Prime Bank

P U T T I N G   Y O U   F I R S T

REQUEST FOR PROPOSAL

PROVISION AND IMPLEMENTATION OF DATA CLASSIFICATION AND DATA DISCOVERY TOOL

TENDER REF: RFP-2023-06/0001

Release Date: Friday 16th June, 2023

Last Date for Receipt of bids:
Friday June 30th, 2023, 5:00 PM (East African Time)

Contents

EXPRESSSION OF INTENT TO PARTICIPATE IN TENDER

This form is to be completed on receipt of the tender document from Prime Bank Limited (PBL).

This page is to be completed immediately and scan copy in PDF format e-mailed to RFP_DPO@primebank.co.ke The data contained in this form will be used to send out any addenda that may arise. Firms that do not register their interest by completing this form may not be sent addenda that may arise.

Name of the firm's representative completing this form:

Name of the firm's representative completing this form:			
Address:		Tel No:	Email Address:
Signature:		Date:	
Signed by (Name):		Position in Firm:	

1 INTRODUCTION

1.0 Purpose of the Tender

The Prime Bank Limited ("PBL") invites qualified firms to submit their proposals for the Provision and implementation of Data Classification & Data Discovery Tool.

This Request for Proposal (RFP) is being made available to interested service providers on a restricted tender basis. This document is intended to provide vendors with sufficient understanding of the PBL's requirements to enable them to respond.

For the purposes of the RFP it is necessary to disclose information in this document, and its schedules, which is considered confidential and should therefore not be used (otherwise other than in furtherance of this tender) or disclosed to any third party without explicit prior written consent of PBL.

PBL on its part also acknowledges that it is requesting through this RFP for information that is confidential and therefore commits in equal terms to reciprocal confidentiality.

1.1 Acknowledgement of Bidding Documents

PBL invites proposals for Provision and Implementation of Data Classification and Data Discovery Tool in accordance with the requirements set out in this document and the attached Business Requirement Document (BRD). Within five (5) working days of receipt of the RFP, the Bidder is required to acknowledge receipt of the RFP, and notify his intention to submit a bid by email to PBL at RFP_DPO@primebank.co.ke. The mail will include the signed registration template on Page 4 of this document.

Working days are defined as being any day of the week between Monday and Friday (0800 – 1700 Hrs.) excluding weekends and gazetted public holidays in the Republic of Kenya).

Failure to do so shall be perceived as an intention not to submit a bid and the Bidder will be eliminated from the bid process, and required to destroy the RFP document in keeping with confidentiality requirements.

1.2 Point of Contact

All enquiries or correspondence concerning the details of this tender should be addressed, in the first instance by e-mail to: RFP_DPO@primebank.co.ke The subject on the email should be "CLARIFICATION ON THE RFP FOR PROVISION OF DATA CLASSIFICATION AND DATA DISCOVERY TOOL"

- All responses from PBL to the Bidder shall be channeled through the Chief Information Security Officer/Data Protection Officer (CISO/DPO) using the e-mail address RFP_DPO@primebank.co.ke.
- It is the responsibility of the Bidder to obtain any further information required to complete this RFP.
- Any clarification request and their associated response will be circulated to all Bidders.
- All clarifications must be sought at the latest 3 days prior to the close of the RFP.

2 ABOUT PRIME BANK

2.0 Organization Profile

Prime Bank Ltd is one of the leading private banks in Kenya and was founded in 1992. Serving its customers for over 30 years, with a network of 23 branches, Prime Bank has the expertise to deliver flexible, efficient and personalized services.
Over the years, the Bank has developed its business interests in other African countries such as Malawi, Botswana, Mozambique, Zambia, and in Zimbabwe where it recently acquired Barclays Bank of Zimbabwe through its associate bank First Capital Bank. In 2017, the group acquired 80.72% shareholding of Tausi Assurance Limited. For more information, please visit primebank.co.ke

2.1 PBL Vision

To be the financial service provider of first choice.

2.2 PBL Mission

To provide quality and acceptable personalized financial services to our customers while observing compliance, growth and shareholder value.

3   OVERVIEW OF THE PROPOSAL

3.0   Overview

Prime Bank Limited is currently looking to Implement a Data protection, Classification & Discovery solution.

