;
* Capacité à intégrer le système de gestion de l'authentification et de l'identification dans les systèmes et applications existants des Pouvoirs locaux, de manière à assurer une intégration transparente et à minimiser les perturbations pour les utilisateurs ;
* Capacité à fournir une solution de gestion de l'authentification et de l'identification qui permet une gestion flexible et évolutive des identités et des accès, en fonction des besoins changeants des Pouvoirs locaux ;
* Capacité à fournir une solution de gestion de l'authentification et de l'identification qui offre une forte sécurité de l'identité et de l'accès, par exemple en utilisant des mécanismes de deux facteurs d’authentification ;
* Capacité à fournir une solution de gestion de l'authentification et de l'identification qui offre un haut niveau de disponibilité et de performance, de manière à assurer un accès continu aux applications et aux services pour les utilisateurs des Pouvoirs locaux.

#### Spécificités techniques

Pour gérer de manière sécurisée l'accès aux systèmes et aux applications utilisés par leur personnel, les Pouvoir locaux wallons souhaitent mettre en place une solution d'authentification et d'identification numérique conforme aux réglementations et aux normes de sécurité en vigueur en Belgique. Le soumissionnaire doit suivre les spécificités techniques suivantes :

* La solution proposée devra utiliser des technologies de sécurité de pointe pour protéger les données sensibles des utilisateurs et garantir la sécurité des systèmes et des applications ;
* La solution proposée devra être compatible avec les systèmes et les applications existants utilisés par les Pouvoirs locaux ;
* Le soumissionnaire devra décrire les mesures de sauvegarde et de reprise après sinistre qu'il mettra en place pour assurer la disponibilité de la solution en cas de problèmes ;
* Le soumissionnaire devra décrire les processus de gestion des mises à jour et des évolutions de la solution au fil du temps ;
* Le soumissionnaire devra présenter une stratégie de gestion de la sécurité de l'information pour assurer la protection des données sensibles des utilisateurs et la sécurité des systèmes et des applications ;
* Le soumissionnaire devra décrire les processus de gestion des incidents de sécurité et de réponse aux incidents de sécurité qu'il mettra en place pour gérer les éventuels problèmes de sécurité qui pourraient survenir ;
* Le soumissionnaire devra démontrer qu'il a une connaissance approfondie des technologies et des protocoles de sécurité utilisés dans les projets d'authentification et d'identification numérique ;
* Le soumissionnaire devra présenter une stratégie de gestion des risques pour la solution proposée, incluant une évaluation des risques et des mesures de prévention et de mitigation ;
* Le soumissionnaire devra présenter une stratégie de gestion de la conformité avec les réglementations et les normes de sécurité en vigueur en Belgique ;
* Le soumissionnaire devra décrire les mesures qu'il prendra pour assurer la confidentialité et l'intégrité des données sensibles des utilisateurs de la solution ;
* Le soumissionnaire devra présenter une stratégie de gestion de la disponibilité de la solution, incluant des processus de surveillance et de maintenance pour garantir une disponibilité maximale de la solution.

#### Rapport et documentations

Afin de jauger la véracité de l’offre, un ensemble de documents peut être demandé aux soumissionnaires :

* Un rapport détaillé sur la solution d'authentification et d'identification numérique proposée, incluant une description des fonctionnalités, des technologies utilisées, et des processus de gestion des droits d'accès et de mise à jour des informations d’identification ;
* Des documentations sur la stratégie de sécurité proposée, incluant des mesures de sécurité pour protéger les données sensibles des utilisateurs et des processus de gestion des incidents de sécurité ;
* Des exemples de projets similaires réalisés par le soumissionnaire, incluant une description des défis rencontrés et de la manière dont ils ont été résolus ;
* Un plan de formation pour les utilisateurs de la solution, incluant des objectifs de formation, des modalités de formation, et un calendrier de formation ;
* Des informations sur le support technique et l'assistance proposés par le soumissionnaire, incluant les canaux de support disponibles (par exemple, téléphone, courriel, chat en direct), les heures de disponibilité, et les processus de gestion des incidents de support ;
* Des rapports réguliers sur l'utilisation de la solution et sur les éventuels problèmes rencontrés, incluant des statistiques d'utilisation et des informations sur les problèmes résolus ;
* Le soumissionnaire devra fournir une documentation sur les processus de gestion de la sécurité de l'information mis en place pour assurer la protection des données sensibles des utilisateurs et la sécurité des systèmes et des applications ;
* Le soumissionnaire devra présenter des preuves de son expérience et de sa capacité à mettre en place des solutions d'authentification et d'identification numérique sécurisées, incluant des références de clients précédents et des témoignages de satisfaction ;
* Le soumissionnaire devra présenter un plan de déploiement détaillé pour la solution d'authentification et d'identification numérique, incluant des échéances et des points de passages clairs ;
* Le soumissionnaire devra décrire les mesures qu'il prendra pour assurer la pérennité de la solution et pour gérer les mises à jour et les évolutions de la solution au fil du temps ;
* Le soumissionnaire devra présenter une stratégie de communication pour informer les utilisateurs de la solution et de toutes les mises à jour et évolutions de la solution.

#### Obligation de résultats

Les Pouvoirs locaux wallons souhaitent mettre en place une solution d'authentification et d'identification numérique afin de gérer de manière sécurisée l'accès aux systèmes et aux applications utilisés par leur personnel. Le soumissionnaire choisi devra fournir une formation au personnel des Pouvoirs locaux sur l'utilisation de la solution, ainsi qu'un support technique et une assistance en cas de problèmes ou de questions. Il devra également mettre en place un processus de gestion des droits d'accès et de mise à jour des informations d'identification et fournir des rapports réguliers sur l'utilisation de la solution et sur les éventuels problèmes rencontrés. De plus, il incombera aux soumissionnaires les obligations de résultats suivants :

* Le soumissionnaire devra mettre en place une solution d'authentification et d'identification numérique sécurisée pour les Pouvoirs locaux wallons ;
* La solution devra être conforme aux réglementations et aux normes de sécurité en vigueur en Belgique ;
* Le soumissionnaire devra fournir une formation au personnel des Pouvoirs locaux sur l'utilisation de la solution ;
* Le soumissionnaire devra fournir un support technique et une assistance aux utilisateurs de la solution en cas de problèmes ou de questions ;
* Le soumissionnaire devra s'assurer que la solution est compatible avec les systèmes existants et les applications utilisées par les Pouvoirs locaux ;
* Le soumissionnaire devra mettre en place un processus de gestion des droits d'accès et de mise à jour des informations d’identification ;
* Le soumissionnaire devra fournir des rapports réguliers sur l'utilisation de la solution et sur les éventuels problèmes rencontrés ;
* Le soumissionnaire devra démontrer qu'il a une connaissance approfondie des réglementations et des normes de sécurité en vigueur en Belgique en matière d'authentification et d'identification numérique ;
* Le soumissionnaire devra présenter des exemples de projets similaires qu'il a réalisés avec succès pour d'autres clients ;
* Le soumissionnaire devra présenter une stratégie de sécurité pour la solution proposée, incluant des mesures de sécurité pour protéger les données sensibles des utilisateurs ;
* Le soumissionnaire devra proposer une stratégie de gestion de la sécurité de l'information pour assurer la protection des données sensibles des utilisateurs et la sécurité des systèmes et des applications ;
* Le soumissionnaire devra décrire les processus de gestion des incidents de sécurité et de réponse aux incidents de sécurité qu'il mettra en place pour gérer les éventuels problèmes de sécurité qui pourraient survenir.

#### Domaines d’expertise à maîtriser

Pour assurer la mise en œuvre réussie et sécurisée de projets liés au management de l'authentification et à l'identification numérique pour les Pouvoirs wallons, nous recherchons des soumissionnaires possédant une solide expertise dans les domaines suivants :

* Connaissance des réglementations et des normes en matière d'authentification et d'identification numérique en Belgique ;
* Expérience dans la mise en place et le déploiement de systèmes d'authentification et d'identification numérique ;
* Compétences en matière de sécurité de l'information et de gestion des risques liés aux systèmes d'authentification et d'identification numérique ;
* Connaissance des technologies et des protocoles utilisés dans les systèmes d'authentification et d'identification numérique (par exemple, OAuth, SAML, OpenID Connect) ;
* Expérience de travail avec des Pouvoirs locaux ou d'autres organismes gouvernementaux ;
* Compétences en matière de communication et de gestion de projet, afin de gérer efficacement la mise en œuvre et le déploiement de projets liés à l'authentification et à l'identification numérique ;
* Expérience de travail avec des plateformes d'authentification et d'identification numérique, telles que des portails de gestion de l'identité (Identity Management) ou des systèmes de gestion de l'authentification (Authentication Management) ;
* Compétences en matière de développement de solutions d'authentification et d'identification numérique, y compris la connaissance de différents langages de programmation ;
* Connaissance des outils et technologies utilisés pour la gestion de l'identité et de l'authentification numérique, tels que les répertoires (annuaires), les bases de données d'identité et les gestionnaires de mots de passe ;
* Capacité à travailler en étroite collaboration avec les équipes de développement et de sécurité pour assurer la mise en œuvre efficace et sécurisée de projets d'authentification et d'identification numérique ;
* Compétences en matière de formation et de support technique pour les utilisateurs finaux, afin de garantir que les systèmes d'authentification et d'identification numérique sont utilisés de manière efficace et sécurisée ;
* Connaissance des tendances et des innovations dans le domaine de l'authentification et de l'identification numérique, afin de pouvoir conseiller et orienter les Pouvoirs locaux sur les meilleures pratiques et les technologies les plus récentes.

#### Scénario pour compléter l’inventaire

Scénario pour le lot "Gestion de l'authentification et identification numérique - 200 utilisateurs.

Volumétrie et spécifications techniques requises :

* L'infrastructure doit être en mesure de prendre en charge un minimum de 200 utilisateurs.
* Le système doit être compatible avec les protocoles d'authentification couramment utilisés, tels que OAuth, SAML et OpenID.
* La solution doit offrir des fonctionnalités de gestion des identités, notamment la création, la modification et la suppression des comptes utilisateurs.
* Le processus d'inscription et de gestion des comptes utilisateurs doit être convivial et permettre une administration centralisée.
* L'authentification doit être réalisée de manière transparente et rapide, offrant une expérience utilisateur fluide.
* La plateforme doit permettre l'intégration avec les annuaires d'entreprises existants et les bases de données d'utilisateurs.

Implémentation pratique :

* Chaque utilisateur doit disposer d'un identifiant unique et sécurisé pour accéder aux ressources et services de l'organisation.
* Si la gestion de l’authentification nécessite du matériel physique, ce dernier sera installé au sein de l'infrastructure du pouvoir local.
* Elle fournira également des options de génération de rapports personnalisés et d'exportation des données, offrant une flexibilité dans l'analyse des logs.
* Une formation et un accompagnement doivent être prévus pour les administrateurs et les utilisateurs afin de faciliter l'adoption et l'utilisation efficace de la solution.

### Lot L3 : Filtrage des messages électroniques

#### Objectif du lot

Afin de protéger la sécurité et la confidentialité des communications électroniques des Pouvoirs locaux wallons, tout en améliorant la productivité des utilisateurs, nous recherchons des produits de filtrage de messages électroniques qui visent à atteindre les objectifs suivants :

* Assurer la sécurité et la confidentialité des messages électroniques des Pouvoirs locaux en filtrant les messages indésirables (spam) et les menaces de sécurité (phishing, virus, etc.) ;
* Améliorer la productivité des utilisateurs en réduisant le volume de messages indésirables reçus. ;
* Offrir une solution flexible et adaptable qui peut être configurée en fonction des besoins spécifiques des Pouvoirs locaux ;
* Fournir une assistance technique de qualité pour l'installation, la configuration et l'utilisation de la solution de filtrage des messages électroniques ;
* Garantir la compatibilité avec les principaux systèmes de messagerie et les plateformes de collaboration utilisées par les Pouvoirs locaux ;
* Mettre en place des mesures de sécurité pour protéger les données des utilisateurs et des Pouvoirs locaux contre les fuites de données et les cyberattaques.

#### Caractéristiques spécifiques du lot

Dans le cadre de notre marché pour la mise à disposition de produits de filtrage des messages électroniques pour les Pouvoirs locaux wallons, nous recherchons des soumissionnaires proposant des solutions répondant aux caractéristiques suivantes :

* Capacité à fournir des fonctionnalités de filtrage de base, telles que le filtrage des courriers indésirables, le filtrage du spam et le filtrage des virus ;
* Capacité à fournir des fonctionnalités avancées de filtrage, telles que la détection de phishing, le filtrage de contenu inapproprié et la protection contre les menaces avancées ;
* Capacité à intégrer le produit de filtrage des messages électroniques avec les systèmes de messagerie existants des Pouvoirs locaux wallons ;
* Capacité à fournir une interface utilisateur conviviale pour la gestion des règles de filtrage et pour la consultation des journaux de filtrage ;
* Capacité à fournir un support technique de qualité pour le déploiement et l'utilisation du produit de filtrage des messages électroniques ;
* Capacité à offrir une formation au personnel des Pouvoirs locaux wallons sur l'utilisation du produit de filtrage des messages électroniques ;
* Capacité à fournir une documentation détaillée sur le fonctionnement et l'utilisation du produit de filtrage des messages électroniques ;
* Capacité à fournir une solution de filtrage des messages électroniques adaptée aux besoins et aux contraintes des Pouvoirs locaux wallons ;
* Capacité à offrir des mises à jour régulières du produit de filtrage des messages électroniques pour assurer sa conformité aux normes de sécurité et de confidentialité en vigueur ;
* Capacité à fournir des outils de rapport et de gestion des performances pour permettre aux Pouvoirs locaux wallons de surveiller et d'optimiser l'efficacité du produit de filtrage des messages électroniques ;
* Capacité à intégrer le produit de filtrage des messages électroniques avec d'autres systèmes de sécurité et de gestion de la confidentialité des données ;
* Capacité à offrir des options de déploiement flexibles, telles que le déploiement en mode SaaS ou en mode hébergé ;
* Capacité à fournir une assistance technique personnalisée et un suivi continu pour assurer le bon fonctionnement du produit de filtrage des messages électroniques ;
* Capacité à offrir des garanties et des assurances en matière de sécurité et de confidentialité des données traitées par le produit de filtrage des messages électroniques.

#### Spécificités techniques

Dans le cadre de notre marché pour la mise à disposition de produits de filtrage des messages électroniques pour les Pouvoirs locaux wallons, nous recherchons des soumissionnaires proposant des solutions répondant aux spécificités techniques suivantes :

* Capacité à prendre en charge les protocoles de messagerie courants, tels qu’Exchange, SMTP, IMAP et POP3;
* Capacité à gérer les fichiers joints de grande taille et à protéger contre les virus et les logiciels malveillants ;
* Capacité à fournir une protection contre le spam et les courriers indésirables grâce à des filtres de contenu avancés ;
* Capacité à détecter et à bloquer les tentatives de phishing et d’hameçonnage ;
* Capacité à intégrer le produit de filtrage des messages électroniques avec les pares-feux et les autres systèmes de sécurité du réseau des Pouvoirs locaux wallons ;
* Capacité à offrir une solution de filtrage des messages électroniques scalable et capable de prendre en charge de grandes quantités de trafic de messagerie ;
* Capacité à fournir une documentation détaillée sur l'architecture et les spécificités techniques du produit de filtrage des messages électroniques ;
* Capacité à fournir une solution de filtrage des messages électroniques fonctionnant en mode cloud ou en mode hébergé, selon les préférences des Pouvoirs locaux wallons ;
* Capacité à intégrer le produit de filtrage des messages électroniques avec d'autres outils de gestion de la messagerie, tels que les boîtes aux lettres partagées et les listes de diffusion ;
* Capacité à prendre en charge les protocoles de chiffrement de bout en bout pour assurer la confidentialité des messages électroniques ;
* Capacité à offrir des fonctionnalités de gestion des politiques de courrier, telles que la définition de règles de routage et de retenue des messages ;
* Capacité à fournir une solution de filtrage des messages électroniques facilement personnalisable et adaptable aux besoins changeants des Pouvoirs locaux wallons ;
* Capacité à offrir une solution de filtrage des messages électroniques respectueuse de la vie privée et conforme aux réglementations en matière de protection des données ;
* Capacité à fournir une solution de filtrage des messages électroniques qui s'intègre facilement dans l'environnement de travail des utilisateurs des Pouvoirs locaux wallons.
* Sandbox

#### Rapport et documentations

Dans le cadre de notre marché pour la mise à disposition de produits de filtrage des messages électroniques pour les Pouvoirs locaux wallons, nous vous demandons de nous fournir les documents et les rapports suivants afin de nous permettre d'évaluer votre offre de manière adéquate. Ces informations nous permettront de mieux comprendre les caractéristiques et les fonctionnalités de votre produit, ainsi que les services de support et les coûts associés à son utilisation :

* Un manuel d'utilisation détaillé du produit de filtrage des messages électroniques, incluant les instructions d'installation et de configuration ;
* Un guide de démarrage rapide pour aider les utilisateurs des Pouvoirs locaux wallons à prendre en main rapidement le produit de filtrage des messages électroniques ;
* Des fiches techniques sur les fonctionnalités et les spécificités techniques du produit de filtrage des messages électroniques ;
* Des guides de formation pour aider les utilisateurs des Pouvoirs locaux wallons à maîtriser les différentes fonctionnalités du produit de filtrage des messages électroniques ;
* Des rapports de performance et de qualité sur le fonctionnement du produit de filtrage des messages électroniques dans différents environnements ;
* Des documents de référence sur les protocoles et les normes de sécurité et de confidentialité applicable aux produits de filtrage des messages électroniques ;
* Des documents de garantie et de responsabilité couvrant les aspects techniques et juridiques liés à l'utilisation du produit de filtrage des messages électroniques ;
* Un catalogue ou une liste des produits proposés, avec une description détaillée de leurs caractéristiques et de leurs fonctionnalités ;
* Une description de la stratégie de filtrage des messages électroniques utilisée par le produit, y compris les méthodes de détection de spam et de virus ;
* Des informations sur la performance du produit, y compris des données sur les taux de faux positifs et de faux négatifs ;
* Des informations sur les mesures de sécurité mises en place pour protéger les données des utilisateurs, y compris la gestion des mots de passe et l'authentification à deux facteurs ;
* Des informations sur les coûts associés à l'utilisation du produit, y compris les frais d'abonnement, les coûts de maintenance et les coûts de mise à niveau ;
* Des références de clients existants utilisant le produit, y compris leurs retours d'expérience et leur niveau de satisfaction ;
* Une description des services de support proposés par le soumissionnaire, y compris les horaires de disponibilité et les méthodes de contact ;
* Une évaluation de la conformité du produit aux réglementations et aux normes en matière de protection de la vie privée et de sécurité des données ;
* Une description de la stratégie de mise à jour et de maintenance du produit, y compris la fréquence des mises à jour et la disponibilité de nouvelles fonctionnalités.

#### Obligation de résultats

Nous demandons à chaque soumission de nous faire parvenir les éléments suivants auquel vous vous engagez :

* Un taux de détection de spam supérieur à X%
* Un taux de détection de virus supérieur à Y%
* Un taux de faux positifs inférieur à Z%
* Un temps de réponse inférieur à T secondes pour la réception et le traitement des messages électroniques
* Une disponibilité de service supérieure à X% en termes de temps de fonctionnement ininterrompu par mois
* Une assistance technique disponible H/24 et 7/7 avec un délai de réponse maximum de Y heures pour les demandes de niveau 1 et de Z heures pour les demandes de niveau 2
* Des mises à jour logicielles et de sécurité mensuelles ou trimestrielles
* Une formation initiale et continue pour les utilisateurs finaux sur l'utilisation du produit et ses fonctionnalités
* Un suivi régulier de la performance du produit et de la satisfaction des utilisateurs avec la mise en place de plans d'actions en cas de défaillance ou de problème.

#### Domaines d’expertise à maîtriser

Dans le cadre de notre marché pour la mise à disposition d’outils de filtrage des messages électroniques pour les Pouvoirs locaux wallons, nous recherchons des soumissionnaires possédant une expertise solide dans les domaines suivants :

* Connaissance de l'environnement législatif et réglementaire en matière d'authentification et d'identification numérique pour les Pouvoirs locaux wallons ;
* Expérience en matière de déploiement de systèmes d'authentification et d'identification numérique pour les Pouvoirs locaux wallons ;
* Expérience en matière de gestion de la sécurité des données et des informations, notamment en ce qui concerne les protocoles de sécurité, les stratégies de gestion des accès et les protocoles de gestion des incidents de sécurité ;
* Maîtrise de technologies de l'authentification et de l'identification numérique, telles que les certificats numériques, les jetons de sécurité et les technologies de l'identité forte ;
* Expérience en matière de développement de solutions de gestion de l'authentification et de l'identification numérique, y compris les applications Web et mobiles ;
* Expérience en matière de gestion de projets liés à l'authentification et à l'identification numérique pour les Pouvoirs locaux wallons, y compris la gestion des délais, des coûts et de la qualité ;
* Compétences en matière de communication et de sensibilisation du personnel aux enjeux de l'authentification et de l'identification numérique;
* Connaissance des différents types de logiciels de filtrage des messages électroniques et de leurs fonctionnalités ;
* Expérience en matière de déploiement et de configuration de logiciels de filtrage des messages électroniques ;
* Maîtrise des protocoles de sécurité et des normes de confidentialité en matière de traitement des messages électroniques ;
* Compétences en matière de gestion de la sécurité des données et des informations, notamment en ce qui concerne les protocoles de sécurité, les stratégies de gestion des accès et les protocoles de gestion des incidents de sécurité ;
* Expérience en matière de développement de solutions de filtrage des messages électroniques, y compris les applications Web et mobiles ;
* Expérience en matière de gestion de projets liés au filtrage des messages électroniques pour les Pouvoirs locaux wallons, y compris la gestion des délais, des coûts et de la qualité ;
* Compétences en matière de communication et de sensibilisation du personnel aux enjeux du filtrage des messages électroniques.

