Termes de référence :

Recrutement d'un cabinet pour fournir les services informatiques au Secrétariat général de la COI

I- INTRODUCTION :

La Commission de l'océan Indien (COI) est une organisation intergouvernementale qui regroupe cinq États membres : l'Union des Comores, la France au titre de La Réunion, Madagascar, Maurice et les Seychelles.

Seule organisation régionale d'Afrique composée exclusivement d'îles, elle défend les spécificités de ses États membres sur les scènes continentale et internationale. Bénéficiant du soutien actif d'une dizaine de partenaires internationaux, la COI donne corps à la solidarité régionale à travers une coopération couvrant un large éventail de domaines et un portefeuille croissant de projets de coopération.

La COI est engagée, depuis 2019, dans un processus de modernisation et de réforme institutionnelle pour laquelle elle a reçu le soutien de l'Union européenne (UE), à travers le Programme de Renforcement des Capacités Institutionnelles (INCA 2019-2021) et continue de recevoir l'appui de l'UE et de l'AFD à travers le Programme COI-Horizon 2030 (2022-2026). Cet appui vise à une mise à niveau des capacités organisationnelles de la COI par la mise en place, le déploiement et l'utilisation effective de procédures et outils de gestion et de contrôle, conformément aux meilleurs standards internationaux et aux bonnes pratiques reconnues. dans le cadre, notamment, de l'accréditation aux 9 piliers de l'UE ainsi qu'au Fonds vert pour le climat (FVC).

Dans cet élan, le Secrétariat général (SG-COI) est appelé à renforcer son environnement informatique TIC pour mieux répondre aux exigences liées aux accréditations et pour soutenir techniquement l'équipe du Secrétariat général et des projets dans le déploiement et l'utilisation des différents outils et logiciels qui seront mis en place notamment au niveau de la gestion des Ressources humaines, de la comptabilité, des marchés et contrat, de l'audit interne, du suivi-évaluation et contrôle interne, de la Gestion Électronique des Documents et Gestion Électronique des Courriers (GEC et GED), etc.

II OBJECTIFS :

L'objectif principal de cette prestation est de garantir un environnement informatique fonctionnel, efficient, sécurisé et conforme aux normes internationales pour les agents du Secrétariat général de la COI.

Plus spécifiquement, cette prestation devra permettre à la COI de :

- Assurer la conformité aux exigences du Secrétariat général et de ses partenaires, tout en maintenant un environnement informatique fiable et sécurisé. Cela inclut une utilisation optimale et conforme des ressources matérielles et logicielles, ainsi que l'intégration des technologies émergentes et la digitalisation des outils professionnels.
- Garantir le respect des réglementations en vigueur, notamment en matière de protection des données comme le RGPD, et de gérer efficacement les risques liés à l'utilisation des outils informatiques, en particulier en matière de cybersécurité.
- Mettre en place des indicateurs clés de performance (KPIs) afin de mesurer la disponibilité des systèmes, la rapidité de résolution des incidents et la satisfaction des utilisateurs

III OBJET DE LA MISSION

Le prestataire de support informatique devra assurer le bon fonctionnement des systèmes informatiques afin, notamment, de prévenir ou d'anticiper les dysfonctionnements numériques, de pouvoir diagnostiquer et de résoudre les problèmes et faiblesses. Il devra également pouvoir former les utilisateurs aux fonctions de base des matériels et veiller à ce que les utilisateurs en tirent le maximum d'avantages. Le prestataire devra adopter une approche basée sur les meilleures pratiques (Information Technology/Infrastructure Library) ITIL pour la gestion des incidents, des demandes de services et des problèmes. La gestion des changements devra se faire selon une procédure validée avec le Secrétariat général afin de minimiser les impacts opérationnels.

Les responsabilités sont les suivantes :

A. Support aux agents de la COI et renforcement des capacités au niveau de l'environnement informatique

- Fournir une assistance technique, sur site et à distance, pour les opérations matérielles et logicielles, 24h/24 et 7j /7, en garantissant des interventions techniques dans les meilleurs délais.
- Fournir une formation de base sur les logiciels et équipements actuellement déployés et qui seront mis en place ainsi que des conseils aux utilisateurs finaux pour optimiser leur utilisation.