3.1   Objective of the Implementation of Data Classification & Data Discovery Solution.

PBL intends to configure and implement data classification and data discovery tool that will locate and classify sensitive data, find out how it is being used, and protect it against loss, theft or leakage.

PBL invites proposals from competent and authorized Bidders for Supply, Installation, Configuration, Commissioning and Maintenance of complete setup of Automated Data Classification and Data Discovery Tool for both structured and unstructured data at PBL's Primary Site and Disaster Recovery Site. The bidder may include information about their Data Encryption solution and how it integrates with the Data Discovery and Classification tool.

3.2   Scope of the Solution

The Data Classification and Data Discovery solution should meet the technical requirements below;

a)   Install & integrate all the necessary software components required for the Data Classification and Data Discovery Tool.

b)   The implementation scope initially will be for 600 users. Please provide cost for additional users in batches of 50 users

Number of users - Initial scope	Additional users Batch 1	Additional users Batch 2	Additional users Batch 3
600	50	100	150

c)   The Solution should be capable of classification of MS Office, pdf, text, e-Mails and other key applications files.

d)   The tool shall be capable to perform the data classification as per PBL data classification policy.

e)   The bidder may include information about the solution ability to provide Data encryption as an integral part of this solution or an addon solution to the data discovery and classification tool.

f)   The solution should trigger policy and classification actions based on different events, such as Open, Save, Print, Forward, Close, Send, or Classification Change. The solution should have the capability of integrating with a helpdesk ticketing system.

g)   The bidder is expected to openly declare the solutions deficiencies in meeting the clients specifications and expectations.

h)   The equipment / solution proposed by the bidder should not be declared as EOL or EOS by the OEM at least one (1) year from the date of completion of the installation.

i)   Successful bidder shall assign project manager and associated support personnel for this project.

j)   The Bidder should provide on the job tool training to PBL. This training will be during the implementation of the project for 10 employees of the bank at no extra cost.

k)   Execute User Acceptance Test (UAT) for the proposed solution i.e. Deployment of Client software on maximum up to 2 machines per department. Acceptance shall be based on the results of the test cases. If during the test period, the proposed Solution experiences no failures and functions according to the requirements of the RFP, as determined by PBL, the Solution shall be considered accepted.

l)   Bidder should demonstrate compliance to technical requirements documented in this document for the solution implemented.

m)   8 x 5 days support post implementation of the proposed solution.

3.2.1   Technical Requirements for Data Classification and Data Discovery Tool

No.	Technical Description	Compliance (Yes/No)	Remarks (if any)
	Data Classification		
1.	The solution should be able to classify unstructured data, namely Word/Excel/PowerPoint/TXT/Pdf Documents and MS Outlook emails.		
2.	The solution should be able to label the documents in Headers/Footers with a pre selection capability for either header or footer or both.		
3.	The solutions should be able to insert metadata tags in the documents and emails which can be read by DLP Solutions.		
4.	The solution should be able to uniquely tag each classified document.		
5.	The solution should be able to track initial classification and reclassification events at both document and central logging level.		
6.	The solution should be able to blacklist domains for blocking emails originating out of Microsoft Outlook and also bind certain classification categories with a fixed domain name.		
7.	The solution should trigger classification for document on Save, Save As, print etc. and should be configurable using a management mechanism		
8.	The solution should trigger classification based on Send, Reply, and Forward emails.		
9.	The solution should provide automated, suggestive and manual classification capability.		
10.	The solution shall have capability to classify multiple documents in one go.		