#### Scénario pour compléter l’inventaire

Scénario pour le lot "Filtrage des messages électroniques" - 150 utilisateurs

Volumétrie et quantités nécessaires :

* 150 licences de filtrage des courriels.
* Tableau de bord interactif
* Formation et documentation pour la gestion au quotidien du système.

Implémentation pratique :

* La solution de filtrage des messages électroniques sera déployée au sein de l'infrastructure du pouvoir local pour sécuriser la messagerie électronique des utilisateurs.
* Elle sera capable de traiter un volume élevé de messages électroniques, assurant une gestion efficace du flux de courrier électronique.
* La solution utilisera des mécanismes de détection avancée pour identifier et bloquer les spams et les emails malveillants, réduisant ainsi le risque d'infiltration de contenus indésirables dans les boîtes de réception.
* Elle effectuera un filtrage des pièces jointes potentiellement dangereuses, empêchant ainsi la propagation de fichiers malveillants par le biais des emails.
* La solution offrira également une protection contre les liens malveillants et les attaques de phishing, aidant à prévenir les tentatives de vol d'informations sensibles.
* Le référent informatique du pouvoir local sera formé sur l'utilisation basique du tableau de bord pour s’assurer du bon fonctionnement de la solution.
* Elle sera intégrée aux solutions de sécurité existantes du pouvoir local, permettant une gestion centralisée des politiques de sécurité et une vue d'ensemble des menaces liées aux emails.

### Lot L4 : Antivirus/antimalware/EDR/XDR

#### Objectif du lot

L'objectif principal de ce lot est de fournir aux Pouvoirs locaux wallons une solution de sécurité de pointe capable de protéger leurs systèmes informatiques et leurs réseaux contre les menaces en ligne les plus récentes, telles que les virus, les logiciels malveillants, les ransomwares et les attaques de phishing. La solution proposée devra inclure une protection antivirus/antimalware fiable et performante, ainsi qu'une technologie avancée de détection et de réponse (EDR/XDR) pour aider les Pouvoirs locaux à détecter et à remédier rapidement aux attaques en cours. En outre, la solution proposée devra être facile à déployer et à gérer, avec une interface utilisateur intuitive et un support technique de qualité supérieure. En garantissant la sécurité de leurs systèmes et de leurs réseaux, les Pouvoirs locaux pourront protéger leur confidentialité, leur intégrité et leur disponibilité des données, ainsi que leur réputation et leur crédibilité auprès des citoyens et des partenaires.

#### Caractéristiques spécifiques du lot

Le choix d'un produit Antivirus/Antimalware/EDR/XDR est crucial pour assurer la sécurité des systèmes informatiques des Pouvoirs locaux. Afin de garantir une protection efficace contre les menaces en ligne, il est important de s'assurer que les produits proposés répondent à certaines caractéristiques techniques précises. Voici une liste des caractéristiques techniques que les soumissionnaires devront prendre en compte dans leur offre :

* Mise à jour automatique des définitions de virus et de menaces en temps réel ;
* Capacité à détecter et à bloquer les menaces connues et inconnues, y compris les ransomwares et les logiciels malveillants avancés ;
* Intégration avec les outils de gestion de la sécurité existants (SIEM, EDR, etc.)
* Fonctionnalités de gestion des licences et de déploiement simplifies ;
* Support technique dédié et temps de réponse rapide en cas de problème ou de question ;
* Certifications reconnues (par exemple, AV-Test, Virus Bulletin, ICSA Labs) et taux de détection élevé selon les tests indépendants ;
* Capacité à détecter et éliminer les virus, logiciels malveillants et autres menaces informatiques en temps réel ;
* Capacité à analyser les comportements suspects et à détecter les logiciels malveillants en utilisant des techniques de Machine Learning ;
* Prise en charge des plateformes de système d'exploitation couramment utilisées par les Pouvoirs locaux wallons ;
* Capacité à intégrer des données provenant de sources externes pour améliorer la détection des menaces ;
* Interfaçage avec les outils de gestion de sécurité existants (ex : SIEM) ;
* Documentation détaillée sur les fonctionnalités et les configurations du produit ;
* Support technique et formation des utilisateurs proposés par le fournisseur.

#### Spécificités techniques

Pour assurer la sécurité informatique de votre organisation, il est essentiel de mettre en place une solution de protection contre les virus, les malwares et les attaques externes. Cela nécessite l'utilisation de produits Antivirus/Antimalware/EDR/XDR performants et adaptés aux besoins des Pouvoirs locaux. Afin de sélectionner le soumissionnaire le plus qualifié pour cette mission, voici les spécificités techniques à prendre en compte :

* Compatibilité avec les différents systèmes d'exploitation et logiciels utilisés par votre organisation ;
* Niveau de protection offert contre les différents types de virus et de malwares
* Capacité de détection et de réponse aux attaques externes (EDR/XDR) ;
* Interface de gestion et de configuration facile à utiliser ;
* Mises à jour et support technique réguliers ;
* Coût et modalités de maintenance et de mise à niveau du produit ;
* Capacité de détection et de suppression des logiciels malveillants, y compris les ransomwares et les menaces avancées ;
* Mise à disposition de mécanismes de protection en temps réel contre les logiciels malveillants et les tentatives d'intrusion ;
* Gestion centralisée des paramètres de sécurité et de configuration, y compris la possibilité de déployer et de mettre à jour les paramètres de sécurité à distance sur les postes de travail et les serveurs ;
* Intégration avec les outils de gestion de la sécurité existants du Pouvoir local, tels que les pares-feux et les gestionnaires de mots de passe ;
* Fonctionnalités de rapport et de surveillance pour suivre les activités de sécurité et détecter les incidents de sécurité potentiels ;
* Capacité de fournir une assistance technique et un support de niveau professionnel en cas de problèmes ou de questions liés à la sécurité ;
* Sandbox pour test des éléments dangereux avant d’être délivrés au destinataire.

#### Rapport et documentations

Pour garantir une protection efficace contre les menaces informatiques, il est essentiel de mettre en place des solutions de sécurité adéquates, telles que des antivirus, des antimalwares, des EDR (Endpoint Detection and Response) et des XDR (Extended Detection and Response). Les Pouvoirs locaux wallons ont la charge de la protection de leurs réseaux et de leurs données, et ils doivent être en mesure de s'assurer que les produits qu'ils utilisent répondent à leurs besoins de sécurité. En ce sens, seront demandés les documents suivants :

* Un rapport de déploiement détaillant les étapes suivies pour mettre en place les produits Antivirus/Antimalware/EDR/XDR sur les différents postes de travail et serveurs des Pouvoirs locaux ;
* Des rapports de performance et de couverture des produits, incluant les résultats des tests de détection et de protection contre les menaces ;
* Des documents de formation destinés aux utilisateurs finaux, incluant des guides d'utilisation et des procédures de gestion des alertes de sécurité ;
* Des documents de support technique, incluant des procédures de dépannage et de résolution des problèmes rencontrés avec les produits Antivirus/Antimalware/EDR/XDR ;
* Des mises à jour régulières sur l'état de la sécurité et les menaces en cours, ainsi que sur les mises à jour et les correctifs appliqués aux produits Antivirus/Antimalware/EDR/XDR ;
* Des rapports de performance et de couverture de la solution antivirus/antimalware, présentant les taux de détection et de faux positifs ;
* Des documents présentant les différentes méthodes utilisées pour détecter et éliminer les logiciels malveillants (signatures, analyses comportementales, etc.) ;
* Des documents détaillant les différentes fonctionnalités de l'EDR/XDR, ainsi que les processus de détection et de réponse aux menaces avancées ;
* Des rapports de tests indépendants de la solution antivirus/antimalware/EDR/XDR, réalisés par des organisations spécialisées dans ce domaine ;
* Des documents présentant les mesures de sécurité mises en place pour protéger les données des utilisateurs (chiffrement, contrôle d'accès, etc.) ;
* Des documents décrivant les plans de maintenance et de support proposés par le soumissionnaire pour assurer le bon fonctionnement de la solution antivirus/antimalware/EDR/XDR sur le long terme.

#### Obligation de résultats

Afin de s’assurer d’un suivi sérieux et qualitatif des titulaires, voici une série d’obligations de résultats non exhaustifs :

* Garantie de couverture complète contre les menaces informatiques, y compris les virus, chevaux de Troie, ransomwares et autres types de logiciels malveillants ;
* Mise à jour régulière des bases de données de signatures de menaces pour assurer une protection en temps réel ;
* Capacité à détecter et à bloquer les comportements suspects ou malveillants sur les réseaux et les appareils ;
* Fonctionnalités de protection avancées telles que l'analyse en profondeur des paquets, la détection des menaces avant leur exécution et la prévention des fuites de données ;
* Support technique de qualité pour assister les utilisateurs en cas de problèmes de sécurité ou de questions sur l'utilisation des produits ;
* Rapports de sécurité détaillés et personnalisables pour suivre les menaces détectées et les mesures prises pour y remédier ;
* Les soumissionnaires doivent être en mesure de fournir une protection complète contre les menaces en ligne, telles que les virus, les logiciels espions, les logiciels publicitaires et autres logiciels malveillants ;
* Ils doivent également être en mesure de fournir une protection contre les attaques de phishing et de ransomwares, ainsi que contre les menaces liées aux réseaux sociaux ;
* En outre, les soumissionnaires doivent être en mesure de fournir une protection en temps réel contre les menaces en ligne et doivent être en mesure de mettre à jour régulièrement leurs produits pour garantir une protection continue ;
* Enfin, les soumissionnaires doivent être en mesure de fournir une assistance technique de qualité pour aider les utilisateurs à résoudre tous les problèmes liés à la sécurité ;
* Fournir une protection en temps réel contre les menaces en ligne et mettre à jour régulièrement les produits pour garantir une protection continue ;
* Offrir une assistance technique de qualité pour aider les utilisateurs à résoudre tous les problèmes liés à la sécurité ;
* Fournir une documentation claire et détaillée sur les produits et leur utilisation ;
* Fournir une formation à l'utilisation des produits aux utilisateurs finaux ;
* Offrir une garantie de remboursement ou de remplacement en cas de non-conformité ou de défaillance du produit.

#### Domaines d’expertise à maîtriser

Le but de ce lot est de fournir aux Pouvoirs locaux wallons une solution complète de sécurité des terminaux qui leur permettra de protéger leurs systèmes contre les menaces en ligne. Cette solution devra être adaptée aux besoins de chaque Pouvoir local et être facilement gérable par leur équipe informatique. En ce sens, le soumissionnaire devra prouver son expertise dans les domaines suivants :

* Expertise en matière de sécurité informatique et de protection contre les menaces informatiques ;
* Connaissance approfondie des produits Antivirus/Antimalware/EDR/XDR, y compris leur fonctionnement et leurs caractéristiques techniques ;
* Compétences en matière de déploiement et de gestion de solutions de sécurité informatique ;
* Expérience en matière de conseil et de mise en place de politiques et de procédures de sécurité informatique ;
* Capacité à fournir un support technique et une formation aux utilisateurs finaux sur l'utilisation des produits Antivirus/Antimalware/EDR/XDR ;
* Connaissance des réglementations et des normes de sécurité informatique pertinents, y compris celles qui s'appliquent aux Pouvoirs locaux wallons ;
* Maîtrise de différentes technologies de protection contre les menaces informatiques, telles que les virus, les logiciels malveillants, les ransomwares, les botnets, etc. ;
* Connaissance approfondie des différents types de logiciels antivirus et antimalware, ainsi que de leurs fonctionnalités et de leur mode de fonctionnement ;
* Expérience dans la mise en place et la gestion de solutions de détection et de réponse avancées (EDR et XDR) dans des environnements informatiques complexes ;
* Capacité à évaluer les besoins en matière de sécurité informatique des Pouvoirs locaux et à recommander des solutions adaptées à leurs exigences ;
* Connaissance des réglementations et des normes en matière de sécurité informatique applicable aux Pouvoirs locaux.

#### Scénario pour compléter l’inventaire

Scénario pour le lot "Antivirus/Antimalware/EDR/XDR" - 200 appareils

Volumétrie et quantités nécessaires :

* 200 licences antivirus/antimalware.
* Tableau de bord interactif
* Formation et documentation pour la gestion au quotidien du système.

Implémentation pratique :

* La solution antivirus/antimalware/EDR/XDR sera déployée sur les appareils de l'infrastructure du pouvoir local, offrant une protection avancée contre les menaces.
* Elle prendra en charge un nombre minimum de 200 appareils, garantissant une protection complète de tous les systèmes utilisés par les utilisateurs.
* La solution utilisera des technologies de pointe pour détecter et bloquer les menaces connues et inconnues en temps réel, réduisant ainsi les risques de compromission des endpoints.
* Les fonctionnalités avancées d'analyse comportementale permettront de détecter les comportements suspects des endpoints, aidant à identifier les attaques avancées et les menaces émergentes.
* En cas d'incident de sécurité, la solution offrira des fonctionnalités de réponse automatisée, telles que l'isolation et la quarantaine des endpoints compromis, permettant de contenir rapidement les attaques et de limiter leur propagation.
* Le référent informatique du pouvoir local sera formé sur l'utilisation basique du tableau de bord pour s’assurer du bon fonctionnement de la solution.
* Un système d’alerte par email sera configuré à destination du dit référent informatique ou du prestataire informatique pour être informé en temps réel de potentiels incidents de sécurité.
* Un tableau de bord centralisé sera mis en place pour la gestion et la surveillance des endpoints, offrant une visibilité complète sur l'état de la sécurité et facilitant la gestion des incidents.

### Lot L5 : Gestion des mots de passe

#### Objectif du lot

Le lot lié aux gestionnaires de mots de passe vise à fournir aux Pouvoirs locaux une solution de gestion et de sécurité des comptes et des accès des utilisateurs. La solution proposée doit être simple à utiliser, fiable et sécurisée, et doit permettre aux Pouvoirs locaux de gérer efficacement les comptes et les accès de leurs utilisateurs, permettre aux utilisateurs de changer et de récupérer facilement leur mot de passe, tout en respectant les politiques de sécurité du Pouvoir local.

#### Caractéristiques spécifiques du lot

Le lot lié aux gestionnaires de mots de passe a pour objectif de mettre en place un système de gestion de la sécurité des mots de passe pour les Pouvoirs locaux wallons. Pour ce faire, le gestionnaire de mot de passe doit posséder les caractéristiques suivantes :

* Gérer les comptes et les accès des utilisateurs de manière sécurisée ;
* Faciliter le changement et la récupération de mots de passe ;
* Gérer les autorisations et les privilèges des utilisateurs de manière fine et granulaire ;
* S'intégrer avec les différents systèmes et applications du Pouvoir local ;
* Imposer l'utilisation de mots de passe forts et complexes.
* Mettre en place un système de gestion de la sécurité des mots de passe : le gestionnaire de mot de passe doit permettre aux Pouvoirs locaux de mettre en place un système de gestion de la sécurité des mots de passe, en utilisant des politiques de sécurité configurables et adaptées aux besoins du Pouvoir local.
* Offrir une interface de gestion simple et intuitive : le gestionnaire de mot de passe doit offrir une interface de gestion simple et intuitive, accessible aux utilisateurs et aux administrateurs du Pouvoir local.
* Prendre en charge les différentes plateformes et environnements de travail : le gestionnaire de mot de passe doit être compatible avec les différentes plateformes et environnements de travail utilisés par le Pouvoir local, et doit permettre la gestion centralisée des mots de passe sur ces différentes plateformes.
* Suivre et auditer les activités de gestion des mots de passe : le gestionnaire de mot de passe doit permettre aux Pouvoirs locaux de suivre et d'auditer les activités de gestion des mots de passe, en fournissant des logs et des journaux détaillés des opérations effectuées.
* Offrir une prise en charge en français : le gestionnaire de mot de passe doit être capable de prendre en charge le français, afin de pouvoir être utilisé par les utilisateurs des Pouvoirs locaux de Wallonie.

#### Spécificités techniques

Le lot de gestionnaire de mots de passe proposé par les soumissionnaires doit répondre aux exigences minimales énoncées ci-dessous. Si le soumissionnaire ne satisfait pas aux exigences minimales requises, il sera éliminé de la compétition. Les soumissionnaires doivent décrire clairement comment ils satisfont à chacune des exigences. Une simple déclaration du soumissionnaire affirmant qu'il peut/va le faire ou une réitération des exigences du marché n'est PAS suffisante à cet égard.

Les spécificités techniques sont les suivantes :

* Prise en charge de plusieurs domaines et de plusieurs annuaires d'utilisateurs, pour permettre la gestion centralisée des mots de passe de différents services et systèmes ;
* Prise en charge de plusieurs protocoles d'authentification, tels que LDAP, SAML, OAuth, RADIUS, etc., pour permettre l'intégration avec un large éventail de systèmes et d'applications ;
* Prise en charge de plusieurs plates-formes et de plusieurs systèmes d'exploitation, tels que Windows, Linux, MacOS, iOS, Android, etc., pour permettre l'utilisation sur un large éventail de dispositifs et d'environnements ;
* Prise en charge de la synchronisation des mots de passe avec les applications et les systèmes tiers, pour permettre la gestion centralisée et la synchronisation des mots de passe entre différents services et systèmes ;
* Prise en charge de l'authentification à deux facteurs et de l'authentification forte, pour renforcer la sécurité des mots de passe et éviter les attaques de type man-in-the-middle ;
* Prise en charge de la récupération des mots de passe oubliés et de la gestion des questions de sécurité, pour permettre aux utilisateurs de récupérer facilement leur mot de passe en cas d'oubli ;
* Prise en charge de la gestion fine et granulaire des autorisations et des privilèges des utilisateurs, en utilisant des rôles et des groupes d'utilisateurs personnalisables ;
* Prise en charge de la gestion de la politique de sécurité des mots de passe, en imposant des règles de complexité et de rotation des mots de passe, et en alertant les utilisateurs et les administrateurs en cas de violations de ces règles ;
* Prise en charge de la gestion de la durée de vie des mots de passe, en imposant des délais de renouvellement et de validité des mots de passe, et en alertant les utilisateurs et les administrateurs en cas d’expiration prochaine ;
* Prise en charge de la gestion des autorisations d'accès et des privilèges des utilisateurs, en permettant l'attribution et la révocation de droits et de permissions en fonction de l'identité de l'utilisateur et de son rôle dans l'organisation ;
* Prise en charge de la gestion de la sécurité des sessions et des connexions, en permettant la déconnexion et la terminaison des sessions inactives et en protégeant les communications de bout en bout contre les attaques de type man-in-the-middle ;
* Prise en charge de la gestion de la sécurité des événements et des journaux, en permettant la collecte, l'analyse et l'alerte sur les événements de sécurité pertinents, tels que les tentatives d'accès non autorisées, les changements de configuration, les violations de politique, etc. ;
* Prise en charge de la gestion de la sécurité des mots de passe dans les bases de données et les systèmes de gestion de données, en utilisant des méthodes de hachage et de chiffrement robustes pour protéger les mots de passe en base de données ;
* Prise en charge de la gestion de la sécurité des mots de passe dans les environnements cloud et distribués, en utilisant des méthodes de synchronisation et de réplication sécurisées pour protéger les mots de passe dans les différentes instances et régions cloud ;
* Prise en charge de la gestion de la sécurité des mots de passe dans les environnements hybrides, en permettant l'intégration et la synchronisation des mots de passe avec les annuaires d'utilisateurs on-premise et cloud.

