REQUEST FOR PROPOSAL

PROVISION OF DATA PROTECTION PROGRAM & DLP SYSTEM IMPLEMENTATION SERVICES

TENDER REF: RFP-2022-11/0001

Release Date: Thursday 17th November, 2022

Last Date for Receipt of bids: Wednesday 7th December, 2022, 5.00 PM (East African Time)

Table of Contents

EXPRESSSION OF INTENT TO PARTICIPATE IN TENDER

This form is to be completed on receipt of the tender document from Holdings Plc (Britam).

This page is to be completed immediately and scan copy in PDF format e-mailed to procurement@britam.com. 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:

_____

Firm's Name:

_____

Address:

_____

Tel No:

_____

Email Address:

_____

Signature:

_____Date:_____

Signed by (Name):

_____

Position in Firm:

_____

1 INTRODUCTION

1.0 Purpose of the Tender

The Britam Holdings Plc ("Britam") invites qualified firms to submit their proposals for the Provision of Data Protection Program & DLP System Implementation Services.

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 Britam'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 Britam.

Britam 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

Britam invites proposals for Provision of Data Protection Program & DLP System Implementation Services 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 Britam at procurement@britam.com. 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: procurement@britam.com. The subject on the email should be "CLARIFICATION ON THE RFP FOR PROVISION OF DATA PROTECTION PROGRAM & DLP SYSTEM IMPLEMENTATION SERVICES"

- All responses from Britam to the Bidder shall be channelled through the Head of Procurement.
- 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 BRITAM

2.0 Organization Profile

Britam is a leading diversified financial services group, listed on the Nairobi Securities Exchange. The group has interests across the Eastern and Southern Africa region, with operations in Kenya, Uganda, Tanzania, Rwanda, South Sudan, Mozambique and Malawi. The group offers a wide range of financial products and services in Insurance, Asset management, Banking and Property. For more information, please visit http://www.britam.com/

2.1 Britam Vision

To be LEADING diversified financial services company in our chosen markets across Africa.

2.2 Britam Mission

Providing you with financial security EVERY STEP OF THE WAY.

3 OVERVIW OF THE PROPOSAL

3.0 Overview

Britam Holdings Plc and Its insurance business subsidiaries is currently looking to Implement Data protection, classification & loss prevention solutions.

3.1 Objective of the Implementation of Data Classification & Data Loss Prevention Solutions.

Understand the Current State of the existing Britam Governance Framework in the context of the prevailing internal, external and regulatory requirements to identify the risk and business drivers for data protection for the Britam entities and Implementation of Data Classification & Data Loss Prevention Solutions.

3.1.1 Deliverables

1. Document & Report on Data Flow and Data Discovery. Identify all the critical data types in scope through automated and manual discovery and document data flow diagrams for the identified critical data types.
2. Data Privacy Gap Analysis.
3. Document the necessary data protection policies and procedures (Business Use Cases) to ensure Britam has a formal framework to meet its data protection requirements.
4. Data classification and labelling.
5. Data handling guidelines.
6. Roles and responsibilities for data protection.
7. Training and awareness to departments on data protection and handling guidelines.
8. Data Classification schema and Implementation of Data Classification Tool.
9. Implement the Forcepoint DLP Tool.
10. Configuration of Compliance Reports.
11. Project manuals specific to the Britam implementation for Forcepoint DLP and Data Classification Solutions. (Enabling Processes: Develop processes that are required to support the use of the tool/ technology: Admin Guide, Policy creation, Policy Fine Tuning, Incident management, classification, incident response/ reporting).
12. Define Key performance indicators (KPI), which are aligned with overall data protection strategy, such as number of data leakage incidents, network

coverage, Rules configured, reduction of false positives, Incidents closed within SLAs etc.

13. The proposed DLP solution should block, quarantine or relocate the channel containing sensitive data.

3.2 Scope of the Solution

The data protection program & data loss protection solution should meet the technical requirements below;

3.2.1 Technical Requirements for Data Loss Prevention Solution

3.2.1.1 Email DLP

- The solution should be able to block outbound emails sent via SMTP if it violates the policy without agent.
- The solution should support Email DLP deployment on Microsoft Azure/On-prem for Office 365/ google workplace.

3.2.1.2 Endpoint Data Monitoring & Protection

- The solution should have pre-defined applications and multiple application groups and allow each application/application group to monitor operations like Cut/Copy, Paste, File Access and Screen Capture or Download.
- The endpoint solution should have capabilities to monitor applications and ensure unauthorized applications do not have access to sensitive files.
- The solution should be able to monitor data copied to network file shares and should enforce structured and unstructured fingerprint policies even when disconnected from corporate network.
- The solution should be able to monitor sensitive content accessed by cloud storage applications on the endpoint and prevent sensitive data from uploading to the cloud storage applications e.g. OneDrive, Dropbox, google drive etc.
- The Endpoint DLP Solution must be able to encrypt data when business classified data is sent to removable media drives.
- The solution should support the multiple Endpoint Profile Creation for the Better Security between the different departments.

3.2.1.3 Automated Response & Incident Management

- The solution should be able to alert and notify sender, sender's manager and the policy owner whenever there is a policy violation, Different notification templates for different audience should be possible.
- The incident should include a clear indication of how the transmission or file violated policy (not just which policy was violated), including clear identification of which content triggered the match.
- The solution should provide automatic notification to incident managers when a new incident is assigned to them.