No.	Technical Description	Compliance (Yes/No)	Remarks (if any)
	Data Classification		
11.	The solution shall ensure the forceful enforcement of classification and should not allow user to bypass classification option in the said document's types using MS Office and MS Outlook.		
12.	The solution should have capability to detect differential classification between an email and its attachments and block the email from being sent.		
13.	The solutions should not restrict the number of classification levels required to be created.		
14.	The solution should have some guidance mechanism while user selects a classification level, to inform the users what is the context of a said classification level as per organization's policy.		
15.	The solution should have the classification plugins integrated within Word, Excel, PowerPoint and MS Outlook.		
16.	The solution shall have capability to send emails from mobile with classification applied for both IOS and Android based mobiles		
17.	The solution should be capable to deploy and enforcing user-based policies.		
18.	The solution should support the map organizations Classification Policy to the Classification Schema it creates		
19.	The solution should be able to identify information like Identification Numbers, Passport Numbers, credit card information for automated classification through either inbuilt capability or should have capability to define regular expressions		
20.	The solution should be able to detect keywords as defined by the organization and enforce classification		
21.	The solution should further allow policies which are based on a combination of keywords and regular expressions		
22.	The solution should allow administrators to define own regex for adding capability to detect any new type of regex.		
23.	The solution should suggest a classification based in content, but should allow user to change the classification if required by taking a justification for the same and recording it in logs.		
24.	The solution should enable administrators to control whether users can override policy warnings.		
25.	The solution should provide the ability to prompt users to enter a justification when overriding a policy warning.		
26.	The solution should provide the ability to warn/prevent users from downgrading the classification		
27.	The solution should provide the ability to save the name of the original classifier in metadata, and to enforce policy so that only the original classifier can change the classification		
28.	The solution should provide the ability to restrict users from sending non-classified email attachments (i.e. attachments that have no classification).		
29.	The solution should support the ability to warn or prevent users from sending password-protected Microsoft Office documents via email. (The metadata in password-protected Office documents is encrypted, so this capability provides an alternative way to enforce policy.)		
30.	The solution should provide built-in reports and dashboards to analyse user behaviour and system health.		
31.	The solution should provide a pre-built starter set of reports for the reporting database (in Excel) and Views and documentation to enable customers to write their own reports		
32.	The solution should provide a built-in dashboard for reviewing data classification scanning results for user activity, deployment.		
33.	The solution should provide role based access for administrators, compliance teams where anyone other than administrators may not have access to full console.		
34.	The solution should have capability to manage the complete solution from a central web console		
35.	The solution should have a capability to deploy, upgrade, uninstall the component without the use of any 3rd party software		
36.	The solution should be able to send classification policy to further changes to the clients without any need or intervention of a 3rd party software		

No.	Technical Description	Compliance (Yes/No)	Remarks (if any)
	Data Classification		
37.	The solution should have capability to deploy classification policies on the basis of users, machines, groups etc.		
38.	The unavailability of a management component/ server in no way shall impact the functioning of a client		
39.	The solution should cache configurations locally for offline use		
40.	The solution shall deploy the client in the background and shall have no interface with the end user on whose PC the solution is being deployed. Same shall be applicable for upgrades, updates and uninstallation.		
41.	The solution should work with email and SMS gateways, O365 and Microsoft Office 2016 and higher version. The product should support both 32- and 64-bit installation.		
42.	The solution should work on MS Windows environment.		
43.	The solution shall be bundled along with professional services to ensure Implementation, sustenance (support) on call basis, knowledge transfer for administrators.		
44.	The solution must have the capability to Discover, Classify and Protect the documents and emails without any user intervention		
45.	The Solution should have capability to integrate with SIEM and can send logs.		
46.	The Solution should be managed via a centralized management console		
47.	The solution should be capable for centralized deployment of the solution components on all network systems and it should be capable to get machine inventory from AD to perform deployment		
48.	Solution should be capable for configuring at DC and DR. Note: please DC and DR Capability should be scoped.		
49.	Solution should be capable to roll-out it's component with using 3rd party software including Active Directory GPO.		
50.	Solution should provide classification logs inside the classified file and at the centralized repository.		
51.	The solution must provide the capability where the Classification solution can add special tags to email messages and the messages are then automatically secured from unauthorized access, especially when shared externally		
52.	The Bidder must have local support centre within Kenya.		
53.	The solution should provide context-sensitive help throughout the user interface to support security training and help users select the correct classification and policy remediation options		
54.	The solution should support hierarchical and conditional classification fields, so that the appearance of a sub-field is conditional on the value selected in the higher-level field. For example, when a user selects "Restricted," a sub-field is presented with a list of departments including "Office use","Branch use", "HR Only" etc.		
55.	The solution should support icon overlays to identify the classification of files in File Explorer.		
56.	The solution should provide tooltips, classification descriptions, and help page links to assist users with classification policy.		
57.	The solution should support the creation of unlimited custom metadata for interoperability (Department, PII type, Document category, PII count etc.), including custom X-headers.		
58.	The solution should support customizable visual markings in email and documents (e.g. font (name/size/features), size, colour, and content).		
59.	The solution should support the ability to quarantine files stored inappropriately, flag files for follow-up, or act based on results of the scan. This may include quarantine, delete, encrypt through 3rd party encryption tools, etc.		
60.	The solution should integrate with DLP, encryption, Information Right Management (IRM) and Digital Rights Management (DRM) solution.		
61.	The solution should provide the ability to attach metadata to information objects, which can be leveraged by e-discovery solutions.		
62.	The solution should provide the ability to write tags which can be read by DLP solution		
63.	The solution must have ability to assign classification level to discovered data elements according to customer policy		