#### Rapport et documentations

Le lot de gestionnaire de mots de passe est un élément clé de la sécurité informatique des Pouvoirs locaux wallons. Il est donc important que les soumissionnaires présentent une solution complète et détaillée répondant aux besoins et aux exigences de ces organisations. Pour évaluer les offres de manière objective et juste, nous vous demandons de fournir les rapports et documentations suivants :

* Une présentation détaillée du produit ou de la solution proposée, y compris des informations sur les caractéristiques clés, les fonctionnalités, les avantages et les bénéfices pour les utilisateurs ;
* Un guide de l'utilisateur décrivant les étapes de configuration, de déploiement et d'utilisation du gestionnaire de mots de passe ;
* Un manuel de l'administrateur contenant des informations sur la gestion et la maintenance du système, y compris la gestion des utilisateurs, la gestion des politiques de sécurité et la résolution des problèmes ;
* Un historique de mise à jour du produit ou de la solution, y compris les versions et les correctifs de sécurité publiés ;
* Des preuves de conformité avec les normes et les réglementations pertinentes, par exemple en matière de protection de la vie privée et de la sécurité des données personnelles ;
* Des références de clients et d'utilisateurs satisfaits, avec des témoignages et des cas d'étude décrivant l'utilisation et les résultats obtenus avec le gestionnaire de mots de passe ;
* Une garantie et un plan de support technique, décrivant les modalités d’assistance et de maintenance proposés par le soumissionnaire ;
* Un résumé de la stratégie de sécurité du produit ou de la solution, y compris les mesures de sécurité incluses et les protections proposées contre les menaces courantes (par exemple, les attaques de phishing, les tentatives de piratage, les violations de données, etc.) ;
* Un aperçu des outils et des fonctionnalités de gestion et de rapport proposés par le gestionnaire de mots de passe, permettant aux administrateurs de suivre l'utilisation et les performances du système, d'identifier les éventuels problèmes et de générer des rapports de sécurité ;
* Des détails sur la scalabilité et la flexibilité du produit ou de la solution, y compris les options de déploiement et de configuration disponibles pour répondre aux besoins et aux exigences spécifiques des Pouvoirs locaux wallons ;
* Une estimation des coûts d'acquisition, de déploiement et de maintenance du gestionnaire de mots de passe, ainsi que les modalités de facturation proposées par le soumissionnaire (par exemple, coût unique, abonnement, modèle de licences en volume, etc.) ;
* Un plan de migration et de mise en œuvre du gestionnaire de mots de passe, décrivant les étapes et les ressources nécessaires pour mettre en place la solution proposée dans les Pouvoirs locaux wallons ;
* Une liste des principaux intégrateurs et partenaires du soumissionnaire, avec des informations sur leur expérience et leur expertise en matière de gestionnaire.

#### Obligation de résultats

Pour assurer le succès du projet de mise à disposition d'un gestionnaire de mot de passe pour les Pouvoirs locaux wallons, il est important de définir clairement les obligations de résultats attendues des soumissionnaires. Les soumissionnaires doivent être en mesure de :

* Mettre en place un système de gestion de mots de passe qui réponde aux normes de sécurité en vigueur et qui soit efficace dans l'aide à la gestion des mots de passe de l'ensemble des utilisateurs du Pouvoir local ;
* Former le personnel du Pouvoir local sur l'utilisation du gestionnaire de mot de passe et sur les bonnes pratiques de gestion de mots de passe ;
* Assurer une assistance technique et une maintenance du système de gestion de mots de passe, avec un temps de réponse garanti en cas de problème ;
* Mettre à disposition de guides de l'utilisateur et de documentations techniques détaillées sur le fonctionnement du gestionnaire de mot de passe ;
* Mettre en place un système de rapport pour suivre l'utilisation du gestionnaire de mot de passe et détecter tout problème éventuel ;
* Mettre en place des procédures de sauvegarde et de restauration du système de gestion de mots de passe en cas de panne ou de dysfonctionnement ;
* Respect des normes de sécurité en vigueur dans le domaine, telles que NIST SP 800-63-3 et ISO 27001 ;
* Mise en place de processus de gestion de la sécurité des mots de passe efficaces et adaptés aux besoins du Pouvoir local ;
* Mise à disposition de fonctionnalités de gestion des utilisateurs, telles que la gestion des droits d'accès, la réinitialisation des mots de passe, etc. ;
* Mise en place de fonctionnalités de rapport et de suivi permettant de mesurer l'efficacité de la gestion des mots de passe et d'identifier les éventuels problèmes de sécurité ;
* Mise en place de fonctionnalités de sécurité avancées, telles que la protection contre les attaques de type "brute force" ou la détection des comportements anormaux d'accès ;
* Mise à disposition de mécanismes de sauvegarde et de restauration permettant de protéger les données de gestion des mots de passe en cas de sinistre.

#### Domaines d’expertise à maîtriser

Le soumissionnaire doit démontrer une expertise solide et une expérience pratique dans les domaines clés suivants liés à la mise à disposition de solutions de gestion de mots de passe pour les Pouvoirs locaux wallons.

Le soumissionnaire devra prouver de sa capacité d’expertise sur les domaines suivants :

* Gestion de la sécurité des mots de passe et des autorisations d'accès, avec une connaissance approfondie des standards et des bonnes pratiques en la matière ;
* Déploiement et gestion de solutions de gestion de mots de passe dans les environnements cloud et hybrides, avec une connaissance approfondie des architectures et des technologies cloud ;
* Intégration et synchronisation de solutions de gestion de mots de passe avec les annuaires d'utilisateurs et les systèmes d'authentification existants ;
* Support et maintenance de solutions de gestion de mots de passe, avec une capacité à résoudre rapidement les problèmes et à fournir un niveau élevé de disponibilité ;
* Formation et sensibilisation des utilisateurs aux bonnes pratiques de gestion de mots de passe et de sécurité informatique en général ;
* Développement et personnalisation de solutions de gestion de mots de passe, avec une capacité à adapter les fonctionnalités et l'interface utilisateur aux besoins spécifiques de l'organisation ;
* Conformité et réglementation en matière de gestion de mots de passe et de sécurité des données, avec une connaissance approfondie des réglementations et des normes en vigueur dans le domaine ;
* Gestion de la politique de sécurité des mots de passe, avec une capacité à définir et à mettre en œuvre des règles de sécurité strictes pour la création et l'utilisation de mots de passe ;
* Protection des mots de passe contre les attaques de type "force brute" et autres techniques de piratage ;
* Intégration de solutions de gestion de mots de passe avec les outils de gestion de la sécurité de l'information et de l'identité (par exemple, gestionnaire de stratégies de sécurité, gestionnaire d'identités et d'accès, etc.) ;
* Mécanismes de récupération de mots de passe en cas d'oubli ou de perte ;
* Prise en charge de l'authentification à deux facteurs ou multi facteurs pour renforcer la sécurité de l'accès aux systèmes et aux données ;
* Gestion de la vie privée et de la protection des données personnelles dans le cadre de la gestion de mots de passe, conformément aux réglementations en vigueur ;
* Expérience de travail avec les Pouvoirs locaux wallons et connaissance des spécificités et des exigences de cet environnement.

#### Scénario pour compléter l’inventaire

Scénario pour le lot "Gestion des mots de passe" - Solution de gestion centralisée :

Volumétrie et quantités nécessaires :

* 100 licences utilisateurs pour la gestion des mots de passe.
* Tableau de bord interactif.
* Formation et documentation pour la gestion au quotidien du système.

Implémentation pratique :

* La solution de gestion des mots de passe sera déployée au sein de l'infrastructure du pouvoir local, offrant une gestion centralisée des comptes et des mots de passe.
* Elle prendra en charge un nombre minimum de 100 utilisateurs, permettant de couvrir les besoins actuels et futurs en matière de gestion des mots de passe.
* Les fonctionnalités de création, de stockage et de gestion sécurisée des mots de passe permettront aux utilisateurs de générer des mots de passe robustes et de les stocker en toute sécurité.
* La solution offrira également la possibilité d'utiliser l'authentification à deux facteurs pour renforcer la sécurité des comptes.
* Elle sera intégrée de manière transparente avec les systèmes existants de l'infrastructure du pouvoir local, garantissant une gestion efficace des mots de passe sans perturber les opérations quotidiennes.
* Le référent informatique du pouvoir local sera formé sur le panel d’administration centrale du système de gestion de mots de passe pour assurer le suivi quotidien (arrivé/départ/réinitiation des mots de passe).
* Les utilisateurs seront formés sur l'utilisation de la solution de gestion des mots de passe et sur les bonnes pratiques en matière de sécurité des mots de passe.

## Dispositions de fin de marché et de réversibilité

### Clause de réversibilité

La réversibilité désigne l’opération de retour de responsabilité technique, par lequel iMio reprend tout ou partie des prestations qu’il avait confié au titulaire du marché, quelle qu’en soit la raison, arrivant à terme, ou avant son terme suivant un délai de prévenance de minimum trois mois à réception de la notification du lancement de la réversibilité, par envoi d'un courrier recommandé avec AR au titulaire du marché.

La période de réversibilité est la période couvrant le retour de responsabilité ci-avant mentionné.

Quelle que soit la cause de la fin prévue ou anticipée du présent accord-cadre, le titulaire s’engage à réaliser l’ensemble des activités nécessaires à la réversibilité. Il coopère avec iMio afin que cette réversibilité de marché s’effectue de façon que les prestations objet de l’accord-cadre puissent être poursuivies sans interruption et dans le respect des engagements, résultats et indicateurs prévus au marché.

La réversibilité peut être totale ou partielle, suivant besoin du Pouvoir local. Elle concerne tout ou partie des services, matériels, logiciels, données et livrables relatifs aux prestations réalisées.

Un plan de réversibilité exposant les tâches respectives à accomplir par chacune des parties ainsi que le planning détaillé de cette phase est établi, dans les trois semaines suivant la réception par le Titulaire de la notification envoyée par iMio, et validé par iMio.

Ce plan détaillera en particulier les mesures encadrant la réversibilité des activités, de compétence et la remise des différents documents.

Les coûts de la réversibilité sont à la charge du titulaire au titre des forfaits du bordereau des prix.

La réversibilité est totale. Elle concerne les développements et paramétrages spécifiques, la documentation relative aux prestations réalisées, la reprise des données clients iMio.

Le titulaire s'engage notamment à :

* Organiser une réunion de kick off au plus tard dans le mois suivant la réception de la notification, avec les interlocuteurs désignés par iMio,
* Remettre tous les documents mis à jour par le titulaire et relatifs aux prestations réalisées et à leur suivi dans le cadre du marché au plus tard un mois avant la mise en œuvre de la réversibilité, selon les « standards du marché »
* Remettre tous les documents archivés dans le cadre du marché au plus tard un mois après la fin de la réversibilité, selon les standards du marché,
* Répondre aux questions d’iMio dans un délai maximum de 48 heures, au moyen d’un espace d'échange proposé par le titulaire et validé par iMio durant toute la phase de réversibilité,
* Le Titulaire devra réaliser la prestation dans un objectif de qualité, conformément au présent marché, jusqu’à la date de fin de marché prévue ou anticipée,
* Remettre les paramétrages et les développements spécifiques réalisés durant toute la durée du marché,
* Assurer un transfert de compétence approfondie nécessaire au personnel d’iMio, permettant la reprise de l'activité et s'appuyant sur les documentations utilisateurs et techniques mise à jour et rédigées par le titulaire,
* Prévoir d'accueillir un mois avant la réversibilité et durant deux semaines, un maximum de trois représentants maximum d’iMio, afin de leur permettre d'observer l'activité de l'équipe en place,
* Assurer une parfaite et complète reprise des données, propriété d’iMio.

La mise à disposition de fichiers se fera suivant un ou plusieurs formats documentés et exploitables en dehors du service fourni par le prestataire.

Des interfaces techniques permettant l’accès aux données suivant un schéma documenté et exploitable (API, format pivot, etc.) seront prévues par le titulaire, voire la possibilité pour iMio de télécharger lui-même ses données ou encore d’utiliser une interface applicative de programmation (API) afin de permettre une migration automatisée vers une solution tierce.

Les dispositions de fin de marché étant réalisées, le titulaire s'engage pendant une durée et selon les conditions définies dans le plan de réversibilité, à maintenir disponible les compétences nécessaires pour assister iMio, dans la reprise des prestations. Pendant cette période, le titulaire s'engage également à répondre aux demandes d'assistance d’iMio dans les meilleurs délais.

Un PV de fin de phase de réversibilité valide la fin de ladite phase par le titulaire et iMio. En cas de non-conformité, de non-réception de tout ou partie des livrables, de non-respect des délais ou des prestations convenues par la présente clause, un allongement de la période de réversibilité sera appliqué à la charge et aux frais du titulaire du marché.

### Clause de transférabilité

La transférabilité désigne l’opération de transfert de responsabilité technique, par lequel iMio fait reprendre par un nouveau titulaire tout ou partie des prestations qu’il avait confiés au titulaire du marché, quelle qu’en soit la raison, arrivant à terme, ou avant son terme suivant un délai de prévenance de minimum trois mois à réception de la notification du lancement de la transférabilité, par envoi d'un courrier recommandé avec AR au titulaire du marché.

La période de transférabilité est la période couvrant le transfert de responsabilité ci-avant mentionné.

Les coûts de la transférabilité sont à la charge du titulaire.

La transférabilité est totale. Elle concerne les développements et paramétrages spécifiques, la documentation relative aux prestations réalisées, la reprise des données clients iMio.

Quelle que soit la cause de la fin prévue ou anticipée du présent accord-cadre, le titulaire s’engage à réaliser l’ensemble des activités nécessaires à la transférabilité. Il coopère avec iMio ainsi que le nouveau titulaire afin que cette transférabilité de marché s’effectue de façon que les prestations objet de l’accord-cadre puissent être poursuivies sans interruption et dans le respect des engagements, résultats et indicateurs prévus au marché.

La transférabilité peut être totale ou partielle, suivant besoin du Pouvoir local. Elle concerne tout ou partie des services, matériels, logiciels, données et livrables relatifs aux prestations réalisées.

Un plan de transférabilité adapté aux clauses du marché du nouveau titulaire et exposant les tâches respectives à accomplir par chacune des parties ainsi que le planning détaillé de cette phase est établi, dans les trois semaines suivant la réception par le Titulaire de la notification envoyée par iMio, et validé par iMio.

Ce plan détaillera en particulier les mesures encadrant le transfert des activités, le transfert de compétence et le transfert des différents documents vers le nouveau titulaire.

Le titulaire s'engage notamment à :

* Organiser une réunion de kick off au plus tard dans le mois suivant la réception de la notification, avec les interlocuteurs désignés par le nouveau titulaire et iMio,
* Transférer tous les documents mis à jour par le titulaire et relatifs aux prestations réalisées et à leur suivi dans le cadre du marché au plus tard un mois avant la mise en œuvre de la transférabilité, selon les « standards du marché ».
* Transmettre tous les documents archivés dans le cadre du marché au plus tard un mois avant la fin de la transférabilité, selon les standards du marché,
* Répondre aux questions du nouveau titulaire ou de iMio dans un délai maximum de 48 heures, au moyen d’un espace d'échange proposé par le titulaire et validé par le nouveau titulaire et iMio durant toute la phase de transférabilité,
* Le Titulaire devra réaliser la prestation dans un objectif de qualité, conformément au présent marché, jusqu’à la date de fin de marché prévue ou anticipée,
* Transmettre les paramétrages et les développements spécifiques réalisés durant toute la durée du marché,
* Assurer un transfert de compétence approfondie nécessaire au personnel du nouveau titulaire, permettant la reprise de l'activité et s'appuyant sur les documentations utilisateurs et techniques mise à jour et rédigées par le titulaire du présent marché,
* Prévoir d'accueillir un mois avant la transférabilité et durant deux semaines, un maximum de trois représentants maximums du nouveau titulaire, afin de leur permettre d'observer l'activité de l'équipe en place,
* Assurer un parfait et complet transfert des données (propriété de Pouvoir local) vers le nouveau titulaire.

La mise à disposition de fichiers se fera suivant un ou plusieurs formats documentés et exploitables en dehors du service fourni par le prestataire.

Des interfaces techniques permettant l’accès aux données suivant un schéma documenté et exploitable (API, format pivot, etc.) seront prévues par le titulaire et en accord avec le nouveau Titulaire, voire la possibilité de télécharger lui-même ses données ou encore d’utiliser une interface applicative de programmation (API) afin de permettre une migration automatisée vers une solution tierce.

Les dispositions de fin de marché étant réalisées, le titulaire s'engage pendant une durée et selon les conditions définies dans le plan de transférabilité, à maintenir disponible les compétences nécessaires pour assister le nouveau titulaire, dans la reprise des prestations. Pendant cette période, le titulaire s'engage également à répondre aux demandes d'assistance du nouveau titulaire dans les meilleurs délais.

1. **FORMULAIRE D’OFFRE**

OFFRE DE PRIX POUR LE MARCHE AYANT POUR OBJET  
“ FOURNITURE ET MAINTENANCE DE MATÉRIELS ET LOGICIELS RELATIFS À LA CYBERSÉCURITÉ ”

Procédure ouverte

Important : ce formulaire doit être complété dans son entièreté. Le montant total de l’offre doit être complété en chiffres ET en toutes lettres.

Personne physique  
Le soussigné (nom et prénom) :  
Qualité ou profession :  
Nationalité :  
Domicile (adresse complète) :

Téléphone :  
GSM :  
Fax :  
E-mail :  
Personne de contact :

**Soit (1)**

Personne morale  
La firme (dénomination, raison sociale) :  
Nationalité :  
ayant son siège à (adresse complète) :

Téléphone :  
GSM :  
Fax :  
E-mail :  
Personne de contact :

Représentée par le(s) soussigné(s) :  
(Les mandataires joignent à leur offre l’acte authentique ou sous seing privé qui leur accorde ses pouvoirs ou une copie de la procuration. Ils peuvent se borner à indiquer le numéro de l’annexe du Moniteur belge qui a publié l’extrait de l’acte concerné.)

**Soit (1)**

Groupement d’opérateurs économiques (y compris la société momentanée)  
  
Nom et prénom ou raison sociale des soumissionnaires et forme juridique :

Qualité ou profession :

Nationalité :

Adresse ou siège social :

Téléphone :

GSM :

E-mail :

Personne de contact :

Nom et prénom ou raison sociale des soumissionnaires et forme juridique :

Qualité ou profession :

Nationalité :

Adresse ou siège social :

Téléphone :

GSM :

E-mail :

Personne de contact :

Ces données doivent être complétées pour chacun des participants au groupement.

Le groupement est représenté par l’un des participants, dont le nom est :

S’ENGAGE(NT) À EXÉCUTER LE MARCHÉ CONFORMÉMENT AUX CLAUSES ET CONDITIONS DU CAHIER DES CHARGES DU MARCHÉ PUBLIC SUSMENTIONNÉ (PO/001/2023/MAT) :

**Lot M1 : Produit MFA**

pour un montant de :

(en chiffres, TVA comprise)

…................................................................................................................................................

(en lettres, TVA comprise)

…................................................................................................................................................

…................................................................................................................................................

**Lot M2 : pare-feu**

pour un montant de :

(en chiffres, TVA comprise)

…................................................................................................................................................

(en lettres, TVA comprise)

…................................................................................................................................................

…................................................................................................................................................

**Lot M3 : Sauvegarde des données sécurisées**

pour un montant de :

(en chiffres, TVA comprise)

…................................................................................................................................................

(en lettres, TVA comprise)

…................................................................................................................................................

…................................................................................................................................................

**Lot L1 : Journalisation des événements**

pour un montant de :

(en chiffres, TVA comprise)

…................................................................................................................................................

(en lettres, TVA comprise)

…................................................................................................................................................

…................................................................................................................................................

**Lot L2 : Projets liés au management de l’authentification et à l’identification numérique**

pour un montant de :

(en chiffres, TVA comprise)

…................................................................................................................................................

(en lettres, TVA comprise)

…................................................................................................................................................

…................................................................................................................................................

**Lot L3 : Filtrage des messages électroniques**

pour un montant de :

(en chiffres, TVA comprise)

…................................................................................................................................................

(en lettres, TVA comprise)

…................................................................................................................................................

…................................................................................................................................................

**Lot L4 Antivirus/antimalware/EDR/XDR**pour un montant de :

(en chiffres, TVA comprise)

…................................................................................................................................................

(en lettres, TVA comprise)

…................................................................................................................................................

…................................................................................................................................................

**Lot L5 : Gestion des mots de passe**

pour un montant de :

(en chiffres, TVA comprise)

…................................................................................................................................................

(en lettres, TVA comprise)

…................................................................................................................................................

…................................................................................................................................................

Informations générales

Numéro d’immatriculation à l’ONSS :  
Numéro d’entreprise (en Belgique uniquement) :  
Le soumissionnaire est une micro-, petite ou moyenne entreprise : OUI / NON (biffer les mentions inutiles) **(2)**

Sous-traitants

Il sera fait appel à des sous-traitants : OUI / NON (biffer les mentions inutiles)

Personnel

Du personnel soumis à la législation sociale d’un autre pays membre de l’Union européenne est employé :

OUI / NON (biffer les mentions inutiles)

Cela concerne le pays membre de l’UE suivant :

Paiements

Les paiements seront effectués valablement par virement ou versement sur le compte (IBAN/BIC) …............................................. de l’institution financière ….............................. ouvert au nom de ….............................. .

Attestations

A cette offre je joins/nous joignons :  
Le DUME, par lequel l’opérateur économique déclare qu’il ne se trouve pas dans une des situations d’exclusion visées aux articles 67 à 69 de la loi du 17 juin 2016.

Documents à joindre à l’offre

À cette offre, sont joints :

- les documents que le cahier des charges impose de fournir ;

- les modèles, échantillons et autres informations, que le cahier des charges impose de fournir.

À savoir :

* Le(s) DUME(s)
* Annexe A : le formulaire d’offre
* Annexe B : Inventaire (s)
* Annexe C : Bordereau(x) de réponse technique
* Annexe G : Engagements sur l’Obligation de résultats
* Un document récapitulatif de l’offre de service proposée ainsi qu’une présentation de la société ;
* Les curriculums vitae des personnes les identifiant de manière unique (Cfr liste expert annexe C)
* Les fiches produits/logiciels des fabricants/éditeurs proposés
* Toute(s) autre(s) annexe(s) nécessaire(s) à la bonne complétion du dossier

Fait à …........................................................................................................................................

