BANQUE DE LA RÉPUBLIQUE
DU BURUNDI

AVIS D'APPEL D'OFFRES INTERNATIONAL POUR LE RENOUVELLEMENT DE LA LICENCE DE L'ANTIVIRUS KASPERSKY A LA BANQUE DE LA REPUBLIQUE DU BURUNDI

La Banque de la République du Burundi, à travers son site web www.brb.bi et le quotidien « Le RENOUVEAU », lance un Avis d'Appel d'Offres International pour le renouvellement de la licence de l'antivirus Kaspersky pour une période d'une année à compter du 22 octobre 2022.

Le Dossier d'Appel d'Offres peut être consulté sur le site web www.brb.bi ou auprès du Service Logistique et Patrimoine de la BRB, 2ème étage, bureau n° 2.08, Tél. (+257) 22 20 40 98.

La participation au marché est ouverte à égalité de conditions, à toutes les personnes morales pouvant justifier par leurs offres qu'elles ont des capacités juridiques, techniques et financières requises pour l'exécution du présent marché.

Ne peut participer à l'appel d'offres toute personne morale frappée par l'un ou l'autre des critères d'inéligibilité aux marchés de la BRB énumérées à l'article 8 du Règlement de Passation des Marchés de la Banque de la République du Burundi, disponible sur le site www.brb.bi.

Les offres sous plis fermés doivent parvenir au Secrétariat de Direction de la Banque (5ème étage) au plus tard le **11/10/2022** à dix heures (**10h00'**). Passé ce délai, aucune offre ne sera acceptée.

L'ouverture des offres aura lieu le même jour à 10 heures et 30 minutes (**10h30'**), dans la salle des réunions du 4ème étage de la Banque de la République du Burundi, en présence des soumissionnaires ou leurs représentants qui le souhaitent.

Fait à Bujumbura, le 28/09/2022

BANQUE DE LA REPUBLIQUE DU BURUNDI

MINANI Cécile
Directrice de l'Administration et de la Comptabilité

Marie Goreth NDAYISHIMIYE
2ème Vice-Gouverneur

1, avenue du Gouvernement- B.P. 705 BUJUMBURA-Tél: (257) 22204000/22204001- Fax : (257) 22223128 - Courriel : brb@brb.bi

BANQUE DE LA REPUBLIQUE DU BURUNDI

DOSSIER D'APPEL D'OFFRES INTERNATIONAL POUR LE RENOUVELLEMENT DE LA LICENCE DE L'ANTIVIRUS KASPERSKY A LA BANQUE DE LA REPUBLIQUE DU BURUNDI

BANQUE DE LA REPUBLIQUE DU BURUNDI
BRB
Logistique et Patrimoine

Bujumbura, septembre 2022

PARTIE I. AVIS D'APPEL D'OFFRES INTERNATIONAL

1. Objet du marché

La Banque de la République du Burundi, à travers son site web www.brb.bi et le quotidien « Le RENOUVEAU », lance un Avis d'Appel d'Offres International pour le renouvellement de la licence de l'antivirus kaspersky pour une période d'une année à compter du 22 octobre 2022 .

2. Financement

Le financement est assuré par les fonds propres de la Banque de la République du Burundi.

3. Délai d'exécution

Les activités prévues dans le cadre de l'exécution de ce marché sont à réaliser dans un délai maximum de sept (7) jours calendrier comptés à partir de la signature du contrat.

4. Condition de Participation

La participation au marché est ouverte à égalité de conditions, à toutes les personnes morales pouvant justifier par leurs offres qu'elles ont des capacités juridiques, techniques et financières requises pour l'exécution du présent marché.

Ne peut participer à l'appel d'offres toute personne morale frappée par l'un ou l'autre des critères d'inéligibilité aux marchés de la BRB énumérées à l'article 8 du Règlement de Passation des Marchés de la Banque de la République du Burundi, disponible sur le site www.brb.bi

5. Contenu du Dossier d'Appel d'Offre

Le Dossier d'Appel d'Offre est constitué par les documents suivants :

- L'Avis d'Appel d'Offres

- Les Données Particulières de l'Appel d'Offres

6. Consultation du Dossier d'Appel d'Offres

Le Dossier d'Appel d'Offres peut être consulté sur le site web www.brb.bi ou auprès du Service Logistique et Patrimoine de la BRB, 2ème étage, bureau n° 2.08,Tél. (+257) 22 20 40 98.