No.	Technical Description	Compliance (Yes/No)	Remarks (if any)
	Data Classification		
64.	The Management console should have role-based access and should integrate with Active directory for login access		
65.	The solution must have the capability to do analysis (discovering sensitive data) Based on Compliance requirement (PII, PHI, etc.)		
66.	The solution must have the capability to do analysis (discovering sensitive data) Based on file types (MS Office, Pdf's, TXT files, XML, HTML, JPEG, Compressed files, Zip files including encrypted files etc.)		
67.	The solution must have the capability to do analysis (discovering sensitive data) along with host details.		
68.	The solution must have the capability to do analysis (discovering sensitive data) based on Current Classification Level and to suggest classification.		
69.	The solution must have the capability to do analysis (discovering sensitive data) along with the User Permission on the sensitive data.		
70.	The solution must have the capability to Delete the sensitive data as a Remediation action if required.		
71.	The solution must have the capability to move the sensitive data as a Remediation action if required.		
72.	The solution must have the capability to replace the sensitive data as a Remediation action if required.		
	Data Discovery		
1.	The solution must have ability to connect to windows share drive and discover data sets		
2.	The solution must have ability to connect to local drive and discover data sets		
3.	The solution must have ability to identify and apply multiple business rules (e.g., KDPA, GDPR PII, PCI, PHI rules)		
4.	The solution must have ability to find unique identities by a data subject's key attributes across all data sources		
5.	The solution must have ability to see all identifiers on a data subject by conducting a search using either a name or other key attributes		
6.	The solution must have ability to develop an inventory of discovered identities		
7.	The solution must have ability to identify what objects within a system contain personal information about a data subject before retrieving the data		
8.	The solution must have ability to control the amount of personal information retrieved in response to a data subject access request to manage volume of data		
9.	Recognize data sources of systems, schemas, tables, data elements		
10.	The solution must have ability to scan structured, semi-structured and unstructured data		
11.	Search data sets by facets, keywords or business terms		
12.	The solution must have ability to assign classification level to discovered data elements according to customer policy		
13.	The solution must have ability to present data in masking format.		
14.	The solution must have ability to encrypt data elements of interest		
15.	The solution must provide audit trail		
16.	The solution must have the capability to Discover, Classify and Protect the documents without any user intervention		
17.	The solution must have the capability to do analysis (discovering sensitive data) Based on Compliance requirement (PII, PHI, etc.) and should also have an ability to defined customized policy to discover customer's IP(Intellectual Properties).		
18.	The solution must have the capability to do analysis (discovering sensitive data) Based on file types (MS Office, Pdf's, TXT files, XML, HTML, JPEG, Compressed file's etc.)		
19.	The solution must have the capability to do analysis (discovering sensitive data) along with host details.		
20.	The solution must have the capability to do analysis (discovering sensitive data) based on Current Classification Level and to suggest classification		
21.	The solution must have the capability to do analysis (discovering sensitive data) along with the User Permission on the sensitive data.		

No.	Technical Description	Compliance (Yes/No)	Remarks (if any)
	Data Discovery		
22.	The solution must have the capability to Move or Delete the sensitive data as a Remediation action if required.		
23.	The solution must have the capability to replace the sensitive data as a Remediation action if required.		
24.	The solution must have the capability to work on Linux, Unix, Windows OSes and Data bases such as Oracle, MS SSQL, MySQL etc.		