Le ….............................................................................................................................................

Le soumissionnaire,

Nom et prénom : ….......................................................................................................................

Fonction : …..................................................................................................................................

Note importante

Les soumissionnaires ne peuvent se prévaloir des vices de forme dont est entachée leur offre, ni des erreurs ou omissions qu’elle comporte (article 82 de l’arrêté royal du 18 avril 2017).

* + - 1. **Biffer les mentions inutiles**

**(2)** Au sens de la recommandation de la Commission Européenne du 6 mai 2013 concernant la définition des micro-, petites et moyennes entreprises.

Microentreprise : Entreprise qui occupe moins de 10 personnes et dont le chiffre d’affaire annuel ou le total du bilan annuel n’excède pas 2 millions d’euros.

Petite entreprise : Entreprise qui occupe moins de 50 personnes et dont le chiffre d’affaire annuel ou le total du bilan annuel n’excède pas 10 millions d’euros.

Moyenne entreprise : Entreprise qui n’est ni une micro- ni une petite entreprise et qui occupe moins de 250 personnes et dont le chiffre d’affaire annuel n’excède pas 50 millions d’euros et/ou le total du bilan annuel ne dépasse pas 43 millions d’euros.

1. **INVENTAIRE**

**“** **FOURNITURE ET MAINTENANCE DE MATÉRIELS ET LOGICIELS RELATIFS À LA CYBERSÉCURITÉ ”**

Lot M1 : Produit MFA

| N° | Description | Type | Unité | Q | PU en chiffres HTVA | Total HTVA |
| --- | --- | --- | --- | --- | --- | --- |
| 1 | À adapter | QP | forfait | 1 |  |  |
| 2 |  | QP | Annuel | 1 |  |  |
| 3 |  | QP | Licence | 1 |  |  |
| 4 |  | QP | Boitier | 1 |  |  |
| 5 |  | QP | Jour-homme | 1 |  |  |
| 6 |  | QP | Etc. | 1 |  |  |
| Etc. |  | QP | À adapter | 1 |  |  |
| Total lot M1 HTVA : | | | | | |  |
| TVA 21% : | | | | | |  |
| Total lot M1 TVAC : | | | | | |  |

|  |
| --- |
| *Les prix unitaires doivent être mentionnés avec 2 chiffres après la virgule. La quantité de produits x le prix unitaire doivent être à chaque fois arrondis à 2 chiffres après la virgule.* |
| Vu, vérifié et complété avec les prix unitaires, les totaux partiels et le total global qui ont servi à déterminer le montant de mon offre de ce jour, pour être joint à mon formulaire d’offre.  Fait à …....................................... le …................................................... Fonction : …...................................................  Nom et prénom : …................................................................. |

Lot M1 : Produit MFA – mise en application de l’inventaire du lot selon le scénario opérationnel

| **N°** | **Description** | **Type** | **Unité** | **Q** | **PU en chiffres HTVA** | **Total HTVA** |
| --- | --- | --- | --- | --- | --- | --- |
| 1 | À reprendre du tableau initial du lot | QP | forfait | 1 |  |  |
| 2 |  | QP | Annuel | 1 |  |  |
| 3 |  | QP | Licence | 1 |  |  |
| 4 |  | QP | Boitier | 1 |  |  |
| 5 |  | QP | Jour-homme | 1 |  |  |
| 6 |  | QP | Etc. | 1 |  |  |
| Etc. |  | QP | À adapter | 1 |  |  |
| **Total lot M1 HTVA :** | | | | | |  |
| **TVA 21% :** | | | | | |  |
| **Total lot M1 TVAC :** | | | | | |  |

|  |
| --- |
| *Les prix unitaires doivent être mentionnés avec 2 chiffres après la virgule. La quantité de produits x le prix unitaire doivent être à chaque fois arrondis à 2 chiffres après la virgule.* |
| Vu, vérifié et complété avec les prix unitaires, les totaux partiels et le total global qui ont servi à déterminer le montant de mon offre de ce jour, pour être joint à mon formulaire d’offre.  Fait à …....................................... le …................................................... Fonction : …...................................................  Nom et prénom : …................................................................. |

**“** **FOURNITURE ET MAINTENANCE DE MATÉRIELS ET LOGICIELS RELATIFS À LA CYBERSÉCURITÉ ”**

Lot M2 : Pare-feu

| **N°** | **Description** | **Type** | **Unité** | **Q** | **PU en chiffres HTVA** | **Total HTVA** |
| --- | --- | --- | --- | --- | --- | --- |
| 1 | À adapter | QP | forfait | 1 |  |  |
| 2 |  | QP | Annuel | 1 |  |  |
| 3 |  | QP | Licence | 1 |  |  |
| 4 |  | QP | Boitier | 1 |  |  |
| 5 |  | QP | Jour-homme | 1 |  |  |
| 6 |  | QP | Etc. | 1 |  |  |
| Etc. |  | QP | À adapter | 1 |  |  |
| **Total lot M2 HTVA :** | | | | | |  |
| **TVA 21% :** | | | | | |  |
| **Total lot M2 TVAC :** | | | | | |  |

|  |
| --- |
| *Les prix unitaires doivent être mentionnés avec 2 chiffres après la virgule. La quantité de produits x le prix unitaire doivent être à chaque fois arrondis à 2 chiffres après la virgule.* |
| Vu, vérifié et complété avec les prix unitaires, les totaux partiels et le total global qui ont servi à déterminer le montant de mon offre de ce jour, pour être joint à mon formulaire d’offre.  Fait à …....................................... le …................................................... Fonction : …...................................................  Nom et prénom : …................................................................. |

Lot M2 : Pare-feu – mise en application de l’inventaire du lot selon le scénario opérationnel

| **N°** | **Description** | **Type** | **Unité** | **Q** | **PU en chiffres HTVA** | **Total HTVA** |
| --- | --- | --- | --- | --- | --- | --- |
| 1 | À reprendre du tableau initial du lot | QP | forfait | 1 |  |  |
| 2 |  | QP | Annuel | 1 |  |  |
| 3 |  | QP | Licence | 1 |  |  |
| 4 |  | QP | Boitier | 1 |  |  |
| 5 |  | QP | Jour-homme | 1 |  |  |
| 6 |  | QP | Etc. | 1 |  |  |
| Etc. |  | QP | À adapter | 1 |  |  |
| **Total lot M2 HTVA :** | | | | | |  |
| **TVA 21% :** | | | | | |  |
| **Total lot M2 TVAC :** | | | | | |  |

|  |
| --- |
| *Les prix unitaires doivent être mentionnés avec 2 chiffres après la virgule. La quantité de produits x le prix unitaire doivent être à chaque fois arrondis à 2 chiffres après la virgule.* |
| Vu, vérifié et complété avec les prix unitaires, les totaux partiels et le total global qui ont servi à déterminer le montant de mon offre de ce jour, pour être joint à mon formulaire d’offre.  Fait à …....................................... le …................................................... Fonction : …...................................................  Nom et prénom : …................................................................. |

**“** **FOURNITURE ET MAINTENANCE DE MATÉRIELS ET LOGICIELS RELATIFS À LA CYBERSÉCURITÉ ”**

Lot M3 : Sauvegardes sécurisées de données

| **N°** | **Description** | **Type** | **Unité** | **Q** | **PU en chiffres HTVA** | **Total HTVA** |
| --- | --- | --- | --- | --- | --- | --- |
| 1 | À adapter | QP | forfait | 1 |  |  |
| 2 |  | QP | Annuel | 1 |  |  |
| 3 |  | QP | Licence | 1 |  |  |
| 4 |  | QP | Boitier | 1 |  |  |
| 5 |  | QP | Jour-homme | 1 |  |  |
| 6 |  | QP | Etc. | 1 |  |  |
| Etc. |  | QP | À adapter | 1 |  |  |
| **Total lot M3 HTVA :** | | | | | |  |
| **TVA 21% :** | | | | | |  |
| **Total lot M3 TVAC :** | | | | | |  |

|  |
| --- |
| *Les prix unitaires doivent être mentionnés avec 2 chiffres après la virgule. La quantité de produits x le prix unitaire doivent être à chaque fois arrondis à 2 chiffres après la virgule.* |
| Vu, vérifié et complété avec les prix unitaires, les totaux partiels et le total global qui ont servi à déterminer le montant de mon offre de ce jour, pour être joint à mon formulaire d’offre.  Fait à …....................................... le …................................................... Fonction : …...................................................  Nom et prénom : …................................................................. |

Lot M3 : Sauvegardes sécurisées de données – mise en application de l’inventaire du lot selon le scénario opérationnel

| **N°** | **Description** | **Type** | **Unité** | **Q** | **PU en chiffres HTVA** | **Total HTVA** |
| --- | --- | --- | --- | --- | --- | --- |
| 1 | À reprendre du tableau initial du lot | QP | forfait | 1 |  |  |
| 2 |  | QP | Annuel | 1 |  |  |
| 3 |  | QP | Licence | 1 |  |  |
| 4 |  | QP | Boitier | 1 |  |  |
| 5 |  | QP | Jour-homme | 1 |  |  |
| 6 |  | QP | Etc. | 1 |  |  |
| Etc. |  | QP | À adapter | 1 |  |  |
| **Total lot M3 HTVA :** | | | | | |  |
| **TVA 21% :** | | | | | |  |
| **Total lot M3 TVAC :** | | | | | |  |

|  |
| --- |
| *Les prix unitaires doivent être mentionnés avec 2 chiffres après la virgule. La quantité de produits x le prix unitaire doivent être à chaque fois arrondis à 2 chiffres après la virgule.* |
| Vu, vérifié et complété avec les prix unitaires, les totaux partiels et le total global qui ont servi à déterminer le montant de mon offre de ce jour, pour être joint à mon formulaire d’offre.  Fait à …....................................... le …................................................... Fonction : …...................................................  Nom et prénom : …................................................................. |

**“** **FOURNITURE ET MAINTENANCE DE MATÉRIELS ET LOGICIELS RELATIFS À LA CYBERSÉCURITÉ ”**

Lot L1 : Journalisation des événements

| **N°** | **Description** | **Type** | **Unité** | **Q** | **PU en chiffres HTVA** | **Total HTVA** |
| --- | --- | --- | --- | --- | --- | --- |
| 1 | À adapter | QP | forfait | 1 |  |  |
| 2 |  | QP | Annuel | 1 |  |  |
| 3 |  | QP | Licence | 1 |  |  |
| 4 |  | QP | Boitier | 1 |  |  |
| 5 |  | QP | Jour-homme | 1 |  |  |
| 6 |  | QP | Etc. | 1 |  |  |
| Etc. |  | QP | À adapter | 1 |  |  |
| **Total lot L1 HTVA :** | | | | | |  |
| **TVA 21% :** | | | | | |  |
| **Total lot L1 TVAC :** | | | | | |  |

|  |
| --- |
| *Les prix unitaires doivent être mentionnés avec 2 chiffres après la virgule. La quantité de produits x le prix unitaire doivent être à chaque fois arrondis à 2 chiffres après la virgule.* |
| Vu, vérifié et complété avec les prix unitaires, les totaux partiels et le total global qui ont servi à déterminer le montant de mon offre de ce jour, pour être joint à mon formulaire d’offre.  Fait à …....................................... le …................................................... Fonction : …...................................................  Nom et prénom : …................................................................. |

Lot L1 : Journalisation des événements – mise en application de l’inventaire du lot selon le scénario opérationnel

| **N°** | **Description** | **Type** | **Unité** | **Q** | **PU en chiffres HTVA** | **Total HTVA** |
| --- | --- | --- | --- | --- | --- | --- |
| 1 | À reprendre du tableau initial du lot | QP | forfait | 1 |  |  |
| 2 |  | QP | Annuel | 1 |  |  |
| 3 |  | QP | Licence | 1 |  |  |
| 4 |  | QP | Boitier | 1 |  |  |
| 5 |  | QP | Jour-homme | 1 |  |  |
| 6 |  | QP | Etc. | 1 |  |  |
| Etc. |  | QP | À adapter | 1 |  |  |
| **Total lot L1 HTVA :** | | | | | |  |
| **TVA 21% :** | | | | | |  |
| **Total lot L1 TVAC :** | | | | | |  |

|  |
| --- |
| *Les prix unitaires doivent être mentionnés avec 2 chiffres après la virgule. La quantité de produits x le prix unitaire doivent être à chaque fois arrondis à 2 chiffres après la virgule.* |
| Vu, vérifié et complété avec les prix unitaires, les totaux partiels et le total global qui ont servi à déterminer le montant de mon offre de ce jour, pour être joint à mon formulaire d’offre.  Fait à …....................................... le …................................................... Fonction : …...................................................  Nom et prénom : …................................................................. |

**“** **FOURNITURE ET MAINTENANCE DE MATÉRIELS ET LOGICIELS RELATIFS À LA CYBERSÉCURITÉ ”**

Lot L2 : Gestion de l’authentification et identification numérique

| **N°** | **Description** | **Type** | **Unité** | **Q** | **PU en chiffres HTVA** | **Total HTVA** |
| --- | --- | --- | --- | --- | --- | --- |
| 1 | À adapter | QP | forfait | 1 |  |  |
| 2 |  | QP | Annuel | 1 |  |  |
| 3 |  | QP | Licence | 1 |  |  |
| 4 |  | QP | Boitier | 1 |  |  |
| 5 |  | QP | Jour-homme | 1 |  |  |
| 6 |  | QP | Etc. | 1 |  |  |
| Etc. |  | QP | À adapter | 1 |  |  |
| **Total lot L2 HTVA :** | | | | | |  |
| **TVA 21% :** | | | | | |  |
| **Total lot L2 TVAC :** | | | | | |  |

|  |
| --- |
| *Les prix unitaires doivent être mentionnés avec 2 chiffres après la virgule. La quantité de produits x le prix unitaire doivent être à chaque fois arrondis à 2 chiffres après la virgule.* |
| Vu, vérifié et complété avec les prix unitaires, les totaux partiels et le total global qui ont servi à déterminer le montant de mon offre de ce jour, pour être joint à mon formulaire d’offre.  Fait à …....................................... le …................................................... Fonction : …...................................................  Nom et prénom : …................................................................. |

Lot L2 : Gestion de l’authentification et identification numérique– mise en application de l’inventaire du lot selon le scénario opérationnel

| **N°** | **Description** | **Type** | **Unité** | **Q** | **PU en chiffres HTVA** | **Total HTVA** |
| --- | --- | --- | --- | --- | --- | --- |
| 1 | À reprendre du tableau initial du lot | QP | forfait | 1 |  |  |
| 2 |  | QP | Annuel | 1 |  |  |
| 3 |  | QP | Licence | 1 |  |  |
| 4 |  | QP | Boitier | 1 |  |  |
| 5 |  | QP | Jour-homme | 1 |  |  |
| 6 |  | QP | Etc. | 1 |  |  |
| Etc. |  | QP | À adapter | 1 |  |  |
| **Total lot L2 HTVA :** | | | | | |  |
| **TVA 21% :** | | | | | |  |
| **Total lot L2 TVAC :** | | | | | |  |

|  |
| --- |
| *Les prix unitaires doivent être mentionnés avec 2 chiffres après la virgule. La quantité de produits x le prix unitaire doivent être à chaque fois arrondis à 2 chiffres après la virgule.* |
| Vu, vérifié et complété avec les prix unitaires, les totaux partiels et le total global qui ont servi à déterminer le montant de mon offre de ce jour, pour être joint à mon formulaire d’offre.  Fait à …....................................... le …................................................... Fonction : …...................................................  Nom et prénom : …................................................................. |

**“** **FOURNITURE ET MAINTENANCE DE MATÉRIELS ET LOGICIELS RELATIFS À LA CYBERSÉCURITÉ ”**

Lot L3 : Filtrage des messages électroniques

| **N°** | **Description** | **Type** | **Unité** | **Q** | **PU en chiffres HTVA** | **Total HTVA** |
| --- | --- | --- | --- | --- | --- | --- |
| 1 | À adapter | QP | forfait | 1 |  |  |
| 2 |  | QP | Annuel | 1 |  |  |
| 3 |  | QP | Licence | 1 |  |  |
| 4 |  | QP | Boitier | 1 |  |  |
| 5 |  | QP | Jour-homme | 1 |  |  |
| 6 |  | QP | Etc. | 1 |  |  |
| Etc. |  | QP | À adapter | 1 |  |  |
| **Total lot L3 HTVA :** | | | | | |  |
| **TVA 21% :** | | | | | |  |
| **Total lot L3 TVAC :** | | | | | |  |

|  |
| --- |
| *Les prix unitaires doivent être mentionnés avec 2 chiffres après la virgule. La quantité de produits x le prix unitaire doivent être à chaque fois arrondis à 2 chiffres après la virgule.* |
| Vu, vérifié et complété avec les prix unitaires, les totaux partiels et le total global qui ont servi à déterminer le montant de mon offre de ce jour, pour être joint à mon formulaire d’offre.  Fait à …....................................... le …................................................... Fonction : …...................................................  Nom et prénom : …................................................................. |

Lot L3 : Filtrage des messages électroniques – mise en application de l’inventaire du lot selon le scénario opérationnel

| **N°** | **Description** | **Type** | **Unité** | **Q** | **PU en chiffres HTVA** | **Total HTVA** |
| --- | --- | --- | --- | --- | --- | --- |
| 1 | À reprendre du tableau initial du lot | QP | forfait | 1 |  |  |
| 2 |  | QP | Annuel | 1 |  |  |
| 3 |  | QP | Licence | 1 |  |  |
| 4 |  | QP | Boitier | 1 |  |  |
| 5 |  | QP | Jour-homme | 1 |  |  |
| 6 |  | QP | Etc. | 1 |  |  |
| Etc. |  | QP | À adapter | 1 |  |  |
| **Total lot L3 HTVA :** | | | | | |  |
| **TVA 21% :** | | | | | |  |
| **Total lot L3 TVAC :** | | | | | |  |

|  |
| --- |
| *Les prix unitaires doivent être mentionnés avec 2 chiffres après la virgule. La quantité de produits x le prix unitaire doivent être à chaque fois arrondis à 2 chiffres après la virgule.* |
| Vu, vérifié et complété avec les prix unitaires, les totaux partiels et le total global qui ont servi à déterminer le montant de mon offre de ce jour, pour être joint à mon formulaire d’offre.  Fait à …....................................... le …................................................... Fonction : …...................................................  Nom et prénom : …................................................................. |

**“** **FOURNITURE ET MAINTENANCE DE MATÉRIELS ET LOGICIELS RELATIFS À LA CYBERSÉCURITÉ ”**

Lot L4 : Antivirus/antimalware/EDR/XDR

| **N°** | **Description** | **Type** | **Unité** | **Q** | **PU en chiffres HTVA** | **Total HTVA** |
| --- | --- | --- | --- | --- | --- | --- |
| 1 | À adapter | QP | forfait | 1 |  |  |
| 2 |  | QP | Annuel | 1 |  |  |
| 3 |  | QP | Licence | 1 |  |  |
| 4 |  | QP | Boitier | 1 |  |  |
| 5 |  | QP | Jour-homme | 1 |  |  |
| 6 |  | QP | Etc. | 1 |  |  |
| Etc. |  | QP | À adapter | 1 |  |  |
| **Total lot L4 HTVA :** | | | | | |  |
| **TVA 21% :** | | | | | |  |
| **Total lot L4 TVAC :** | | | | | |  |

|  |
| --- |
| *Les prix unitaires doivent être mentionnés avec 2 chiffres après la virgule. La quantité de produits x le prix unitaire doivent être à chaque fois arrondis à 2 chiffres après la virgule.* |
| Vu, vérifié et complété avec les prix unitaires, les totaux partiels et le total global qui ont servi à déterminer le montant de mon offre de ce jour, pour être joint à mon formulaire d’offre.  Fait à …....................................... le …................................................... Fonction : …...................................................  Nom et prénom : …................................................................. |

Lot L4 : Antivirus/antimalware/EDR/XDR – mise en application de l’inventaire du lot selon le scénario opérationnel

| **N°** | **Description** | **Type** | **Unité** | **Q** | **PU en chiffres HTVA** | **Total HTVA** |
| --- | --- | --- | --- | --- | --- | --- |
| 1 | À reprendre du tableau initial du lot | QP | forfait | 1 |  |  |
| 2 |  | QP | Annuel | 1 |  |  |
| 3 |  | QP | Licence | 1 |  |  |
| 4 |  | QP | Boitier | 1 |  |  |
| 5 |  | QP | Jour-homme | 1 |  |  |
| 6 |  | QP | Etc. | 1 |  |  |
| Etc. |  | QP | À adapter | 1 |  |  |
| **Total lot L4 HTVA :** | | | | | |  |
| **TVA 21% :** | | | | | |  |
| **Total lot L4 TVAC :** | | | | | |  |

|  |
| --- |
| *Les prix unitaires doivent être mentionnés avec 2 chiffres après la virgule. La quantité de produits x le prix unitaire doivent être à chaque fois arrondis à 2 chiffres après la virgule.* |
| Vu, vérifié et complété avec les prix unitaires, les totaux partiels et le total global qui ont servi à déterminer le montant de mon offre de ce jour, pour être joint à mon formulaire d’offre.  Fait à …....................................... le …................................................... Fonction : …...................................................  Nom et prénom : …................................................................. |