7. Présentation des offres

Les offres, rédigées en français et accompagnées des différents documents exigés (voir point 8), seront présentées en quatre (4) exemplaires dont un (1) original et trois (3) copies et seront présentées dans deux (2) enveloppes fermées et séparées, comportant la mention **« OFFRE TECHNIQUE »** et **« OFFRE FINANCIERE ».**

Les deux (2) enveloppes seront glissées dans une enveloppe extérieure fermée portant la mention « **Offre pour le renouvellement de la licence de l'antivirus kaspersky à la Banque de la République du Burundi** ».

Les enveloppes contenant les offres technique et financière seront envoyées à l'adresse ci-après :

Monsieur le Gouverneur de la Banque de la République du Burundi
1, Avenue du Gouvernement
B.P. 705 Bujumbura
Tél. (+257) 22 20 40 00/Fax. (+257) 22 22 3128
E-mail : brb@brb.bi

Outre cette adresse, l'enveloppe extérieure portera les inscriptions: **« A n'ouvrir qu'en séance d'ouverture des offres ».**

L'enveloppe extérieure ne doit comporter aucun signe distinctif du soumissionnaire.

Toute enveloppe ouverte ou ne respectant pas la formalisation ci-dessus ne pourra pas être acceptée.

8. Contenu des offres

L'offre technique devra contenir :

a. Les documents administratifs :

BANQUE DE LA REPUBLIQUE DU BURUNDI
BRB
Logistique et Patrimoine

- La lettre de soumission signée par une personne ayant les pouvoirs d'engager la société soumissionnaire, accompagnée par une procuration écrite authentifiée par un notaire en cas de délégation ;

- Les statuts de la firme et son organigramme ;
- Le certificat d'immatriculation au registre de commerce ;
- Le numéro d'identification fiscale (NIF) ;
- Trois (3) références des marchés similaires exécutés avec preuve de bonne exécution à l'appui au cours des cinq (5) dernières années
- Un certificat valide de partenariat avec l'éditeur de l'Antivirus « Kaspersky Lab » (B2B certificat).
- Le délai d'exécution

b. <u>Les fonctionnalités de la clé de la licence de l'antivirus</u> :

L'offre garantira que la clé de l'antivirus fournira à la Banque ces fonctionnalités :

1. PROTECTION FROM KNOWN, UNKNOWN AND ADVANCED THREATS

- Best-in-class anti-malware combines with Automatic Exploit Prevention and Real-time cloud-assisted security intelligence from Kaspersky Security Network to provide proactive, targeted protection against the latest threats.
- System Watcher provides unique file restoration capabilities while Host-based Intrusion Prevention System (HIPS) with Personal Firewall help secure and control application and network activity.

2. ENDPOINT CONTROLS

- Application Control with Dynamic Whitelisting — using real-time file reputations from the Kaspersky Security Network, IT administrators can allow, block or regulate applications, including operating 'Default Deny' whitelisting in a live or test environment.
- Application Privilege Control and Vulnerability Scanning monitor applications and restrict those performing suspicious.
- Web Control — browsing policies can be created around pre-set or customizable categories, ensuring comprehensive oversight and administrative efficiency.
- Device Control — granular data policies controlling the connection of removable storage and other peripheral devices can be set, scheduled and enforced, using masks for simultaneous deployment to multiple devices.

3. FILE SERVER SECURITY

- Managed together with endpoint security through Kaspersky Security Center.

4. MOBILE SECURITY

- Powerful Security for Mobile Devices — advanced, proactive and cloud-assisted technologies deliver multi-layered real-time mobile endpoint protection.
- Web protection, anti-spam and anti-phishing components further increase device security.
- Remote Anti-Theft — Lock, Wipe, Locate, SIM Watch, Alarm, Mugshot and Full or Selective Wipe prevent unauthorized access to corporate data if a mobile device is lost or stolen. Administrator and end-user enablement, together with Google Cloud Management support, delivers quick activation if required.
- Mobile Application Management (MAM) — controls limit users to running whitelisted applications, preventing the deployment of unwanted or unknown software.

'Application wrapping' isolates corporate data on employee owned devices. Additional encryption or 'Selective Wipe' can be remotely enforced.