- Recommander et, le cas échéant accompagner, le déploiement de nouvelles applications informatiques : installation, formation, contrôle, suivi.

- Améliorer l'expérience utilisateur en soutenant les agents de la COI et autres utilisateurs concernés dans l'utilisation optimale des matériels et logiciels et en assurant la liaison avec les structures pertinentes à cette fin.- Assurer une assistance aux utilisateurs informatiques sur site, par téléphone, e-mail et à distance, en résolvant leurs problèmes techniques et en fournissant la documentation procédurale lorsque nécessaire, tout en utilisant un système de « ticket électronique » pour suivre et gérer les demandes de support.

- Aider les utilisateurs finaux à transférer des données par voie électronique avec les procédures de sécurité requises (ex : clé de chiffrement, mot de passe etc)

- Préparer et diffuser les communications internes liées aux TIC – e-mails, manuels, dépliants, bonnes pratiques, FAQ…

B. Infrastructure TIC et accessibilité aux services et solutions TIC :

- Installer, configurer, surveiller, entretenir, gérer (y compris le renouvellement des équipements et licences) le matériel informatique, les réseaux, les systèmes d'exploitation et les applications (ordinateurs, logiciels, équipements d'impression, système de vidéoconférence et de téléphonie, et serveurs).
- Surveiller et entretenir les systèmes et réseaux informatiques, y compris la téléphonie, la vidéoconférence, l'équipement d'impression et les connexions Internet.
- Prévenir les risques de pannes matérielles et logicielles par un suivi régulier et efficace des utilisation et échéances
- Diagnostiquer les pannes et problèmes puis assurer les dépannages et/ou configurations adéquates, tant sur les matériels que les réseaux et logiciels, en suivant des instructions écrites, dont les manuels utilisateurs des pourvoyeurs de matériels / logiciels, tant sur site qu'à distance.
- Créer des comptes et des profils utilisateurs, gérer les mots de passe et assurer le contrôle d'accès de tout agent de sa prise de fonction et à sa cessation de fonction.
- Identifier et corriger ou conseiller sur les problèmes opérationnels avec les systèmes informatiques des utilisateurs finaux.
- Gérer les sauvegardes de tous les systèmes en s'assurant qu'elles fonctionnent correctement et gérer la rotation des sauvegardes hors

site pour un stockage sécurisé ainsi qu'assurer des tests annuels des sauvegardes.

- Mettre régulièrement à jour les systèmes et les serveurs avec les mises à jour logicielles approuvées en suivant la procédure de gestion des modifications.
- Surveiller les alertes des journaux du réseau, du système et du serveur, en suivant tout problème de sécurité ou de performances.
- Assurer une veille technologique et, le cas échéant, tester et évaluer les nouvelles technologies selon les exigences et besoins actuels et prévus de la COI
- Contribuer à établir les spécifications techniques des équipements et logiciels informatiques selon les besoins de la COI. Lors des processus de passation de marchés, participer aux comités d'évaluation des offres en tant qu'observateur si requis.
- Gérer l'équipement audiovisuel lors de réunions, de conférences ou de formations et gérer les ressources audiovisuelles.
- Participer à la mise en œuvre des politiques informatiques et sécurité informatique.
- Travailler en étroite collaboration avec le Secrétariat général ou toute autre expert ou entité dûment habilitée par la COI pour la sécurité informatique pour maintenir la conformité avec les pratiques et normes de sécurité. *Le prestataire devra réaliser des audits réguliers de sécurité des systèmes, y compris des tests d'intrusion, et fournir des recommandations pour corriger les vulnérabilités identifiées. Un rapport semestriel de sécurité doit être fourni au Secrétariat général.*
- Assurer la maintenance des réseaux, des systèmes et des applications conformément au « Service Level agreement » (SLA) des fournisseurs.
- Le prestataire devra réaliser des maintenances proactives et fournir un rapport mensuel sur l'état des systèmes, incluant l'évaluation des risques, la gestion des vulnérabilités et les mises à jour critiques des systèmes et logiciels.

C. Administration TIC :

- Maintenir le système de 'ticket électronique', en enregistrant tous les incidents et demandes, leurs accusés de réception et leurs résolutions et en garantissant que tous les tickets d'assistance sont traités efficacement et rapidement selon les procédures internes définies.