**“** **FOURNITURE ET MAINTENANCE DE MATÉRIELS ET LOGICIELS RELATIFS À LA CYBERSÉCURITÉ ”**

Lot L5 : Gestion des mots de passe

| **N°** | **Description** | **Type** | **Unité** | **Q** | **PU en chiffres HTVA** | **Total HTVA** |
| --- | --- | --- | --- | --- | --- | --- |
| 1 | À adapter | QP | forfait | 1 |  |  |
| 2 |  | QP | Annuel | 1 |  |  |
| 3 |  | QP | Licence | 1 |  |  |
| 4 |  | QP | Boitier | 1 |  |  |
| 5 |  | QP | Jour-homme | 1 |  |  |
| 6 |  | QP | Etc. | 1 |  |  |
| Etc. |  | QP | À adapter | 1 |  |  |
| **Total lot L5 HTVA :** | | | | | |  |
| **TVA 21% :** | | | | | |  |
| **Total lot L5 TVAC :** | | | | | |  |

|  |
| --- |
| *Les prix unitaires doivent être mentionnés avec 2 chiffres après la virgule. La quantité de produits x le prix unitaire doivent être à chaque fois arrondis à 2 chiffres après la virgule.* |
| Vu, vérifié et complété avec les prix unitaires, les totaux partiels et le total global qui ont servi à déterminer le montant de mon offre de ce jour, pour être joint à mon formulaire d’offre.  Fait à …....................................... le …................................................... Fonction : …...................................................  Nom et prénom : …................................................................. |

Lot L5 : Gestion des mots de passe – mise en application de l’inventaire du lot selon le scénario opérationnel

| **N°** | **Description** | **Type** | **Unité** | **Q** | **PU en chiffres HTVA** | **Total HTVA** |
| --- | --- | --- | --- | --- | --- | --- |
| 1 | À reprendre du tableau initial du lot | QP | forfait | 1 |  |  |
| 2 |  | QP | Annuel | 1 |  |  |
| 3 |  | QP | Licence | 1 |  |  |
| 4 |  | QP | Boitier | 1 |  |  |
| 5 |  | QP | Jour-homme | 1 |  |  |
| 6 |  | QP | Etc. | 1 |  |  |
| Etc. |  | QP | À adapter | 1 |  |  |
| **Total lot L5 HTVA :** | | | | | |  |
| **TVA 21% :** | | | | | |  |
| **Total lot L5 TVAC :** | | | | | |  |

|  |
| --- |
| *Les prix unitaires doivent être mentionnés avec 2 chiffres après la virgule. La quantité de produits x le prix unitaire doivent être à chaque fois arrondis à 2 chiffres après la virgule.* |
| Vu, vérifié et complété avec les prix unitaires, les totaux partiels et le total global qui ont servi à déterminer le montant de mon offre de ce jour, pour être joint à mon formulaire d’offre.  Fait à …....................................... le …................................................... Fonction : …...................................................  Nom et prénom : …................................................................. |

1. **BORDEREAU DE REPONSE TECHNIQUE**

**“ FOURNITURE ET MAINTENANCE DE MATÉRIELS ET LOGICIELS RELATIFS À LA CYBERSÉCURITÉ ”**

**Lot M1 – Produits MFA**

**Critère 2 - Maîtrise des domaines d'expertise liés à ce lot**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **#** | **Domaines d'expertise** | **Expert 1 - N° de CV** | **Expert 2 - N° de CV** | **Expert 3 - N° de CV** |
| 1 | Expérience dans la conception et la fabrication d'appareils MFA physique | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non |
| 2 | Connaissance des protocoles d'authentification à plusieurs facteurs (MFA) tels que TOTP, HOTP, RSA SecurID, etc. | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non |
| 3 | Connaissance des protocoles de communication courants pour la communication entre l'appareil et les systèmes d'authentification tels que NFC, Bluetooth, USB | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non |
| 4 | Connaissance des protocoles de cryptage courants pour chiffrer les données stockées sur l'appareil | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non |
| 5 | Connaissance des protocoles de gestion de clés courants tels que PKI pour renforcer la sécurité des communications entre l'appareil et les systèmes d'authentification ; | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non |
| 6 | Connaissance des protocoles de communication courants pour la communication entre l'appareil et les systèmes d'authentification tels que RADIUS, TOTP, HOTP ; | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non |
| 7 | Expérience dans la mise en place et la gestion de solutions MFA physique pour les organisations ; | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non |
| 8 | Connaissance des normes de sécurité courantes telles que ISO 27001 et NIS 2 ; | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non |
| 9 | Connaissance des différents types d'appareils MFA physique tels que les tokens, les clés USB, les cartes à puce, les lecteurs d'empreintes digitales, les caméras d'empreintes faciales, etc. ; | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non |
| 10 | Expérience dans la personnalisation des appareils MFA physique pour répondre aux besoins spécifiques de l'organisation, tels que les exigences de branding, les paramètres de configuration, etc. ; | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non |
| 11 | Connaissance des différents systèmes d'exploitation couramment utilisés pour les appareils MFA physique, tels que Windows, iOS, Android, etc. ; | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non |
| 12 | Connaissance des exigences réglementaires et normatives liées à l'utilisation d'appareils MFA physique ; | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non |
| 13 | Connaissance des meilleures pratiques de sécurité pour la gestion et la maintenance des appareils MFA physique, tels que la gestion des mots de passe, la sauvegarde de données, la gestion des clés de chiffrement, etc ; | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non |
| 14 | Une connaissance approfondie des meilleures pratiques de sécurité, telles que l'identification et la gestion des vulnérabilités, la protection contre les attaques brute force, la sécurisation des communications, etc. | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non |
| 15 | Une capacité à mettre en place des mesures de sécurité robustes afin de protéger les dispositifs MFA physiques contre les attaques physiques et logiques, ainsi que pour garantir la confidentialité, l'intégrité et la disponibilité des données traitées. | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non |
| 16 | Une expertise dans le protocole d’authentification couramment utilisé tel que SAML, Radius, OAUTH. La mise en œuvre de ces protocoles doit se faire de manière sécurisée en utilisant des mécanismes d’échange de clés, de chiffrement et d’authentification forte | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non |

**Critère 3 - Méthodologie d’analyse et d’implémentation**

|  |  |  |
| --- | --- | --- |
| **#** | **Question** | **Réponse** |
| 1 | Décrivez la méthodologie utilisée pour cerner les besoins du Pouvoir Local. |  |
| 2 | Décrivez la méthodologie utilisée pour transposer les besoins identifiés à la proposition technique |  |
| 3 | Décrivez la méthodologie utilisée pour présenter au Pouvoir local la proposition technique, vérifier l'adéquation aux besoins et faire valider la proposition |  |
| 4 | Décrivez la méthodologie utilisée pour vérifier et contrôler la bonne installation selon la proposition technique et les tests réalisés pour assurer l'adéquation de la solution implémentée au besoin identifié |  |
| 5 | Décrivez la méthodologie utilisée pour définir le contenu de la formation nécessaire. |  |
| 6 | Décrivez la méthodologie utilisée pour vérifier les acquis suite à la formation |  |
| 7 | Décrivez la méthodologie de renforcement et formation continue proposée aux Pouvoirs locaux découlant de l'installation réalisée. |  |
| 8 | Décrivez la méthodologie de réversibilité au terme du contrat. |  |

**Critère 4 - Qualité de la documentation (analyse, installation, projet)**

|  |  |  |
| --- | --- | --- |
| **#** | **Question** | **Réponse** |
| 1 | Décrivez la documentation d'analyse qui est réalisée. |  |
| 2 | Décrivez la documentation d'installation/configuration qui est réalisée. |  |
| 3 | Décrivez la documentation des procédures d'exploitation qui est faite. |  |
| 4 | Décrivez la documentation des incidents et de leurs procédures de solutionnement |  |
| 5 | Décrivez la documentation des failles constatées et leur mitigation du risque |  |
| 6 | Décrivez la documentation relative aux administrateurs qui est mise à leur disposition. |  |
| 7 | Décrivez la documentation relative aux utilisateurs qui est mise à leur disposition. |  |

**Critère 5 – Qualité technique**

|  |  |  |  |
| --- | --- | --- | --- |
| **#** | **Question** | **Conformité** | **Réponse** |
| 1 | Quels sont les moyens (méthodes) d’authentification existants | Oui – Non |  |
| 2 | Comment votre solution de MFA prend-elle en charge les systèmes d’accès réseau actuels (ou futurs) ? | Oui - Non |  |
| 3 | Comment votre solution de MFA fonctionne-t-elle avec toutes les applications stratégiques des pouvoirs locaux wallons (applications cloud, applications locales, AD ou LDAP, autres solutions de gestion des identités telles que les gestionnaires de mots de passe et les solutions de sécurité des terminaux) ? | Oui - Non |  |
| 4 | Comment votre solution de MFA permet-elle la mise en place de stratégies d’authentification flexibles et sophistiquées au niveau granulaire ? | Oui - Non |  |
| 5 | La solution de MFA prend-elle en charge les standards modernes et courants pour des connexions sécurisées aux applications Web ? Quels sont les standards supportés et quels en sont les avantages ? | Oui - Non |  |
| 6 | Par quels moyens les développeurs peuvent-ils personnaliser et intégrer votre solution de MFA avec des applications personnalisées et des systèmes tiers ? | Oui - Non |  |
| 7 | Comment votre solution de MFA prend-elle en charge tous les utilisateurs autorisés qui accèdent aux systèmes et données ? Quels sont les appareils, susceptibles d’être utilisés par ces utilisateurs, qui sont pris en charge ? | Oui - Non |  |
| 8 | Quels sont les rapports réalisables par votre solution de MFA permettant d’améliorer la sécurité à partir des données détectées sur les menaces et de respecter les exigences en matière de conformité ? | Oui - Non |  |
| 9 | Votre solution de MFA utilise-t-elle une analyse des comportements pour s’adapter intelligemment ? Comment tient-elle compte de l’appareil d’authentification utilisé et quels avantages en découlent ? | Oui – Non |  |
| 10 | Quelles attaques votre solution de MFA permet-elle d’éviter (contrer) ? | Oui - Non |  |

**Critère 6 – Licence libre**

|  |  |  |
| --- | --- | --- |
| **#** | **Question** | **Réponse** |
| 1 | Le matériel ou le logiciel proposé est-il basé et reste lui-même sous licence libre ? Dans l'affirmative, quelle licence libre est-ce ? |  |

**Lot M2 – Pare-feu**

**Crit 2 – Maîtrise des domaines d’expertise liés à ce lot**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **#** | **Domaines d'expertise** | **Expert 1 - N° de CV** | **Expert 2 - N° de CV** | **Expert 3 - N° de CV** |
| 1 | Connaissance approfondie des technologies de sécurité réseau, notamment des protocoles de sécurité et des technologies de chiffrement ; | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non |
| 2 | Maîtrise des différents protocoles de routage et de commutation utilisés dans les réseaux locaux et étendus ; | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non |
| 3 | Connaissance des normes et réglementations en matière de sécurité des réseaux, notamment celles applicables aux Pouvoirs locaux wallons ; | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non |
| 4 | Expérience de la mise en œuvre et de la gestion de pare-feu dans des environnements de petite et moyenne taille ; | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non |
| 5 | Capacité à fournir un support technique de qualité et à répondre rapidement aux demandes d’assistance des utilisateurs ; | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non |
| 6 | Connaissance des outils et des processus de gestion de la sécurité, tels que la gestion des mises à jour de logiciels et de la documentation, la gestion des événements de sécurité et la gestion des alertes de sécurité ; | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non |
| 7 | Capacité à fournir une évaluation de l'infrastructure réseau existante et à proposer des solutions de mise à niveau ou de mise à jour pour améliorer la sécurité et la performance ; | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non |
| 8 | Compétences en matière de déploiement et de configuration de pare-feu en grappe, en particulier en mode active/active et active/passive ; | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non |
| 9 | Connaissance des meilleures pratiques de gestion de la sécurité et de la performance des pares-feux, y compris les processus de monitoring et de rapport ; | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non |
| 10 | Expérience de la mise en œuvre de règles de sécurité avancées, telles que l'inspection de contenu et l'analyse de comportement ; | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non |
| 11 | Capacité à fournir une formation et un support technique aux utilisateurs du pare-feu, y compris la mise en place de documents de référence et de guides d'utilisation ; | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non |
| 12 | Connaissance des technologies de virtualisation et de la manière de déployer et de gérer des pare-feux virtuels dans un environnement de cloud computing. | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non |

**Critère 3 - Méthodologie d’analyse et d’implémentation**

|  |  |  |
| --- | --- | --- |
| **#** | **Question** | **Réponse** |
| 1 | Décrivez la méthodologie utilisée pour cerner les besoins du Pouvoir Local. |  |
| 2 | Décrivez la méthodologie utilisée pour transposer les besoins identifiés à la proposition technique |  |
| 3 | Décrivez la méthodologie utilisée pour présenter au Pouvoir local la proposition technique, vérifier l'adéquation aux besoins et faire valider la proposition |  |
| 4 | Décrivez la méthodologie utilisée pour vérifier et contrôler la bonne installation selon la proposition technique et les tests réalisés pour assurer l'adéquation de la solution implémentée au besoin identifié |  |
| 5 | Décrivez la méthodologie utilisée pour définir le contenu de la formation nécessaire. |  |
| 6 | Décrivez la méthodologie utilisée pour vérifier les acquis suite à la formation |  |
| 7 | Décrivez la méthodologie de renforcement et formation continue proposée aux Pouvoirs locaux découlant de l'installation réalisée. |  |
| 8 | Décrivez la méthodologie de réversibilité au terme du contrat. |  |

**Critère 4 - Qualité de la documentation (analyse, installation, projet)**

|  |  |  |
| --- | --- | --- |
| **#** | **Question** | **Réponse** |
| 1 | Décrivez la documentation d'analyse qui est réalisée. |  |
| 2 | Décrivez la documentation d'installation/configuration qui est réalisée. |  |
| 3 | Décrivez la documentation des procédures d'exploitation qui est faite. |  |
| 4 | Décrivez la documentation des incidents et de leurs procédures de solutionnement |  |
| 5 | Décrivez la documentation des failles constatées et leur mitigation du risque |  |
| 6 | Décrivez la documentation relative aux administrateurs qui est mise à leur disposition. |  |
| 7 | Décrivez la documentation relative aux utilisateurs qui est mise à leur disposition. |  |

**Critère 5 – Qualité technique**

|  |  |  |  |
| --- | --- | --- | --- |
| **#** | **Question** | **Conformité** | **Réponse** |
| 1 | Comment le pare-feu permet-il le fonctionnement de « stateful inspection » complètes ? | Oui – Non |  |
| 2 | Le pare-feu offre-t-il un accès à distance sécurisé et robuste pour les utilisateurs mobiles ? | Oui - Non |  |
| 3 | Comment le pare-feu assure-t-il une protection proactive contre les menaces ? | Oui - Non |  |
| 4 | Comment le pare-feu reste performant lorsque plusieurs services de sécurité s'exécutent ? | Oui - Non |  |
| 5 | Comment le pare-feu assure-t-il une visibilité complète et un contrôle précis des applications ? | Oui - Non |  |
| 6 | Quelles informations le pare-feu est-il en mesure de donner à propos des utilisateurs, du réseau, des applications et des périphériques afin d'assurer une protection par prise en compte du contexte ? | Oui - Non |  |
| 7 | Le pare-feu assure-t-il la sécurité web cloud ? | Oui - Non |  |
| 8 | Pouvez-vous déployer une solution qui évoluera à mesure que votre entreprise grandira ? | Oui - Non |  |
| 9 | Le fournisseur du pare-feu offre-t-il une assistance et des services complets pour faciliter la migration depuis l’installation existante vers l’architecture cible ? | Oui – Non |  |
| 10 | Quels moyens le fournisseur du pare-feu offre-t-il pour faciliter la migration depuis son pare-feu vers une autre solution au terme de l’utilisation (réversibilité) ? | Oui - Non |  |

**Critère 6 – Licence libre**

|  |  |  |
| --- | --- | --- |
| **#** | **Question** | **Réponse** |
| 1 | Le matériel ou le logiciel proposé est-il basé et reste lui-même sous licence libre ? Dans l'affirmative, quelle licence libre est-ce ? |  |

**Lot M3 – Sauvegardes sécurisées de données**

**Critère 2 – Maîtrise des domaines d’expertise liés à ce lot**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **#** | **Domaines d'expertise** | **Expert 1 - N° de CV** | **Expert 2 - N° de CV** | **Expert 3 - N° de CV** |
| 1 | Connaissance des réglementations et des normes en matière de sauvegarde et restauration des données en Belgique ; | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non |
| 2 | Expérience dans la mise en place et le déploiement en matière de sauvegarde et restauration des données ; | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non |
| 3 | Compétences en matière de sécurité de l'information et de gestion des risques liés à la sauvegarde et restauration des données ; | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non |
| 4 | Connaissance des normes et des réglementations en matière de sauvegarde et de protection des données (par exemple, RGPD) ; | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non |
| 5 | Compétences en matière de planification et de mise en place de stratégies de sauvegarde ; | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non |
| 6 | Connaissance des différents types de sauvegarde (par exemple, incrémentielle, différentielle, complète) et des technologies associées (par exemple, sauvegarde sur bande, sauvegarde sur disque, sauvegarde dans le cloud) ; | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non |
| 7 | Compétences en matière de sécurité des systèmes pour protéger les données sauvegardées contre les attaques externes et internes ; | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non |
| 8 | Compétences en matière de surveillance et de gestion des performances des systèmes de sauvegarde pour assurer la disponibilité des données en cas de besoin ; | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non |
| 9 | Connaissance des outils de sauvegarde et de restauration pour gérer les processus de sauvegarde et de restauration des données ; | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non |
| 10 | Connaissance de la récupération des données pour pouvoir récupérer les données en cas de besoin. ; | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non |
| 11 | Connaissance des politiques de RTO et RPO pour garantir la restauration des données en temps voulu et dans les limites de tolérance de perte de données ; | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non |
| 12 | Compétences en matière de formation et de support technique pour les utilisateurs finaux, afin de garantir que la sauvegarde et la restauration des données sont utilisées de manière efficace et sécurisée ; | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non |
| 13 | Connaissance des tendances et des innovations dans le domaine de la sauvegarde et la restauration des données, afin de pouvoir conseiller et orienter les Pouvoirs locaux sur les meilleures pratiques et les technologies les plus récentes. | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non |

**Critère 3 - Méthodologie d’analyse et d’implémentation**

|  |  |  |
| --- | --- | --- |
| **#** | **Question** | **Réponse** |
| 1 | Décrivez la méthodologie utilisée pour cerner les besoins du Pouvoir Local. |  |
| 2 | Décrivez la méthodologie utilisée pour transposer les besoins identifiés à la proposition technique |  |
| 3 | Décrivez la méthodologie utilisée pour présenter au Pouvoir local la proposition technique, vérifier l'adéquation aux besoins et faire valider la proposition |  |
| 4 | Décrivez la méthodologie utilisée pour vérifier et contrôler la bonne installation selon la proposition technique et les tests réalisés pour assurer l'adéquation de la solution implémentée au besoin identifié |  |
| 5 | Décrivez la méthodologie utilisée pour définir le contenu de la formation nécessaire. |  |
| 6 | Décrivez la méthodologie utilisée pour vérifier les acquis suite à la formation |  |
| 7 | Décrivez la méthodologie de renforcement et formation continue proposée aux Pouvoirs locaux découlant de l'installation réalisée. |  |
| 8 | Décrivez la méthodologie de réversibilité au terme du contrat. |  |

**Critère 4 - Qualité de la documentation (analyse, installation, projet)**

|  |  |  |
| --- | --- | --- |
| **#** | **Question** | **Réponse** |
| 1 | Décrivez la documentation d'analyse qui est réalisée. |  |
| 2 | Décrivez la documentation d'installation/configuration qui est réalisée. |  |
| 3 | Décrivez la documentation des procédures d'exploitation qui est faite. |  |
| 4 | Décrivez la documentation des incidents et de leurs procédures de solutionnement |  |
| 5 | Décrivez la documentation des failles constatées et leur mitigation du risque |  |
| 6 | Décrivez la documentation relative aux administrateurs qui est mise à leur disposition. |  |
| 7 | Décrivez la documentation relative aux utilisateurs qui est mise à leur disposition. |  |