4 FORMAT OF RESPONSE TO TENDER

4.0 Information to be provided by bidders

All bids should contain ALL INFORMATION REQUESTED IN SECTIONS 4.1 TO 4.5. The information should be in the following order.

4.1 General Information about the firm

Provide the following documentation in respect of your company.

(i) Certificate of registration (or its equivalent) that is valid in accordance with any legally recognized jurisdiction

(ii) Tax compliance certificate (or its equivalent) that is valid in accordance with any legally recognized jurisdiction

(iii) CR12 (This is an official communication by the registrar of companies in Kenya as to whom the directors/shareholders of a company are) or its equivalent that is valid in accordance with any legally recognized jurisdiction in your area of operations

(iv) Current County Trade license/Business permit (If your operations are within Kenya)

(v) Company Profile, with a clear organogram and area of specialty

(vi) List of Directors (Name, ID Number/passport number, Nationality, Telephone and physical address

(vii) PBL Non-Disclosure Agreement (document to be provided to accompany this RFP)

(viii) PBL Supplier Code of Conduct (document to be provided to accompany this RFP)

(ix) PBL Business Litigation and Probity; and Lead Time and Credit Period Declaration Form (document to be provided to accompany this RFP)

4.2 Organization of the firm

- Depth of the firm's practice in serving global clients of the scale and scope of PBL.
- Briefly highlight the profiles and technical qualifications of key staff to be involved in the project where necessary – § experience in IFRSs, Accounting, Project Management, Risk, IT, etc. is highly recommended.
- Statement summarizing the benefit to PBL of engaging the firm.
- State the firm's compliance with International Standards for Assurance Engagements (ISAEs).
- Details of any implementation partner where necessary detailing all the above requirements under 4.1 and 4.2.

4.3 Reference Sites

Statement of capabilities and references in similar projects undertaken over the last three years including a brief description of the projects undertaken and reference letters. The firm needs to have conducted similar work with a Banking institution in Africa of the same or bigger, size and operation with PBL.

By responding to this Tender the service provider confirms that they have no objection to PBL obtaining independent references from their current customers in furtherance of this Tender.

4.4 Particulars of the Project Deliverables

This section shall provide details including but not limited to how your solution is able to achieve the scope detailed in section 3.2 and your project methodology and major project milestones and deliverables per phase of the project as outlined in paragraph 3.3. It should also include the timelines the implementation could take assuming all data and resources are made available.

4.5 Bid Preparation and Submission

Bid documents should be put in plain sealed envelopes labelled as below and dropped in the tender box located on 4th floor PBL HEAD OFFICE, RIVERSIDE DRIVE, Nairobi.

RFP FOR PROVISION AND IMPLEMENTATION OF DATA CLASSIFICATION AND DATA DISCOVERY TOOL – PBL
Prime Bank Limited

Tenders may also be posted 7 days earlier than the deadline to:

The Head of Procurement PBL Head Office
River side Drive/Ring Road Westlands Road Junction,
P. O. BOX 43825-00100 NAIROBI

And marked at the top "DO NOT OPEN BEFORE March 31st 2023, 3:00 PM (GMT +3)"

Offers must be submitted in two separate documents, a technical and commercial bid and must be submitted in separate files envelopes, clearly labelled as:
- The file with the technical proposal should be identified as follow

NAME OF THE COMPANY, TECHNICAL PROPOSAL

- The file with commercial proposal should be identified as follows:

NAME OF THE COMPANY, COMMERCIAL / FINANCIAL PROPOSAL

A soft copy of the bid should also be submitted in a Flash Disk together with the bid documents through the tender box. No soft copy submission of the bid shall be made through any electronic means prior to the bid opening. Any such electronic submission shall lead to disqualification of the bid.

5 GENERAL CONDITIONS OF CONTRACT

5.1. Introduction
Specific terms of contract shall be discussed with the bidder whose proposal will be accepted by the Company. The resulting contract shall include but not be limited to the general terms of contract as stated below from 5.2 to 5.14.

5.2. Award of Contract
Following the opening and evaluation of proposals, the Company will award the Contract to the successful bidder whose bid has been determined to be substantially responsive and has been determined as the best evaluated bid. PBL will communicate to the selected bidder its intention to finalize the draft conditions engagement in consultation with the bidder
Participating unsuccessful bidders will be notified in writing either through a letter or an email.