- En lien avec les services du Secrétariat général, confirmer les besoins en matériels et logiciels, suivre l'acquisition et vérifier la conformité des équipements reçus.
- Soutenir, les collaborateurs ponctuels, les invités, participants aux réunions pour se connecter aux outils TIC conformément à la politique IT.
- Appuyer techniquement le SG-COI dans l'application des recommandations issues des rapports d'audit sur l'informatique.
- S'assurer d'une connectivité optimale du réseau informatique.
- Proposer des solutions optimales permettant la réalisation d'économies d'échelle.

D. Plan de continuité des activités :

Mise en place d'un processus de gestion des incidents structuré afin de garantir une réponse rapide et efficace aux situations critiques informatiques. Ce processus permettra d'identifier, de gérer et de résoudre les incidents de manière à minimiser les interruptions de service. Le prestataire devra ainsi fournir un plan de continuité des activités (BCP) détaillé, spécifiquement conçu pour les situations critiques, telles que des pannes majeures ou des cyberattaques etc. Ce plan doit inclure des procédures pour assurer la disponibilité des systèmes essentiels, la protection des données et la reprise rapide des activités, afin de limiter les impacts sur les opérations du Secrétariat général et de garantir la résilience organisationnelle face aux imprévus.

IV – PRODUITS/LIVRABLES

- Rapport mensuel d'intervention faisant ressortir : (i) l'état des systèmes, (ii) les appuis effectués, (iii) les problèmes rencontrés, et (iv) les solutions préconisées pour la pérennisation et la bonne marche du système informatique de la COI. Rapport à remettre au plus tard le dix (10) du mois suivant.
- Rapport semestriel de sécurité au Secrétariat général.

V - DUREE DE LA MISSION

Un (01) an renouvelable après évaluation concluante de l'intervention faite par la COI.

VI - PROFILS DU CABINET ET COMPOSITION DE L'EQUIPE :

- Cabinet informatique constitué légalement, existant depuis au moins 10 ans.
- Ayant une expérience avec organismes, institutions et compagnies de référence international ou régional.

- Implanté à Maurice ou disposant d'une antenne à Maurice.
- Disposant d'au moins cinq (05) personnels permanents.
- Ayant assuré une assistance informatique permanente auprès des entreprises ou organisation dans la sous-région ou autre pendant au moins deux (02) ans.
- Dirigé par un ingénieur informatique disposant d'au moins dix (10) ans d'expérience professionnelle
- Pouvant déployer de manière permanente au moins deux techniciens informatiques (niveau Bac +3) et disposant d'au moins cinq (05) années d'expérience professionnelle en matière d'assistance aux entreprises ou organisations.
- Le prestataire doit disposer de certifications reconnues dans le domaine des services informatique et de la sécurité des systèmes d'information (ex. ISO/IEC 27001, ISO/IEC 20000, ou tout autre certification équivalente ou pertinente) et justifier d'une expérience avérée dans la gestion informatique conforme aux standards ITIL
- Pouvant assurer une assistance rapide et rapprochée à la demande et pouvant intervenir au plus-tard, trois heures après avoir été saisie pour une assistance.

VII – Ethique et confidentialité.

Le prestataire devra se conformer scrupuleusement aux règles en vigueur au sein de la COI.
Le Cabinet retenu signera une lettre d'engagement de confidentialité avec la COI avant ses interventions. Ladite lettre fera partie intégrante du contrat.

Le cabinet doit s'engager à respecter des accords de niveau de service (SLA - Service Level Agreement) stricts, définissant des objectifs clairs de disponibilité des systèmes, de temps de réponse et de résolution des incidents, ainsi qu'une conformité totale aux normes de cybersécurité et de protection des données.

La responsabilité civile, pénale et financière du prestataire pourra être engagée en cas de non-respect des obligations prévues dans la lettre d'engagement de confidentialité, ou de toute violation des textes, dispositions, lois et règlements en vigueur à la COI. Toute infraction à ces engagements pourra entraîner des conséquences juridiques et financières pour le prestataire, incluant des poursuites civiles et pénales ainsi que des sanctions financières proportionnelles aux dommages subis par la COI. Cette clause vise à garantir le strict respect des obligations de confidentialité et à protéger les intérêts de la COI.