**Critère 5 – Qualité technique**

|  |  |  |  |
| --- | --- | --- | --- |
| **#** | **Question** | **Conformité** | **Réponse** |
| 1 | Comment votre application permet-elle la sauvegarde des données sur différents supports et à différents emplacements ? | Oui – Non |  |
| 2 | Comment votre application permet-elle un un chiffrement fort des données pour protéger les données sauvegardées contre les accès non autorisés ? | Oui - Non |  |
| 3 | Comment votre application permet-elle de garantir que les données sont sauvegardées régulièrement et de manière fiable ? | Oui - Non |  |
| 4 | Comment votre application permet-elle de protéger les données contre les risques locaux, tels que les incendies ou les inondations ? | Oui - Non |  |
| 5 | Comment votre application permet-elle d’assurer une haute disponibilité pour garantir la disponibilité des données en cas de besoin ? | Oui - Non |  |
| 6 | Par quels biais votre application permet-elle d’optimiser la rapidité de la sauvegarde et de la restauration des données ? | Oui - Non |  |
| 7 | Quels sont les moyens de journalisation pour suivre les actions de sauvegarde et de restauration des données ? | Oui - Non |  |
| 8 | Quelles sont les stratégies de sauvegarde et de restauration pour toutes les données vitales possibles et/ou existantes ? | Oui - Non |  |
| 9 | Comment votre application permet-elle d’établir des ​​règles de sauvegarde et de restauration différenciée selon le type de données ? | Oui – Non |  |
| 10 | Quel niveau de redondance est-il possible de mettre en place afin d’assurer la sécurité des données ? | Oui - Non |  |
| 11 | Quels moyens de tests de sauvegarde et de restauration réguliers permettent-ils de vérifier l'intégrité des données ? | Oui - Non |  |

**Critère 6 – Licence libre**

|  |  |  |
| --- | --- | --- |
| **#** | **Question** | **Réponse** |
| 1 | Le matériel ou le logiciel proposé est-il basé et reste lui-même sous licence libre ? Dans l'affirmative, quelle licence libre est-ce ? |  |

**Lot L1 – Journalisation des événements**

**Critère 2 – Maîtrise des domaines d’expertise liés à ce lot**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **#** | **Domaines d'expertise** | **Expert 1 - N° de CV** | **Expert 2 - N° de CV** | **Expert 3 - N° de CV** |
| 1 | Connaissance des règlementations et normes en matière de journalisation des évènements (par exemple, PCI DSS, GDPR, ISO 27001) ; | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non |
| 2 | Expérience dans l'implémentation de solutions de journalisation des évènements dans des environnements de taille similaire à celui des Pouvoirs locaux wallons ; | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non |
| 3 | Maîtrise des technologies et protocoles utilisés dans les solutions de journalisation des évènements (par exemple, Syslog, CEF, JSON) ; | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non |
| 4 | Capacité à intégrer des solutions de journalisation des évènements dans des architectures de sécurité existantes ; | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non |
| 5 | Expérience dans la gestion de grandes quantités de données de journalisation et dans l'analyse de ces données pour identifier des anomalies et des menaces potentielles ; | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non |
| 6 | Capacité à configurer et à personnaliser les règles de journalisation et les alertes en fonction des besoins spécifiques du client ; | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non |
| 7 | Expérience en matière de gestion et d'analyse des journaux d'événements, notamment en utilisant des outils de visualisation de données et de corrélation d’événements ; | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non |
| 8 | Bonne compréhension des architectures de réseau et des protocoles de communication courants, ainsi que des enjeux de sécurité associés ; | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non |
| 9 | Capacité à travailler en étroite collaboration avec les équipes de sécurité et de réseau pour définir les besoins en matière de journalisation et mettre en œuvre des solutions adaptées | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non |

**Critère 3 - Méthodologie d’analyse et d’implémentation**

|  |  |  |
| --- | --- | --- |
| **#** | **Question** | **Réponse** |
| 1 | Décrivez la méthodologie utilisée pour cerner les besoins du Pouvoir Local. |  |
| 2 | Décrivez la méthodologie utilisée pour transposer les besoins identifiés à la proposition technique |  |
| 3 | Décrivez la méthodologie utilisée pour présenter au Pouvoir local la proposition technique, vérifier l'adéquation aux besoins et faire valider la proposition |  |
| 4 | Décrivez la méthodologie utilisée pour vérifier et contrôler la bonne installation selon la proposition technique et les tests réalisés pour assurer l'adéquation de la solution implémentée au besoin identifié |  |
| 5 | Décrivez la méthodologie utilisée pour définir le contenu de la formation nécessaire. |  |
| 6 | Décrivez la méthodologie utilisée pour vérifier les acquis suite à la formation |  |
| 7 | Décrivez la méthodologie de renforcement et formation continue proposée aux Pouvoirs locaux découlant de l'installation réalisée. |  |
| 8 | Décrivez la méthodologie de réversibilité au terme du contrat. |  |

**Critère 4 - Qualité de la documentation (analyse, installation, projet)**

|  |  |  |
| --- | --- | --- |
| **#** | **Question** | **Réponse** |
| 1 | Décrivez la documentation d'analyse qui est réalisée. |  |
| 2 | Décrivez la documentation d'installation/configuration qui est réalisée. |  |
| 3 | Décrivez la documentation des procédures d'exploitation qui est faite. |  |
| 4 | Décrivez la documentation des incidents et de leurs procédures de solutionnement |  |
| 5 | Décrivez la documentation des failles constatées et leur mitigation du risque |  |
| 6 | Décrivez la documentation relative aux administrateurs qui est mise à leur disposition. |  |
| 7 | Décrivez la documentation relative aux utilisateurs qui est mise à leur disposition. |  |

**Critère 5 – Qualité technique**

|  |  |  |  |
| --- | --- | --- | --- |
| **#** | **Question** | **Conformité** | **Réponse** |
| 1 | Comment l’application peut-elle veiller à la bonne synchronisation des horloges entre système de journalisation et les systèmes faisant l’objet de la journalisation des événements | Oui – Non |  |
| 2 | Comment procédez-vous pour Identifier et activer les journaux Windows utiles aux activités de détection et d’analyse | Oui - Non |  |
| 3 | Quels sont les systèmes que votre application est en mesure de surveiller et effectuer la journalisation des événements ? | Oui - Non |  |
| 4 | Comment votre application permet-elle de gérer le déploiement des serveurs de collecte ? | Oui - Non |  |
| 5 | À quel format les événements sont-ils journalisés ? | Oui - Non |  |
| 6 | Comment faites-vous pour cloisonner les serveurs de collecte ? | Oui - Non |  |
| 7 | Quelles sont les analyses possibles des journaux d’événements ? | Oui - Non |  |
| 8 | Quelles sont les catégories d’événements qui peuvent faire l’objet d’une journalisation dans votre application ? | Oui - Non |  |
| 9 | Comment la journalisation des événements permet-elle d’identifier la source des événements ? | Oui – Non |  |
| 10 | Comment et par quel biais votre journalisation des événements est-elle sécurisée ? | Oui - Non |  |
| 11 | Quelles sont les configurations des politiques de journalisation sur les équipements réalisables ? | Oui - Non |  |
| 12 | À quelle granularité la journalisation des événements est-elle réalisable ? | Oui - Non |  |
| 13 | Comment votre application permet-elle de garantir la résilience de la collecte des événements ? | Oui - Non |  |
| 14 | Quelle supervision de la chaîne de collecte des évènements de sécurité est possible ? | Oui - Non |  |
| 15 | Comment votre application permet-elle de différer (temporellement) le transfert des journaux ? | Oui - Non |  |

**Critère 6 – Licence libre**

|  |  |  |
| --- | --- | --- |
| **#** | **Question** | **Réponse** |
| 1 | Le matériel ou le logiciel proposé est-il basé et reste lui-même sous licence libre ? Dans l'affirmative, quelle licence libre est-ce ? |  |

**Lot L2 – Gestion de l’authentification et identification numérique**

**Critère 2 – Maîtrise des domaines d’expertise liés à ce lot**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **#** | **Domaines d'expertise** | **Expert 1 - N° de CV** | **Expert 2 - N° de CV** | **Expert 3 - N° de CV** |
| 1 | Connaissance des réglementations et des normes en matière d'authentification et d'identification numérique en Belgique ; | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non |
| 2 | Expérience dans la mise en place et le déploiement de systèmes d'authentification et d'identification numérique ; | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non |
| 3 | Compétences en matière de sécurité de l'information et de gestion des risques liés aux systèmes d'authentification et d'identification numérique ; | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non |
| 4 | Connaissance des technologies et des protocoles utilisés dans les systèmes d'authentification et d'identification numérique (par exemple, OAuth, SAML, OpenID Connect) ; | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non |
| 5 | Expérience de travail avec des Pouvoirs locaux ou d'autres organismes gouvernementaux ; | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non |
| 6 | Compétences en matière de communication et de gestion de projet, afin de gérer efficacement la mise en œuvre et le déploiement de projets liés à l'authentification et à l'identification numérique ; | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non |
| 7 | Expérience de travail avec des plateformes d'authentification et d'identification numérique, telles que des portails de gestion de l'identité (Identity Management) ou des systèmes de gestion de l'authentification (Authentication Management) ; | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non |
| 8 | Compétences en matière de développement de solutions d'authentification et d'identification numérique, y compris la connaissance de différents langages de programmation ; | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non |
| 9 | Connaissance des outils et technologies utilisés pour la gestion de l'identité et de l'authentification numérique, tels que les répertoires (annuaires), les bases de données d'identité et les gestionnaires de mots de passe ; | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non |
| 10 | Capacité à travailler en étroite collaboration avec les équipes de développement et de sécurité pour assurer la mise en œuvre efficace et sécurisée de projets d'authentification et d'identification numérique ; | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non |
| 11 | Compétences en matière de formation et de support technique pour les utilisateurs finaux, afin de garantir que les systèmes d'authentification et d'identification numérique sont utilisés de manière efficace et sécurisée ; | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non |
| 12 | Connaissance des tendances et des innovations dans le domaine de l'authentification et de l'identification numérique, afin de pouvoir conseiller et orienter les Pouvoirs locaux sur les meilleures pratiques et les technologies les plus récentes ; | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non |

**Critère 3 - Méthodologie d’analyse et d’implémentation**

|  |  |  |
| --- | --- | --- |
| **#** | **Question** | **Réponse** |
| 1 | Décrivez la méthodologie utilisée pour cerner les besoins du Pouvoir Local. |  |
| 2 | Décrivez la méthodologie utilisée pour transposer les besoins identifiés à la proposition technique |  |
| 3 | Décrivez la méthodologie utilisée pour présenter au Pouvoir local la proposition technique, vérifier l'adéquation aux besoins et faire valider la proposition |  |
| 4 | Décrivez la méthodologie utilisée pour vérifier et contrôler la bonne installation selon la proposition technique et les tests réalisés pour assurer l'adéquation de la solution implémentée au besoin identifié |  |
| 5 | Décrivez la méthodologie utilisée pour définir le contenu de la formation nécessaire. |  |
| 6 | Décrivez la méthodologie utilisée pour vérifier les acquis suite à la formation |  |
| 7 | Décrivez la méthodologie de renforcement et formation continue proposée aux Pouvoirs locaux découlant de l'installation réalisée. |  |
| 8 | Décrivez la méthodologie de réversibilité au terme du contrat. |  |

**Critère 4 - Qualité de la documentation (analyse, installation, projet)**

|  |  |  |
| --- | --- | --- |
| **#** | **Question** | **Réponse** |
| 1 | Décrivez la documentation d'analyse qui est réalisée. |  |
| 2 | Décrivez la documentation d'installation/configuration qui est réalisée. |  |
| 3 | Décrivez la documentation des procédures d'exploitation qui est faite. |  |
| 4 | Décrivez la documentation des incidents et de leurs procédures de solutionnement |  |
| 5 | Décrivez la documentation des failles constatées et leur mitigation du risque |  |
| 6 | Décrivez la documentation relative aux administrateurs qui est mise à leur disposition. |  |
| 7 | Décrivez la documentation relative aux utilisateurs qui est mise à leur disposition. |  |

**Critère 5 – Qualité technique**

|  |  |  |  |
| --- | --- | --- | --- |
| **#** | **Question** | **Conformité** | **Réponse** |
| 1 | Comment votre application permet-elle de faire une gestion avancée des authentifications et identifications ? | Oui – Non |  |
| 2 | Comment votre application permet-elle de s’Intégrer avec les systèmes de gestion de l'identité existants | Oui - Non |  |
| 3 | Comment votre application permet-elle une intégration à un système d'authentification à multiples facteurs ? | Oui - Non |  |
| 4 | Quelles sont les gestions des politiques d'accès et des processus de vérification existantes et possibles ? | Oui - Non |  |
| 5 | Quelles sont les fonctionnalités de rapport et de surveillance des activités d'authentification et d’identification ? | Oui - Non |  |
| 6 | Quelle sont les compatibilités avec les normes et réglementations en matière de sécurité de l'identité et de l'authentification numérique ? | Oui - Non |  |
| 7 | Comment votre application permet-elle d’intégrer le système de gestion de l'authentification et de l'identification dans les systèmes et applications existants des Pouvoirs locaux, de manière à assurer une intégration transparente et à minimiser les perturbations pour les utilisateurs ? | Oui - Non |  |
| 8 | Comment votre application permet-elle de faire la gestion de l'authentification et de l'identification afin de mettre en place une gestion flexible et évolutive des identités et des accès, en fonction des besoins changeants des Pouvoirs locaux ? | Oui - Non |  |
| 9 | Comment votre application permet-elle d’assurer sa haute disponibilité ? | Oui – Non |  |

**Critère 6 – Licence libre**

|  |  |  |
| --- | --- | --- |
| **#** | **Question** | **Réponse** |
| 1 | Le matériel ou le logiciel proposé est-il basé et reste lui-même sous licence libre ? Dans l'affirmative, quelle licence libre est-ce ? |  |

**Lot L3 – Filtrage des messages électroniques**

**Critère 2 – Maîtrise des domaines d’expertise liés à ce lot**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **#** | **Domaines d'expertise** | **Expert 1 - N° de CV** | **Expert 2 - N° de CV** | **Expert 3 - N° de CV** |
| 1 | Connaissance de l'environnement législatif et réglementaire en matière d'authentification et d'identification numérique pour les Pouvoirs locaux wallons ; | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non |
| 2 | Expérience en matière de déploiement de systèmes d'authentification et d'identification numérique pour les Pouvoirs locaux wallons ; | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non |
| 3 | Expérience en matière de gestion de la sécurité des données et des informations, notamment en ce qui concerne les protocoles de sécurité, les stratégies de gestion des accès et les protocoles de gestion des incidents de sécurité ; | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non |
| 4 | Maîtrise de technologies de l'authentification et de l'identification numérique, telles que les certificats numériques, les jetons de sécurité et les technologies de l'identité forte ; | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non |
| 5 | Expérience en matière de développement de solutions de gestion de l'authentification et de l'identification numérique, y compris les applications Web et mobiles ; | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non |
| 6 | Expérience en matière de gestion de projets liés à l'authentification et à l'identification numérique pour les Pouvoirs locaux wallons, y compris la gestion des délais, des coûts et de la qualité ; | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non |
| 7 | Compétences en matière de communication et de sensibilisation du personnel aux enjeux de l'authentification et de l'identification numérique ; | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non |
| 8 | Connaissance des différents types de logiciels de filtrage des messages électroniques et de leurs fonctionnalités ; | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non |
| 9 | Expérience en matière de déploiement et de configuration de logiciels de filtrage des messages électroniques ; | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non |
| 10 | Maîtrise des protocoles de sécurité et des normes de confidentialité en matière de traitement des messages électroniques ; | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non |
| 11 | Compétences en matière de gestion de la sécurité des données et des informations, notamment en ce qui concerne les protocoles de sécurité, les stratégies de gestion des accès et les protocoles de gestion des incidents de sécurité ; | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non |
| 12 | Expérience en matière de développement de solutions de filtrage des messages électroniques, y compris les applications Web et mobiles ; | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non |
| 13 | Expérience en matière de gestion de projets liés au filtrage des messages électroniques pour les Pouvoirs locaux wallons, y compris la gestion des délais, des coûts et de la qualité ; | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non |
| 14 | Compétences en matière de communication et de sensibilisation du personnel aux enjeux du filtrage des messages électroniques. | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non |

**Critère 3 - Méthodologie d’analyse et d’implémentation**

|  |  |  |
| --- | --- | --- |
| **#** | **Question** | **Réponse** |
| 1 | Décrivez la méthodologie utilisée pour cerner les besoins du Pouvoir Local. |  |
| 2 | Décrivez la méthodologie utilisée pour transposer les besoins identifiés à la proposition technique |  |
| 3 | Décrivez la méthodologie utilisée pour présenter au Pouvoir local la proposition technique, vérifier l'adéquation aux besoins et faire valider la proposition |  |
| 4 | Décrivez la méthodologie utilisée pour vérifier et contrôler la bonne installation selon la proposition technique et les tests réalisés pour assurer l'adéquation de la solution implémentée au besoin identifié |  |
| 5 | Décrivez la méthodologie utilisée pour définir le contenu de la formation nécessaire. |  |
| 6 | Décrivez la méthodologie utilisée pour vérifier les acquis suite à la formation |  |
| 7 | Décrivez la méthodologie de renforcement et formation continue proposée aux Pouvoirs locaux découlant de l'installation réalisée. |  |
| 8 | Décrivez la méthodologie de réversibilité au terme du contrat. |  |

**Critère 4 - Qualité de la documentation (analyse, installation, projet)**

|  |  |  |
| --- | --- | --- |
| **#** | **Question** | **Réponse** |
| 1 | Décrivez la documentation d'analyse qui est réalisée. |  |
| 2 | Décrivez la documentation d'installation/configuration qui est réalisée. |  |
| 3 | Décrivez la documentation des procédures d'exploitation qui est faite. |  |
| 4 | Décrivez la documentation des incidents et de leurs procédures de solutionnement |  |
| 5 | Décrivez la documentation des failles constatées et leur mitigation du risque |  |
| 6 | Décrivez la documentation relative aux administrateurs qui est mise à leur disposition. |  |
| 7 | Décrivez la documentation relative aux utilisateurs qui est mise à leur disposition. |  |

**Critère 5 – Qualité technique**

|  |  |  |  |
| --- | --- | --- | --- |
| **#** | **Question** | **Conformité** | **Réponse** |
| 1 | Comment votre application permet le filtrage de base, telles que le filtrage des courriers indésirables, le filtrage du spam et le filtrage des virus ? | Oui – Non |  |
| 2 | Quelles sont les fonctionnalités avancées de filtrage, telles que la détection de phishing, le filtrage de contenu inapproprié et la protection contre les menaces avancées | Oui - Non |  |
| 3 | Par quel biais votre application permet-elle de s’intégrer avec les systèmes de messagerie existants des Pouvoirs locaux wallons ? | Oui - Non |  |
| 4 | Comment et par quel biais votre application permet-elle d’effectuer la gestion des règles de filtrage et la consultation des journaux de filtrage ? | Oui - Non |  |
| 5 | Comment votre application permet-elle de faire des mises à jour régulières du produit de filtrage des messages électroniques pour assurer sa conformité aux normes de sécurité et de confidentialité en vigueur ? | Oui - Non |  |
| 6 | Quels sont les outils de rapport et de gestion des performances pour permettre aux Pouvoirs locaux wallons de surveiller et d'optimiser l'efficacité du produit de filtrage des messages électroniques ? | Oui - Non |  |
| 7 | Comment votre application peut-elle intégrer le produit de filtrage des messages électroniques avec d'autres systèmes de sécurité et de gestion de la confidentialité des données ? | Oui - Non |  |
| 8 | Quelles sont les options de déploiement flexibles, telles que le déploiement en mode SaaS ou en mode hébergé ? | Oui - Non |  |
| 9 | Comment votre application permet-elle d’assurer la sécurité et la confidentialité des données traitées par le produit de filtrage des messages électroniques ? | Oui – Non |  |

**Critère 6 – Licence libre**

|  |  |  |
| --- | --- | --- |
| **#** | **Question** | **Réponse** |
| 1 | Le matériel ou le logiciel proposé est-il basé et reste lui-même sous licence libre ? Dans l'affirmative, quelle licence libre est-ce ? |  |

**Lot L4 – Antivirus/antimalware/EDR/XDR**

**Critère 2 – Maîtrise des domaines d’expertise liés à ce lot**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **#** | **Domaines d'expertise** | **Expert 1 - N° de CV** | **Expert 2 - N° de CV** | **Expert 3 - N° de CV** |
| 1 | Expertise en matière de sécurité informatique et de protection contre les menaces informatiques ; | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non |
| 2 | Connaissance approfondie des produits Antivirus/Antimalware/EDR/XDR, y compris leur fonctionnement et leurs caractéristiques techniques ; | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non |
| 3 | Compétences en matière de déploiement et de gestion de solutions de sécurité informatique ; | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non |
| 4 | Expérience en matière de conseil et de mise en place de politiques et de procédures de sécurité informatique ; | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non |
| 5 | Capacité à fournir un support technique et une formation aux utilisateurs finaux sur l'utilisation des produits Antivirus/Antimalware/EDR/XDR ; | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non |
| 6 | Connaissance des réglementations et des normes de sécurité informatique pertinents, y compris celles qui s'appliquent aux Pouvoirs locaux wallons ; | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non |
| 7 | Maîtrise de différentes technologies de protection contre les menaces informatiques, telles que les virus, les logiciels malveillants, les ransomwares, les botnets, etc. ; | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non |
| 8 | Connaissance approfondie des différents types de logiciels antivirus et antimalware, ainsi que de leurs fonctionnalités et de leur mode de fonctionnement ; | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non |
| 9 | Expérience dans la mise en place et la gestion de solutions de détection et de réponse avancées (EDR et XDR) dans des environnements informatiques complexes ; | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non |
| 10 | Capacité à évaluer les besoins en matière de sécurité informatique des Pouvoirs locaux et à recommander des solutions adaptées à leurs exigences ; | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non |
| 11 | Connaissance des réglementations et des normes en matière de sécurité informatique applicable aux Pouvoirs locaux ; | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non |