5.3. Tender Cancellation
The company reserves the right to cancel a tender if management decides it is in its best interest to withdraw. The bidders will be notified of such a decision in writing either through a letter or an email.

5.4. Application of General Conditions of Contract
These General Conditions (sections 5.2 to 5.14) shall apply to the extent that they are not superseded by provisions in other parts of the Contract that shall be signed.

5.5. Bid Validity Period
Bidders are requested to hold their proposals valid for ninety (90) days from the closing date for the submission.

5.6. Non-variation of Costs
The prices quoted for the service and subsequently agreed and into the contract shall be held fixed for the contract period.

5.7. Delays in the Bidder's Performance
5.7.1. Delivery and performance of the Transaction shall be made by the successful Bidder in accordance with the time schedule as per Agreement.
5.7.2. If at any time during the performance of the Contract, the Bidder should encounter conditions impeding timely delivery and performance of the Services, the Bidder shall promptly notify the Company in writing of the fact of the delay, its likely duration and its cause(s). As soon as practicable after receipt of the Bidder's notice, the Company shall evaluate the situation and may at its discretion extend the Bidder's time for performance, with or without liquidated damages, in which case the extension shall be ratified by the parties by amendment of the Contract.
5.7.3. Except in the case of "force majeure" as provided in Clause 5.14, a delay by the Bidder in the performance of its delivery obligations shall render the Bidder liable to the imposition of liquidated damages pursuant to Clause 5.8.

5.8. Liquidated damages for delay
The contract resulting out of this RFP shall incorporate suitable provisions for the payment of liquidated damages by the bidders in case of delays in performance of contract.

5.9. Governing Language
The Contract shall be written in the English Language. All correspondence and other documents pertaining to the Contract which are exchanged by the parties shall also be in English language.

5.10. Applicable Law
This agreement arising out of this RFP shall be governed by and construed in accordance with the laws of Kenya and the parties submit to the exclusive jurisdiction of the Kenyan Courts.

5.11. Successful Bidder's Obligations
The successful bidder:
5.11.1. Is obliged to work closely with PBL staff, act within its own authority, and abide by directives issued by the Company that are consistent with the terms of the Contract
5.11.2. Will abide by the job safety measures and will indemnify the Company from all demands or responsibilities arising from accidents or loss of life, the cause of which is the Bidder's negligence. The Bidder will pay all indemnities arising from such incidents and will not hold the Company responsible or obligated.

5.11.3. Will be responsible for managing the activities of its personnel, or subcontracted personnel, and will hold itself responsible for any misdemeanours.

5.11.4. Will not disclose the Company`s information it has access to, during the course of the work, to any other third parties without the prior written authorization of the Company. This clause shall survive the expiry or earlier termination of the contract

5.12. PAYMENT TERMS
PBL will not make any payments in advance. PBL will issue an LPO for all services required and the LPO will be paid 30 days from receipt of invoices in arrears.

6 PBL SUPPLIER CODE OF CONDUCT

6.1 GENERAL
This Code is applicable to all PBL suppliers (hereinafter "Supplier" or "Suppliers") and their employees (be they temporary, casual or permanent) and sub-contractors throughout the world. PBL requires all Suppliers to conduct their business dealings with PBL in compliance with this Code and in compliance with all laws applicable to the Supplier's' business, wherever conducted. By entering into business transactions with PBL, the Supplier agrees to abide by the terms of this Code and acknowledge that compliance with this Code is required to maintain the Supplier's status as a PBL Supplier. PBL shall have the right to terminate any Supplier's contract for failure to comply with the provisions of this Code. PBL recognizes that local laws may in some instances be less restrictive than the provisions of this Code. In such instances Suppliers are expected to comply with the Code. If local laws are more restrictive than the Code, then Suppliers are expected to comply with applicable local laws.