- Mobile Device Management (MDM) — a unified interface for Microsoft® Exchange ActiveSync and iOS MDM devices with OTA (Over the Air) policy deployment. Samsung KNOX for Android™-based devices is also supported.
- Self-Service Portal — allows self-registration of employee-owned approved devices onto the network with automatic installation of all required certificates and keys, and user/owner emergency activation of anti-theft features, reducing the IT administrative workload

5. SYSTEMS MANAGEMENT

- Vulnerability and Patch Management — automated OS and application vulnerability detection and prioritization, combined with rapid, automated distribution of patches and updates.
- Operating System Deployment — easy creation, storage and deployment of OS golden images from a central location, including UEFI support.
- Software Distribution and Troubleshooting — remote software deployment, application, and OS update available on-demand or scheduled, including Wake-on-LAN support. Time-saving remote troubleshooting and efficient software distribution is supported through Multicast technology.
- Hardware and Software Inventories and Licensing Management — identification, visibility and control (including blocking), together with license usage management, provides insight into all software and hardware deployed across the environment, including removable devices. Software and hardware license management, guest device detection, privilege controls and access provisioning are also available.
- SIEM Integration — support for IBM® QRadar and HP ArcSight SIEM systems.
- Role Based Access Control (RBAC) — administrative responsibilities can be assigned across complex networks, with console views customized according to assigned roles and rights.

6. ENCRYPTION

- Powerful Data Protection — file/folder (FLE) and Full Disk (FDE) encryption can be applied to endpoints. Support for "portable mode" ensures encryption administration across devices leaving administrative domains.
- Flexible User Login — pre-boot authentication (PBA) for added security includes optional 'single sign-on' for user transparency. 2-factor or token based authentication is also available.
- Integrated Policy Creation — unique integration of encryption with application and device controls provides an additional layer of security and administrative ease.

N.B : L'absence de l'un des éléments énumérés ci-dessus (a et b) constitue une cause de rejet de l'offre.

L'offre financière devra contenir les documents suivants :

- La lettre de soumission financière
- Le bordereau du prix Taxe sur Valeur Ajoutée Comprise (TVAC)

10. Dépôt des offres et ouverture des offres

Les offres sous plis fermés doivent parvenir au Secrétariat de Direction de la Banque (5ème étage) au plus tard le 11/10/2022 à dix heures (10h00'). Passé ce délai, aucune offre ne sera acceptée.

L'ouverture des offres aura lieu le même jour à 10 heures et 30 minutes (10h30'), dans la salle des réunions du 4ème étage de la Banque de la République du Burundi, en présence des soumissionnaires qui le souhaitent.

11. Critères d'évaluation des offres

- Seront qualifiées au moment de l'analyse des offres techniques :
  - Les offres contenant tous les documents administratifs exigés.
  - Les offres qui acceptent de fournir la clé de la licence avec les fonctionnalités exigées (celle de Kaspersky Endpoint Security for Business Advanced).
  - Les offres présentant un délai d'exécution conforme au délai d'exécution exigé.

N.B : les offres qui n'auront pas présentés tous les documents administratifs, qui proposeront une clé d'activation non conforme à celle demandée et un délai d'exécution supérieur à celui exigé seront rejetées d'office.

- L'analyse des offres financières tiendra compte du montant de chacune des offres.

Le soumissionnaire ayant proposé le montant global le **moins élevé** par rapport aux autres sera classé le **premier**.

12. Attribution et notification du marché

Le marché sera attribué au soumissionnaire qui aura fourni une offre la plus avantageuse.

La notification de l'attribution du marché pourra être faite par courrier recommandé ou par tout autre moyen de transmission fiable.

13. Modalités de paiement

Le paiement interviendra après l'exécution entière et parfaite du contrat. Il se fera par virement ou chèque bancaire suivant les instructions données par le soumissionnaire gagnant.

14. Renseignements complémentaires

Tout renseignement complémentaire concernant le présent Avis d'Appel d'Offres peut être obtenu au Service Logistique et Patrimoine de la Banque de la République du Burundi à l'adresse mentionnée ci-dessus, au point 6 du présent Dossier d'Appel d'Offres.

15. Droit applicable

Le présent marché est régi par le Droit burundais, en particulier le Règlement de passation des marchés de la BRB, disponible sur le site www.brb.bi.

PARTIE II. DONNEES PARTICULIERES DE L'APPEL D'OFFRES

L'exécution du présent marché comprend au moins la liste des activités suivantes :

1) Fournir la clé d'activation / de renouvellement de la licence de l'antivirus **Kaspersky EndPoint Security for Business Advanced,** valide pour une période d'une année à compter du 22 octobre 2022 et effective pour **800 devices** (Desktops, Laptops, serveurs et mobiles) de la Banque;

2) Envoyer la clé d'activation de la licence au courriel suivant : platform@brb.bi;

3) Assister les Administrateurs de la Banque dans l'activation de la licence sur le serveur de l'antivirus de la Banque. Cette opération pourra être faite à distance ou sur site;

4) Garantir que les fonctionnalités recherchées sont disponibles ;

5) Paramétrer et tester les fonctionnalités du « System management » de l'antivirus Kaspersky de la Banque.