**Critère 3 - Méthodologie d’analyse et d’implémentation**

|  |  |  |
| --- | --- | --- |
| **#** | **Question** | **Réponse** |
| 1 | Décrivez la méthodologie utilisée pour cerner les besoins du Pouvoir Local. |  |
| 2 | Décrivez la méthodologie utilisée pour transposer les besoins identifiés à la proposition technique |  |
| 3 | Décrivez la méthodologie utilisée pour présenter au Pouvoir local la proposition technique, vérifier l'adéquation aux besoins et faire valider la proposition |  |
| 4 | Décrivez la méthodologie utilisée pour vérifier et contrôler la bonne installation selon la proposition technique et les tests réalisés pour assurer l'adéquation de la solution implémentée au besoin identifié |  |
| 5 | Décrivez la méthodologie utilisée pour définir le contenu de la formation nécessaire. |  |
| 6 | Décrivez la méthodologie utilisée pour vérifier les acquis suite à la formation |  |
| 7 | Décrivez la méthodologie de renforcement et formation continue proposée aux Pouvoirs locaux découlant de l'installation réalisée. |  |
| 8 | Décrivez la méthodologie de réversibilité au terme du contrat. |  |

**Critère 4 - Qualité de la documentation (analyse, installation, projet)**

|  |  |  |
| --- | --- | --- |
| **#** | **Question** | **Réponse** |
| 1 | Décrivez la documentation d'analyse qui est réalisée. |  |
| 2 | Décrivez la documentation d'installation/configuration qui est réalisée. |  |
| 3 | Décrivez la documentation des procédures d'exploitation qui est faite. |  |
| 4 | Décrivez la documentation des incidents et de leurs procédures de solutionnement |  |
| 5 | Décrivez la documentation des failles constatées et leur mitigation du risque |  |
| 6 | Décrivez la documentation relative aux administrateurs qui est mise à leur disposition. |  |
| 7 | Décrivez la documentation relative aux utilisateurs qui est mise à leur disposition. |  |

**Critère 5 – Qualité technique**

|  |  |  |  |
| --- | --- | --- | --- |
| **#** | **Question** | **Conformité** | **Réponse** |
| 1 | Comment votre application permet-elle une mise à jour automatique des définitions de virus et de menaces en temps réel ? | Oui – Non |  |
| 2 | Comment votre application permet-elle de détecter et bloquer les menaces connues et inconnues, y compris les ransomwares et les logiciels malveillants avancés ? | Oui - Non |  |
| 3 | Comment votre application fait-elle la gestion des licences et des déploiements simplifiés ? | Oui - Non |  |
| 4 | Quelles sont les certifications reconnues (par exemple, AV-Test, Virus Bulletin, ICSA Labs) et taux de détection élevé selon les tests indépendants ? | Oui - Non |  |
| 5 | Comment votre application permet-elle de détecter et éliminer les virus, logiciels malveillants et autres menaces informatiques en temps réel ? | Oui - Non |  |
| 6 | Quelle est la capacité de votre application à analyser les comportements suspects et à détecter les logiciels malveillants en utilisant des techniques de Machine Learning ? | Oui - Non |  |
| 7 | Quels outils de gestion de sécurité existants peuvent être intégrés à votre application ? | Oui - Non |  |
| 8 | Quelles sont les fonctionnalités de rapport et de surveillance pour suivre les activités de sécurité et détecter les incidents de sécurité potentiels ? | Oui - Non |  |
| 9 | Quelles Intégrations avec les outils de gestion de la sécurité existants du Pouvoir local, tels que les pare-feu et les gestionnaires de mots de passe, sont possibles ? | Oui – Non |  |

**Critère 6 – Licence libre**

|  |  |  |
| --- | --- | --- |
| **#** | **Question** | **Réponse** |
| 1 | Le matériel ou le logiciel proposé est-il basé et reste lui-même sous licence libre ? Dans l'affirmative, quelle licence libre est-ce ? |  |

**Lot L5 – Gestion des mots de passe**

**Critère 2 – Maîtrise des domaines d’expertise liés à ce lot**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **#** | **Domaines d'expertise** | **Expert 1 - N° de CV** | **Expert 2 - N° de CV** | **Expert 3 - N° de CV** |
| 1 | Gestion de la sécurité des mots de passe et des autorisations d'accès, avec une connaissance approfondie des standards et des bonnes pratiques en la matière ; | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non |
| 2 | Déploiement et gestion de solutions de gestion de mots de passe dans les environnements cloud et hybrides, avec une connaissance approfondie des architectures et des technologies cloud ; | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non |
| 3 | Intégration et synchronisation de solutions de gestion de mots de passe avec les annuaires d'utilisateurs et les systèmes d'authentification existants ; | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non |
| 4 | Support et maintenance de solutions de gestion de mots de passe, avec une capacité à résoudre rapidement les problèmes et à fournir un niveau élevé de disponibilité ; | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non |
| 5 | Formation et sensibilisation des utilisateurs aux bonnes pratiques de gestion de mots de passe et de sécurité informatique en général ; | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non |
| 6 | Développement et personnalisation de solutions de gestion de mots de passe, avec une capacité à adapter les fonctionnalités et l'interface utilisateur aux besoins spécifiques de l'organisation ; | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non |
| 7 | Conformité et réglementation en matière de gestion de mots de passe et de sécurité des données, avec une connaissance approfondie des réglementations et des normes en vigueur dans le domaine ; | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non |
| 8 | Gestion de la politique de sécurité des mots de passe, avec une capacité à définir et à mettre en œuvre des règles de sécurité strictes pour la création et l'utilisation de mots de passe ; | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non |
| 9 | Protection des mots de passe contre les attaques de type "force brute" et autres techniques de piratage ; | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non |
| 10 | Intégration de solutions de gestion de mots de passe avec les outils de gestion de la sécurité de l'information et de l'identité (par exemple, gestionnaire de stratégies de sécurité, gestionnaire d'identités et d'accès, etc.) ; | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non |
| 11 | Mécanismes de récupération de mots de passe en cas d'oubli ou de perte ; | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non |
| 12 | Prise en charge de l'authentification à deux facteurs ou multi facteurs pour renforcer la sécurité de l'accès aux systèmes et aux données ; | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non |
| 13 | Gestion de la vie privée et de la protection des données personnelles dans le cadre de la gestion de mots de passe, conformément aux réglementations en vigueur ; | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non |
| 14 | Expérience de travail avec les Pouvoirs locaux wallons et connaissance des spécificités et des exigences de cet environnement. | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non | Oui (+réf projet CV) - Non |

**Critère 3 - Méthodologie d’analyse et d’implémentation**

|  |  |  |
| --- | --- | --- |
| **#** | **Question** | **Réponse** |
| 1 | Décrivez la méthodologie utilisée pour cerner les besoins du Pouvoir Local. |  |
| 2 | Décrivez la méthodologie utilisée pour transposer les besoins identifiés à la proposition technique |  |
| 3 | Décrivez la méthodologie utilisée pour présenter au Pouvoir local la proposition technique, vérifier l'adéquation aux besoins et faire valider la proposition |  |
| 4 | Décriver la méthodologie utilisée pour vérifier et contrôler la bonne installation selon la proposition technique et les tests réalisés pour assurer l'adéquation de la solution implémentée au besoin identifié |  |
| 5 | Décrivez la méthodologie utilisée pour définir le contenu de la formation nécessaire. |  |
| 6 | Décriver la méthodologie utilisée pour vérifier les acquis suite à la formation |  |
| 7 | Décrivez la méthodologie de rencforcement et formation continue proposée aux Pouvoirs locaux découlant de l'installation réalisée. |  |
| 8 | Décrivez la méthodologie de réversibilité au terme du contrat. |  |

**Critère 4 - Qualité de la documentation (analyse, installation, projet)**

|  |  |  |
| --- | --- | --- |
| **#** | **Question** | **Réponse** |
| 1 | Décrivez la documentation d'analyse qui est réalisée. |  |
| 2 | Décrivez la documentation d'installation/configuration qui est réalisée. |  |
| 3 | Décrivez la documentation des procédures d'exploitation qui est faite. |  |
| 4 | Décrivez la documentation des incidents et de leurs procédures de solutionnement |  |
| 5 | Décrivez la documentation des failles constatées et leur mitigation du risque |  |
| 6 | Décrivez la documentation relative aux administrateurs qui est mise à leur disposition. |  |
| 7 | Décrivez la documentation relative aux utilisateurs qui est mise à leur disposition. |  |

**Critère 5 – Qualité technique**

|  |  |  |  |
| --- | --- | --- | --- |
| **#** | **Question** | **Conformité** | **Réponse** |
| 1 | Comment est-il possible de gérer les comptes et les accès des utilisateurs de manière sécurisée ? | Oui – Non |  |
| 2 | Par quel biais pouvez-vous faciliter le changement et la récupération de mots de passe ? | Oui - Non |  |
| 3 | Comment est-il possible de gérer les autorisations et les privilèges des utilisateurs de manière fine et granulaire ? | Oui - Non |  |
| 4 | Comment votre logiciel peut-il s'intégrer avec les différents systèmes et applications du Pouvoir local ? | Oui - Non |  |
| 5 | Par quels moyens votre logiciel peut-il imposer l'utilisation de mots de passe forts et complexes. | Oui - Non |  |
| 6 | Comment le gestionnaire de mot de passe permet-il aux Pouvoirs locaux de mettre en place un système de gestion de la sécurité des mots de passe, en utilisant des politiques de sécurité configurables et adaptées aux besoins du Pouvoir local ? | Oui - Non |  |
| 7 | Décrivez les atouts en termes de gestion simple et intuitive de l’application pour les utilisateurs et administrateurs. | Oui - Non |  |
| 8 | Avec quelles plateformes et environnements de travail utilisés votre outil de gestion centralisée des mots de passe est-il utilisable ? | Oui - Non |  |
| 9 | Comment le gestionnaire de mot de passe permet-il aux Pouvoirs locaux de suivre et d'auditer les activités de gestion des mots de passe, des logs et des journaux détaillés des opérations effectuées ? | Oui – Non |  |
| 10 | Votre logiciel permet-il la prise en charge de plusieurs domaines et de plusieurs annuaires d'utilisateurs, pour permettre la gestion centralisée des mots de passe de différents services et systèmes ? | Oui - Non |  |
| 11 | Quels sont les protocoles d'authentification, tels que LDAP, SAML, OAuth, RADIUS, etc., pour permettre l'intégration de votre logiciel avec systèmes tiers ? | Oui - Non |  |
| 12 | Comment est-il possible d’assurer une synchronisation des mots de passe avec les applications et les systèmes tiers, pour permettre la gestion centralisée et la synchronisation des mots de passe entre différents services et systèmes ? | Oui - Non |  |
| 13 | Comment votre application permet-elle l'authentification à deux facteurs et de l'authentification forte, pour renforcer la sécurité des mots de passe et éviter les attaques de type man-in-the-middle ? | Oui - Non |  |
| 14 | Comment votre application permet-elle la récupération des mots de passe oubliés et de la gestion des questions de sécurité, pour permettre aux utilisateurs de récupérer facilement leur mot de passe en cas d'oubli ? | Oui - Non |  |
| 15 | Quelle gestion fine et granulaire des autorisations et des privilèges des utilisateurs est réalisable par votre logiciel, en utilisant des rôles et des groupes d'utilisateurs personnalisables ? | Oui - Non |  |
| 16 | Comment votre logiciel rend-il possible la gestion de la politique de sécurité des mots de passe, en imposant des règles de complexité et de rotation des mots de passe, et en alertant les utilisateurs et les administrateurs en cas de violations de ces règles ? | Oui - Non |  |
| 17 | Comment votre logiciel intègre-t-il la gestion de la durée de vie des mots de passe, en imposant des délais de renouvellement et de validité des mots de passe, et en alertant les utilisateurs et les administrateurs en cas d’expiration prochaine ? | Oui – Non |  |
| 18 | Quelle est la prise en charge de la gestion des autorisations d'accès et des privilèges des utilisateurs, en permettant l'attribution et la révocation de droits et de permissions en fonction de l'identité de l'utilisateur et de son rôle dans l'organisation ? | Oui - Non |  |
| 19 | Comment faites-vous, dans votre logiciel, la gestion de la sécurité des sessions et des connexions, en permettant la déconnexion et la terminaison des sessions inactives et en protégeant les communications de bout en bout contre les attaques de type man-in-the-middle ? | Oui - Non |  |
| 20 | Quelle est la gestion de la sécurité des événements et des journaux, en permettant la collecte, l'analyse et l'alerte sur les événements de sécurité pertinents, tels que les tentatives d'accès non autorisées, les changements de configuration, les violations de politique, etc. ? | Oui - Non |  |
| 21 | Par quel biais assurez-vous la gestion de la sécurité des mots de passe dans les bases de données et les systèmes de gestion de données, en utilisant des méthodes de hachage et de chiffrement robustes pour protéger les mots de passe en base de données ? | Oui - Non |  |
| 22 | Quelles méthodes de synchronisation et de réplication sécurisées sont disponibles pour protéger les mots de passe dans les différentes instances et régions cloud ? | Oui - Non |  |
| 23 | Comment intégrez-vous la gestion de la sécurité des mots de passe dans les environnements hybrides, en permettant l'intégration et la synchronisation des mots de passe avec les annuaires d'utilisateurs on-premise et cloud ? | Oui - Non |  |

**Critère 6 – Licence libre**

|  |  |  |
| --- | --- | --- |
| **#** | **Question** | **Réponse** |
| 1 | Le matériel ou le logiciel proposé est-il basé et reste lui-même sous licence libre ? Dans l'affirmative, quelle licence libre est-ce ? |  |

1. **LISTE DES POUVOIRS ADJUDICATEURS BÉNÉFICIAIRES DE LA CENTRALE D’ACHAT**

“ FOURNITURE ET MAINTENANCE DE MATÉRIELS ET LOGICIELS RELATIFS À LA CYBERSÉCURITÉ ”