6.2 PROVISIONS
In particular, Suppliers must comply with the following:
6.2.1 Relations with competitors
Suppliers will be required to comply with applicable antitrust or competition laws and will not engage in any restrictive trade practices. Suppliers will at all time act in a manner that will uphold and encourage healthy competition. The applicable anti-trust legislation with regard to Kenya operations is the Restrictive Trade Practices, Monopolies and Price Control Act (Cap 504 Laws of Kenya).
6.2.2 Bribes, Conflicts of Interest, Gifts and other Courtesies

6.2.2.1 Bribes
Suppliers shall not make or offer bribes or payments of money or anything of value to any PBL employee or any other person including officials, employees, or representatives of any government or public or international organization, or to any other third party for the purpose of obtaining or retaining business with PBL. For the avoidance of doubt PBL considers an act of bribery to include the giving of money or anything of value to anyone where there is belief that it will be passed on to a government official or PBL employee for this purpose. Suppliers are required to comply with all applicable local anti-bribery laws.

6.2.2.2 Gifts and other business courtesies

Suppliers shall ensure that any expenditure incurred in relation to any particular PBL employee or government official is in the ordinary and proper course of business and cannot reasonably be construed as a bribe or so as to secure unfair preferential treatment. A general guideline for evaluating whether a business courtesy is appropriate is whether public disclosure would be embarrassing to the Supplier or PBL.
PBL employees may accept unsolicited gifts from Suppliers provided:
• they are items of nominal value – KShs 1500 or less, or
• they are advertising or promotional materials having wide distribution e.g. calendars, stationaries, diaries, etc; and
• acceptance of the gift does not violate any applicable law and PBL policies.

6.2.2.3 Conflicts of Interest
No supplier shall enter into a financial or any other relationship with a PBL employee that creates a conflict of interest for PBL. A conflict of interest arises when the material personal interests of the PBL employee are inconsistent with the responsibilities of his/her position with the company. All such conflicts must be disclosed and approval to the transaction given.

6.2.3 Compliance and implementation
6.2.3.1 Licenses and Returns
The Supplier will be required to obtain and renew, in accordance with any law or regulations all permits, licenses and authorizations required for it to carry out its business. In addition, the Supplier will be required to prepare and file any returns that it may be required to file under its incorporation statute, the Companies Act (Cap 486 Laws of Kenya) or applicable local or Kenyan revenue legislation.

6.2.3.2 Taxation, Financial Integrity and Retention of Records
• The Supplier will comply with all revenue laws and will not evade tax.
• Suppliers will be required to maintain accurate and reliable financial and business records and shall not have any false or inaccurate accounting books or records related to PBL for any reason. Suppliers shall maintain all business records at the minimum in compliance with the provisions outlined by the Kenya Revenue Authority or local revenue authorities from time to time.
• When any government investigation or audit is pending or ongoing then Suppliers will not destroy any relevant records until the matter has been investigated and closed.

6.2.4 Violations
If a Supplier becomes aware of any known or suspected improper behaviour by another Supplier in relation to their dealings with PBL or if a bribe or other inducement is requested from a Supplier by any PBL employee or any other person with the promise of influencing PBL's position as far as that Supplier is concerned or if the Supplier feels that a conflict of interests exists with one of PBL's employees then all pertinent details should be reported in confidence to the following Contact Address RFP_DPO@primebank.co.ke

6.2.5 Variations
PBL reserves the right to vary this Code at any time.

6.2.6 Performance guarantee
• Within twenty-one (21) days after the Bidder's receipt of Notification of Contract Award, the Bidder shall furnish Performance Guarantee to the Bank for an amount equivalent to the Total Cost of Ownership (TCO) valid up to not earlier than 1 year from the date of notification of award of contract, for punctual performance and fulfillment of the contract. TCO is the total cost of the project for one years as quoted by the Bidder.
• Performance Guarantee shall be denominated in KENYAN SHILLINGS (KES) only and shall be a Bank Guarantee
issued by a Scheduled Commercial Bank located in Kenya in the format provided in the RFP (Annexure 13-Performance Guarantee).
• The Bank shall notify the Bidder in writing of its invocation of its right to receive such compensation within validity period, indicating the contractual obligation(s) for which the Bidder is in default. Performance Guarantee may be invoked if the Bidder fails to comply with performance obligations during Warranty and AMC/ATS period.
• The proceeds of the Performance Guarantee shall be payable to the Bank as compensation for any loss resulting from the Bidder's failure to complete its obligations under the Contract.