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Ville, commune** | **Type d'organisation** | **LOT M1 : Produit MFA** | **LOT M2 : pare-feu** | **LOT M3 : Sauvegarde des données sécurisées** | **LOT L1 : Journalisation des événements** | **LOT L2 : Projets liés à la gestion de l’authentification et à l’identification numérique** | **LOT L3 : Filtrage des messages électroniques** | **LOT L4 Antivirus/antimalware/EDR/XDR** | **LOT L5 : Gestion des mots de passe** |
| Total par lot | | 196 | 163 | 175 | 190 | 192 | 185 | 181 | 204 |
| Aiseau-Presles | AC | Oui | Oui | Oui | Oui | Oui | Oui | Oui | Oui |
| Aiseau-Presles | CPAS | Oui | Oui | Oui | Oui | Oui | Oui | Oui | Oui |
| Anderlues | CPAS | Oui | Oui | Oui | Oui | Oui | Oui | Oui | Oui |
| Anderlues | AC | Oui | Oui | Oui | Oui | Oui | Oui | Oui | Oui |
| Anhée | AC | Oui | Oui | Oui | Oui | Oui | Oui | Oui | Oui |
| Anhée | CPAS | Oui | Oui | Oui | Oui | Oui | Oui | Oui | Oui |
| Anthisnes | CPAS | Oui | Oui | Oui | Oui | Oui | Oui | Oui | Oui |
| Anthisnes | AC & CPAS | Oui | Non | Non | Oui | Oui | Oui | Non | Oui |
| Arlon | AC & CPAS | Oui | Oui | Oui | Oui | Oui | Oui | Oui | Oui |
| Ath | AC | Oui | Oui | Oui | Oui | Oui | Oui | Oui | Oui |
| Attert | AC | Non | Non | Oui | Oui | Oui | Oui | Non | Oui |
| Aubange | CPAS | Oui | Oui | Oui | Oui | Oui | Oui | Oui | Oui |
| Aubange | AC | Oui | Oui | Oui | Oui | Oui | Oui | Oui | Oui |
| Awans | AC | Oui | Oui | Oui | Oui | Oui | Oui | Oui | Oui |
| Aywaille | CPAS | Oui | Oui | Oui | Oui | Oui | Oui | Oui | Oui |
| Aywaille | AC | Oui | Oui | Oui | Oui | Oui | Oui | Oui | Oui |
| Bastogne | AC & CPAS | Oui | Non | Non | Oui | Oui | Oui | Oui | Oui |
| Bastogne | CPAS | Oui | Oui | Oui | Oui | Oui | Oui | Oui | Oui |
| Beauvechain | AC & CPAS | Oui | Non | Non | Non | Oui | Oui | Non | Non |
| Beloeil | AC | Oui | Oui | Oui | Oui | Oui | Oui | Oui | Oui |
| Berloz | AC | Oui | Oui | Oui | Oui | Oui | Oui | Oui | Oui |
| Bernissart | CPAS | Oui | Oui | Oui | Oui | Oui | Oui | Oui | Oui |
| Bièvre | AC & CPAS | Oui | Oui | Oui | Oui | Oui | Oui | Oui | Oui |
| Binche | AC | Oui | Non | Oui | Oui | Oui | Oui | Oui | Oui |
| Blégny | AC | Oui | Oui | Oui | Oui | Oui | Oui | Oui | Oui |
| Bouillon | AC | Oui | Oui | Oui | Oui | Oui | Oui | Oui | Oui |
| Boussu | CPAS | Oui | Oui | Oui | Oui | Oui | Oui | Oui | Oui |
| Boussu | AC | Oui | Oui | Oui | Oui | Oui | Oui | Oui | Oui |
| Braine-l'Alleud | AC & CPAS | Oui | Oui | Oui | Oui | Oui | Oui | Oui | Oui |
| Braine-le-Comte | AC | Oui | Non | Non | Oui | Oui | Non | Non | Oui |
| Braine-le-Comte | CPAS | Oui | Non | Non | Oui | Oui | Non | Non | Oui |
| Brunehaut | AC & CPAS | Oui | Oui | Oui | Oui | Oui | Oui | Oui | Oui |
| Cerfontaine | AC | Oui | Oui | Oui | Oui | Oui | Oui | Oui | Oui |
| Chapelle-lez-Herlaimont | AC & CPAS | Oui | Non | Non | Non | Non | Oui | Oui | Oui |
| Charleroi | AC | Oui | Non | Oui | Oui | Oui | Non | Non | Oui |
| Charleroi | CPAS | Oui | Oui | Oui | Oui | Oui | Oui | Oui | Oui |
| Chaudfontaine | AC & CPAS | Oui | Oui | Oui | Oui | Oui | Oui | Oui | Oui |
| Chaumont-Gistoux | AC & CPAS | Oui | Oui | Oui | Oui | Oui | Oui | Non | Oui |
| Chièvres | AC | Oui | Non | Non | Non | Non | Oui | Non | Non |
| Chièvres | CPAS | Oui | Non | Non | Non | Non | Oui | Non | Non |
| Clavier | AC | Oui | Oui | Oui | Non | Oui | Non | Oui | Oui |
| Clavier | CPAS | Oui | Non | Non | Oui | Non | Non | Oui | Oui |
| Comblain-au-Pont | AC | Non | Non | Oui | Oui | Oui | Oui | Oui | Oui |
| Comines-Warneton | AC | Oui | Non | Non | Oui | Oui | Non | Non | Oui |
| Courcelles | AC | Oui | Oui | Non | Oui | Oui | Oui | Oui | Oui |
| Courcelles | CPAS | Oui | Oui | Oui | Oui | Non | Non | Oui | Oui |
| Court-Saint-Etienne | AC | Oui | Oui | Oui | Oui | Oui | Oui | Oui | Oui |
| Couvin | CPAS | Oui | Oui | Oui | Oui | Non | Oui | Oui | Oui |
| Daverdisse | AC | Non | Non | Non | Oui | Oui | Non | Non | Oui |
| Daverdisse | CPAS | Oui | Oui | Oui | Oui | Oui | Oui | Oui | Oui |
| Dinant | AC & CPAS | Oui | Oui | Non | Oui | Oui | Oui | Oui | Oui |
| Dison | CPAS | Oui | Oui | Oui | Oui | Oui | Oui | Oui | Oui |
| Dison | AC | Oui | Oui | Oui | Oui | Oui | Oui | Oui | Oui |
| Dour | AC | Non | Oui | Oui | Oui | Oui | Oui | Oui | Oui |
| Dour | CPAS | Non | Oui | Oui | Oui | Oui | Oui | Oui | Oui |
| Ecaussinnes | CPAS | Non | Non | Non | Oui | Non | Oui | Non | Non |
| Ecaussinnes | AC | Non | Oui | Oui | Non | Non | Non | Non | Non |
| Enghien | CPAS | Oui | Oui | Oui | Oui | Oui | Oui | Oui | Oui |
| Engis | CPAS | Oui | Oui | Oui | Oui | Oui | Oui | Oui | Oui |
| Engis | AC | Oui | Oui | Oui | Oui | Oui | Oui | Oui | Oui |
| Erezée | AC | Non | Non | Non | Non | Non | Non | Non | Non |
| Erezée | CPAS | Non | Non | Non | Non | Non | Non | Non | Non |
| Esneux | AC | Oui | Non | Non | Oui | Oui | Oui | Oui | Oui |
| Estaimpuis | AC & CPAS | Oui | Oui | Oui | Oui | Oui | Oui | Oui | Non |
| Estinnes | AC | Oui | Oui | Oui | Oui | Non | Oui | Oui | Oui |
| Farciennes | AC | Oui | Non | Non | Non | Non | Non | Oui | Oui |
| Farciennes | CPAS | Oui | Oui | Oui | Oui | Oui | Oui | Oui | Oui |
| Fexhe-le-Haut-Clocher | AC | Oui | Oui | Oui | Oui | Oui | Oui | Oui | Oui |
| Fleurus | AC | Non | Non | Oui | Oui | Oui | Non | Non | Oui |
| Floreffe | AC & CPAS | Oui | Oui | Oui | Oui | Oui | Oui | Oui | Oui |
| Florennes | AC | Oui | Oui | Oui | Oui | Oui | Oui | Oui | Oui |
| Florenville | AC | Non | Non | Non | Non | Non | Non | Non | Oui |
| Fosses-la-Ville | AC | Oui | Non | Oui | Oui | Oui | Non | Non | Oui |
| Frameries | AC | Oui | Oui | Oui | Oui | Oui | Oui | Oui | Oui |
| Frameries | CPAS | Oui | Oui | Oui | Oui | Oui | Oui | Oui | Oui |
| Frasnes-lez-Anvaing | AC | Oui | Oui | Non | Non | Oui | Non | Non | Non |
| Froidchapelle | CPAS | Oui | Oui | Oui | Oui | Oui | Oui | Oui | Oui |
| Gembloux | AC | Oui | Oui | Oui | Oui | Oui | Oui | Oui | Oui |
| Genappe | AC | Oui | Oui | Oui | Oui | Oui | Oui | Oui | Oui |
| Gesves | CPAS | Oui | Oui | Oui | Oui | Oui | Oui | Oui | Oui |
| Gouvy | CPAS | Oui | Oui | Oui | Oui | Oui | Oui | Oui | Oui |
| Gouvy | AC | Oui | Oui | Oui | Oui | Oui | Oui | Oui | Oui |
| Grez-Doiceau | CPAS | Oui | Oui | Oui | Oui | Oui | Oui | Oui | Oui |
| Grez-Doiceau | AC | Oui | Oui | Oui | Oui | Oui | Oui | Oui | Oui |
| Habay | AC & CPAS | Oui | Oui | Oui | Oui | Oui | Oui | Oui | Oui |
| Hamois | AC | Oui | Oui | Oui | Oui | Oui | Oui | Oui | Oui |
| Hastière | AC | Oui | Oui | Oui | Oui | Oui | Oui | Oui | Oui |
| Havelange | AC | Oui | Oui | Oui | Oui | Oui | Oui | Oui | Oui |
| Hélécine | CPAS | Oui | Oui | Oui | Oui | Oui | Oui | Oui | Oui |
| Hélécine | AC | Oui | Oui | Oui | Oui | Oui | Oui | Oui | Oui |
| Hensies | CPAS | Oui | Oui | Oui | Oui | Oui | Oui | Oui | Oui |
| Hensies | AC | Oui | Oui | Oui | Oui | Oui | Oui | Oui | Oui |
| Herbeumont | AC & CPAS | Oui | Oui | Oui | Oui | Oui | Oui | Oui | Oui |
| Hotton | AC | Oui | Oui | Oui | Oui | Oui | Oui | Oui | Oui |
| Houffalize | AC | Oui | Oui | Oui | Oui | Oui | Oui | Oui | Oui |
| Houyet | AC | Oui | Oui | Oui | Oui | Oui | Oui | Oui | Oui |
| Huy | AC & CPAS | Oui | Oui | Oui | Oui | Oui | Oui | Oui | Oui |
| Ittre | AC | Oui | Oui | Oui | Oui | Oui | Oui | Oui | Oui |
| Jalhay | AC | Non | Oui | Oui | Oui | Non | Oui | Oui | Oui |
| Juprelle | CPAS | Oui | Non | Non | Non | Non | Non | Non | Oui |
| Juprelle | AC | Oui | Non | Non | Non | Non | Non | Non | Oui |
| Jurbise | AC | Oui | Oui | Oui | Oui | Oui | Oui | Oui | Oui |
| Jurbise | CPAS | Oui | Oui | Oui | Oui | Oui | Oui | Oui | Oui |
| La Bruyère | AC & CPAS | Oui | Oui | Oui | Oui | Oui | Oui | Oui | Oui |
| La Hulpe | AC | Oui | Non | Non | Non | Oui | Oui | Oui | Oui |
| La Roche-en-Ardenne | CPAS | Oui | Oui | Oui | Oui | Oui | Oui | Oui | Oui |
| La Roche-en-Ardenne | AC | Oui | Oui | Oui | Oui | Oui | Oui | Oui | Oui |
| Lasne | CPAS | Oui | Oui | Oui | Oui | Oui | Oui | Oui | Oui |
| Lens | AC & CPAS | Oui | Oui | Oui | Oui | Oui | Oui | Oui | Oui |
| Les Bons Villers | AC | Non | Non | Non | Non | Oui | Oui | Oui | Non |
| Lessines | CPAS | Non | Non | Oui | Oui | Oui | Oui | Oui | Oui |
| Leuze-en-Hainaut | CPAS | Oui | Oui | Oui | Oui | Oui | Oui | Oui | Oui |
| Leuze-en-Hainaut | AC | Oui | Oui | Oui | Oui | Oui | Oui | Oui | Oui |
| Libin | AC | Oui | Oui | Oui | Oui | Oui | Oui | Oui | Oui |
| Libramont-Chevigny | AC & CPAS | Oui | Oui | Oui | Oui | Oui | Oui | Oui | Oui |
| Libramont-Chevigny | AC | Oui | Oui | Oui | Oui | Oui | Oui | Oui | Oui |
| Liège | CPAS | Oui | Oui | Oui | Oui | Oui | Oui | Oui | Oui |
| Liège | AC | Oui | Oui | Oui | Oui | Oui | Oui | Oui | Oui |
| Lierneux | AC & CPAS | Oui | Non | Non | Oui | Oui | Oui | Non | Oui |
| Lincent | AC | Oui | Oui | Oui | Oui | Oui | Oui | Oui | Oui |
| Lincent | CPAS | Oui | Oui | Oui | Oui | Oui | Oui | Oui | Oui |
| Malmedy | AC | Oui | Non | Non | Non | Non | Non | Non | Non |
| Marche-en-Famenne | AC & CPAS | Oui | Oui | Oui | Oui | Oui | Oui | Oui | Oui |
| Meix-devant-Virton | AC | Oui | Oui | Oui | Oui | Oui | Oui | Oui | Oui |
| Merbes-le-Château | AC | Oui | Oui | Oui | Oui | Oui | Oui | Oui | Oui |
| Merbes-le-Château | CPAS | Oui | Oui | Oui | Oui | Oui | Oui | Oui | Oui |
| Messancy | AC | Oui | Non | Oui | Oui | Oui | Oui | Oui | Oui |
| Messancy | CPAS | Oui | Oui | Oui | Oui | Oui | Oui | Oui | Oui |
| Modave | CPAS | Oui | Oui | Oui | Oui | Oui | Oui | Oui | Oui |
| Momignies | AC & CPAS | Oui | Oui | Oui | Oui | Oui | Oui | Oui | Oui |
| Mont-de-l'Enclus | AC | Oui | Oui | Oui | Oui | Oui | Oui | Oui | Oui |
| Mont-Saint-Guibert | AC | Oui | Oui | Oui | Oui | Oui | Oui | Oui | Oui |
| Montigny-le-Tilleul | AC & CPAS | Oui | Oui | Oui | Oui | Oui | Oui | Oui | Oui |
| Morlanwelz | CPAS | Non | Non | Non | Non | Non | Non | Non | Non |
| Morlanwelz | AC | Oui | Oui | Oui | Oui | Oui | Oui | Oui | Oui |
| Namur | CPAS | Non | Non | Non | Non | Non | Non | Non | Oui |
| Namur | AC | Oui | Oui | Oui | Oui | Oui | Oui | Oui | Oui |
| Nandrin | AC & CPAS | Oui | Non | Oui | Oui | Oui | Oui | Oui | Oui |
| Nassogne | AC | Oui | Oui | Oui | Oui | Oui | Oui | Oui | Oui |
| Nassogne | CPAS | Oui | Oui | Oui | Oui | Oui | Oui | Oui | Oui |
| Nivelles | AC | Oui | Oui | Oui | Oui | Oui | Oui | Oui | Oui |
| Ohey | AC | Oui | Oui | Oui | Oui | Oui | Oui | Oui | Oui |
| Olne | AC | Oui | Oui | Oui | Oui | Oui | Oui | Oui | Oui |
| Onhaye | AC | Oui | Oui | Oui | Oui | Oui | Oui | Oui | Oui |
| Oreye | AC | Non | Oui | Oui | Non | Non | Oui | Non | Oui |
| Ottignies-Louvain-la-Neuve | AC | Oui | Oui | Oui | Oui | Oui | Oui | Oui | Oui |
| Oupeye | AC | Oui | Oui | Oui | Oui | Oui | Oui | Oui | Oui |
| Oupeye | CPAS | Oui | Oui | Oui | Oui | Oui | Oui | Oui | Oui |
| Paliseul | AC | Oui | Oui | Oui | Oui | Oui | Oui | Oui | Oui |
| Péruwelz | AC & CPAS | Oui | Oui | Oui | Oui | Oui | Oui | Oui | Oui |
| Perwez | AC | Oui | Oui | Oui | Oui | Non | Non | Oui | Non |
| Perwez | CPAS | Oui | Oui | Oui | Oui | Oui | Non | Oui | Non |
| Philippeville | AC | Oui | Oui | Oui | Oui | Oui | Oui | Oui | Oui |
| Pont-à-Celles | AC | Oui | Oui | Oui | Oui | Oui | Oui | Oui | Oui |
| Profondeville | CPAS | Oui | Oui | Non | Oui | Non | Non | Non | Oui |
| Profondeville | AC | Oui | Non | Oui | Oui | Oui | Non | Non | Oui |
| Quévy | AC | Oui | Non | Non | Non | Oui | Oui | Oui | Oui |
| Ramillies | AC | Oui | Oui | Oui | Oui | Oui | Oui | Oui | Oui |
| Ramillies | CPAS | Oui | Oui | Oui | Oui | Oui | Oui | Oui | Oui |
| Rebecq | AC | Oui | Oui | Oui | Oui | Oui | Oui | Oui | Oui |
| Rendeux | AC | Oui | Oui | Oui | Oui | Oui | Oui | Oui | Oui |
| Rendeux | CPAS | Oui | Oui | Oui | Oui | Oui | Oui | Oui | Oui |
| Rixensart | CPAS | Oui | Non | Oui | Oui | Non | Oui | Non | Oui |
| Rixensart | CPAS | Oui | Oui | Oui | Oui | Oui | Oui | Oui | Oui |
| Rixensart | AC | Oui | Non | Oui | Oui | Oui | Non | Non | Oui |
| Rochefort | AC | Oui | Non | Non | Oui | Non | Non | Oui | Oui |
| Rochefort | CPAS | Oui | Oui | Oui | Oui | Oui | Oui | Oui | Oui |
| Rouvroy | AC | Oui | Oui | Oui | Oui | Oui | Oui | Oui | Oui |
| Saint-Georges-sur-Meuse | AC & CPAS | Oui | Non | Non | Oui | Oui | Oui | Oui | Oui |
| Saint-Ghislain | AC | Oui | Non | Oui | Non | Oui | Oui | Non | Oui |
| Saint-Ghislain | CPAS | Oui | Non | Oui | Non | Oui | Oui | Non | Oui |
| Saint-Léger (Lux.) | AC | Oui | Oui | Oui | Oui | Oui | Oui | Oui | Oui |
| Saint-Nicolas | AC | Oui | Non | Non | Oui | Oui | Oui | Non | Oui |
| Sainte-Ode | AC | Oui | Oui | Oui | Oui | Oui | Oui | Oui | Oui |
| Sambreville | AC | Oui | Oui | Non | Oui | Oui | Oui | Oui | Oui |
| Sambreville | CPAS | Oui | Oui | Non | Oui | Oui | Oui | Oui | Oui |
| Seneffe | AC | Oui | Oui | Oui | Oui | Oui | Oui | Oui | Oui |
| Seneffe | CPAS | Oui | Oui | Oui | Oui | Oui | Oui | Oui | Oui |
| Seraing | AC | Oui | Non | Oui | Non | Oui | Non | Oui | Oui |
| Silly | AC | Oui | Oui | Oui | Oui | Oui | Oui | Oui | Oui |
| Silly | CPAS | Oui | Oui | Oui | Oui | Oui | Oui | Oui | Oui |
| Soignies | AC | Oui | Oui | Oui | Oui | Oui | Oui | Oui | Oui |
| Sombreffe | AC & CPAS | Non | Non | Non | Oui | Non | Non | Non | Non |
| Somme-Leuze | AC | Oui | Oui | Oui | Oui | Oui | Oui | Oui | Oui |
| Somme-Leuze | CPAS | Oui | Oui | Oui | Oui | Oui | Oui | Oui | Oui |
| Stavelot | AC | Non | Oui | Oui | Oui | Oui | Oui | Non | Non |
| Stavelot | CPAS | Oui | Oui | Oui | Oui | Oui | Oui | Oui | Oui |
| Tellin | AC | Oui | Oui | Oui | Oui | Oui | Oui | Oui | Oui |
| Theux | AC | Oui | Oui | Oui | Oui | Oui | Oui | Oui | Oui |
| Thimister-Clermont | AC & CPAS | Non | Non | Non | Non | Non | Non | Non | Oui |
| Thuin | AC | Oui | Oui | Oui | Oui | Oui | Oui | Oui | Oui |
| Tinlot | CPAS | Oui | Non | Non | Non | Non | Non | Oui | Oui |
| Tinlot | AC | Oui | Non | Non | Non | Oui | Non | Non | Oui |
| Tintigny | AC | Oui | Oui | Oui | Oui | Oui | Oui | Oui | Oui |
| Tournai | AC | Oui | Oui | Oui | Oui | Oui | Oui | Oui | Oui |
| Tournai | CPAS | Oui | Oui | Oui | Oui | Oui | Oui | Oui | Oui |
| Trooz | AC | Oui | Non | Oui | Non | Oui | Non | Non | Oui |
| Vaux-sur-Sûre | AC & CPAS | Oui | Non | Non | Oui | Oui | Non | Non | Oui |
| Verlaine | AC | Oui | Oui | Oui | Oui | Oui | Oui | Oui | Oui |
| Verviers | CPAS | Oui | Oui | Oui | Oui | Oui | Oui | Oui | Oui |
| Verviers | AC | Oui | Non | Non | Non | Oui | Oui | Oui | Oui |
| Villers-le-Bouillet | AC | Oui | Non | Non | Non | Non | Non | Non | Non |
| Virton | CPAS | Oui | Oui | Oui | Oui | Oui | Oui | Oui | Oui |
| Virton | AC | Oui | Oui | Non | Oui | Oui | Oui | Oui | Non |
| Visé | AC | Non | Oui | Oui | Oui | Oui | Non | Oui | Non |
| Visé | CPAS | Non | Non | Non | Oui | Non | Non | Non | Oui |
| Waimes | AC & CPAS | Non | Non | Oui | Oui | Oui | Oui | Non | Oui |
| Walcourt | AC | Non | Non | Non | Oui | Oui | Oui | Oui | Oui |
| Wanze | AC | Oui | Oui | Oui | Oui | Oui | Oui | Oui | Oui |
| Waremme | AC | Oui | Oui | Oui | Oui | Oui | Oui | Oui | Oui |
| Waterloo | CPAS | Oui | Oui | Oui | Oui | Oui | Oui | Oui | Oui |
| Wavre | CPAS | Oui | Oui | Oui | Oui | Oui | Oui | Oui | Oui |
| Welkenraedt | AC | Oui | Oui | Oui | Oui | Oui | Oui | Oui | Oui |
| Wellin | AC | Oui | Oui | Oui | Oui | Oui | Oui | Oui | Oui |
| Yvoir | AC | Oui | Oui | Oui | Oui | Oui | Oui | Oui | Oui |
| Namur | AC | Non | Non | Oui | Oui | Oui | Oui | Oui | Oui |
| Walhain | AC | Non | Non | Oui | Non | Oui | Oui | Oui | Oui |
| Gesves | AC | Oui | Non | Non | Non | Non | Oui | Oui | Oui |
| Cerfontaine | CPAS | Oui | Oui | Oui | Oui | Oui | Oui | Oui | Oui |
| Chimay | AC | Oui | Non | Non | Non | Oui | Oui | Oui | Oui |
| Walcourt | AC | Non | Non | Non | Non | Non | Non | Oui | Oui |
| Chimay | CPAS | Oui | Oui | Oui | Oui | Oui | Oui | Oui | Oui |
| Fléron | CPAS | Oui | Oui | Oui | Oui | Oui | Oui | Oui | Oui |
| Somme-Leuze | AC | Oui | Oui | Oui | Oui | Oui | Oui | Oui | Oui |

1. **RAPPORT DE LIVRAISON**

**“ FOURNITURE ET MAINTENANCE DE MATÉRIELS ET LOGICIELS RELATIFS À LA CYBERSÉCURITÉ ”**

Le rapport de livraison doit au minimum contenir les éléments suivants et être transmis à iMio après signature pour réception par le PAB. Aucune prestation ou livraison ne faisant pas l’objet d’un rapport de livraison complété tel que demandé et signé par le représentant du fonctionnaire dirigeant du PAB ne peut faire l’objet d’une facturation.

Titre : RAPPORT DE LIVRAISON

Coordonnées PAB

* AC-CPAS de XYZ
* Rue N°
* CP Commune
* Date adhésion à la CA Cybersécurité
* Fonctionnaire dirigeant et identification de son représentant

Coordonnées Adjudicataire

* Nom de société
* Rue N°
* CP Commune

Centrale d’achat : “FOURNITURE ET MAINTENANCE DE MATÉRIELS ET LOGICIELS RELATIFS À LA CYBERSÉCURITÉ”

Références dossier :

* N° de marché / centrale d’achat
* N° de bon de commande PAB
* N° de devis réalisé par le prestataire

Ci-après dénommé le client : "Nom du PAB”

* Le client, représenté par la personne de contact " Fonctionnaire dirigeant et identification de son représentant“ réceptionne en date du \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ les livrables suivants avec satisfaction :
* Description des matériels, logiciels et services fournis/prestés

Les anomalies ou points d’attentions suivants doivent être suivis :

* Description exhaustive des éléments nécessitant encore un suivi, ces éléments doivent être mineurs et en aucun cas n’empêcher le bon fonctionnement des matériels/logiciels fournis

La signature de ce rapport de livraison vaut pour acceptation des matériel/logiciel/prestations dont ce rapport de livraison fait mention.

Signatures :

* Représentant fonctionnaire dirigeant PAB
* Représentant adjudicataire

1. **DELIBERATION D’ADHESION A LA CENTRALE D’ACHAT**

**“ FOURNITURE ET MAINTENANCE DE MATÉRIELS ET LOGICIELS RELATIFS À LA CYBERSÉCURITÉ ”**

Une délibération d’adhésion a été mise à disposition de tous les PAB, la voici : <https://www.imio.be/cda/cybersecurite/phase-1-audits-prealables/deliberation_conseil.docx/view>

Cette décision d’adhésion doit avoir été prise par le PAB pour que les adjudicataires du marché puissent leur faire une proposition dans le cadre de cette centrale d’achat.

1. **ENGAGEMENTS SUR L’OBLIGATION DE RÉSULTATS**

**“ FOURNITURE ET MAINTENANCE DE MATÉRIELS ET LOGICIELS RELATIFS À LA CYBERSÉCURITÉ ”**

Dans cette annexe, le soumissionnaire répond à chacun des points évoqués dans chacune des sections « Obligations de résultat » correspondante au lot soumissionné, il faut donc une annexe G par lot auquel le soumissionnaire remet une offre.

Exemple :

Chaque lot possède une section liée aux obligations de résultats, à titre d’exemple voici la section du lot L3 – Filtrage de messages électroniques :

Nous demandons à chaque soumission de nous faire parvenir les éléments suivants auquel vous vous engagez :

* Un taux de détection de spam supérieur à X%
* Un taux de détection de virus supérieur à Y%
* Un taux de faux positifs inférieur à Z%
* Un temps de réponse inférieur à T secondes pour la réception et le traitement des messages électroniques
* Une disponibilité de service supérieure à X% en termes de temps de fonctionnement ininterrompu par mois
* Une assistance technique disponible H/24 et 7/7 avec un délai de réponse maximum de Y heures pour les demandes de niveau 1 et de Z heures pour les demandes de niveau 2
* Des mises à jour logicielles et de sécurité mensuelles ou trimestrielles
* Une formation initiale et continue pour les utilisateurs finaux sur l'utilisation du produit et ses fonctionnalités
* Un suivi régulier de la performance du produit et de la satisfaction des utilisateurs avec la mise en place de plans d'actions en cas de défaillance ou de problème.

En réponse à ces éléments, le soumissionnaire répond point par point dans cette annexe. Cet exemple doit être supprimé de la soumission.