3.2.1.4 Role Based Access and Privacy Control

- The system should create separate roles for technical administration of servers, user administration, policy creation and editing, incident remediation, and incident viewing for data at rest, in motion, or at the endpoint.
- The system should allow incident managers and administrators to use their Active directory credentials to login into the console.
- The system should allow incident managers and administrators to use their Active directory credentials to login into the console.

3.2.1.5 Reporting and Analytics

- The solution should have a dashboard view designed to provide information about data in motion (network), data at rest (storage), data at the endpoint (endpoint), incidents etc.
- The solution should have the option of sending email reports and allow automatic schedule of reports to identified recipients.
- The reports should be exported to at least CSV, PDF, HTML formats.
- The system should have lots of pre-defined reports which administrators can leverage.
- The solution should provide statistical analysis by use of machine learning or other statistical methods such as Bayesian analysis to trigger policy violations in secure content

3.2.1.6 Integrations

- The solution should provide flexibility to send user logs to SIEM, syslog server, text file, and Windows event logs as per the need.
- The system should have the ability to integrate to Active directory to enable administrators to use their Active directory credentials to login into the console.

3.2.1.7 Auditing and reporting

- The solution should provide a built-in dashboard for reviewing data discovery scanning results for user activity, deployment, data storage trends, and data inventory. The solution should log user activity while users are handling email, documents, and files. The solution should provide built-in reports and dashboards to analyze user behavior and system health.
- The solution should integrate with third-party reporting tools to provide meaningful reports on user activity and deployment.
- The solution should provide a pre-built starter set of reports for the reporting database (in tab separated values/ Excel or Database format) and Views and documentation to enable customers to write their own reports.

3.2.1.8 Information protection

- The solution should support functionality to check recipients marked in an email and alert/prevent the user from sending the mail if external recipients are marked. Example: An email containing internally classified document as attachment should be prevented from being sent if external recipients are marked in that mail. The user should also get an alert for the same.
- Provides fine-grained control over the policy actions that apply to different use cases, such as when to classify automatically, via machine learning, and/or when to prompt the user.
- The solution should support creation of policy which can embed specific actionable information (e.g.: Sensitivity, data retention/legal holds, regulation applicability, information type, diagnostic codes, etc.).
- The solution should be able to identify information like National ID numbers, Passport numbers, credit card information for automated classification thru either inbuilt capability or should have capability to define regular expressions.

- The solution should have capability to detect differential classification between an email and its attachments and block the email from being sent.
- The solution should support different classification values for different applications. This can be combined with user targeting to present detailed classification options based on application and user identity. For example, users in the accounting department may be able to capture additional accounting and retention metadata for Excel files, but use a simplified classification schema for email.
- The solution should support the ability to natively allow password to protect/encrypt sensitive files by throwing a pop-up whenever user is trying to share confidential file to authorized recipients.
- The solution should provide the ability to warn/prevent users from downgrading or changing a classification.
- The solution should provide the ability to allow only specific users and AD groups to downgrade, upgrade and change classification.
- The solution should provide the ability to warn users when opening sensitive Office documents natively.
- The solution should provide the ability to prevent printing of sensitive email and Office documents based on classification to specific printers natively.
- The solution should provide the ability to highlight sensitive information within an email and redact the sensitive content so that users can remediate any policy violations before the email leaves the desktop.
- The solution should provide advanced control over email via policies that evaluate content, recipients, sender, classification, filename, file size, and other attributes.
- The solution should support the ability to restrict email based on sender. For example, one user may be authorized to send sensitive information externally, but others are not allowed to do this. The policy decision may be based on the sender's email, name, or AD attributes or group membership.
- The solution should support policy combinations to enable more advanced use cases, such as checking whether a document is having regulatory data, and then blocking an unauthorized user from sending the document as an attachment in mail.
- The solution should support multiple classification types (i.e. dropdowns, multi-selects, date fields, and user type-in).

- The solution should provide the ability to evaluate the number of instances of sensitive data within a document, and then apply the appropriate policy. For example, users may be allowed to save a document with one credit card number as General Business, but if there is more than one unique credit card number, the document should be saved automatically as restricted classification.
- The solution should provide the native ability to restrict users from sending non-classified email attachments (i.e. attachments that have no classification).
- The solution should be able to label the documents in Headers/Footers with a preselection capability for either header or footer or both.
- The solution should be able to track initial classification and reclassification events at both document and central logging level.

3.2.2 Technical Specification of Data Classification

- The solution should evaluate content, context, identity, and other attributes of unstructured data to make classification, categorization, and policy decisions.
- The solution should support automated, suggested, and user-driven classification.
- The solution should label documents and emails when they are first created. Existing documents in data stores must be scanned for Sensitive Data and classified and labelled as per agreed upon Data Classification Policy. These data stores are both on premises and in the cloud.
- The solution should label documents with visual markings such as watermarks, header, or footers. The files will need to be electronically marked.
- The solution must have monitoring and detection capabilities. Once a document has been classified and marked the solution must have the flexibility to set up actions to be taken including blocking transmission of the document, and provide a warning to the sender, send notification to the creator or owner of the document, or send notification to the administrator.
- The solution should be able to monitor for policy warnings and violations and have the flexibility to report via text, email, or console view.
- The solution must have the capability to provide on-demand, daily, weekly and trending reports showing all policy violations and warnings including trending over a prescribed period. The reports should show an analysis of documents that have been automatically classified as well as a historical view of all documents.

- The solution should have auditing capabilities to ensure that documents are continuing to be classified in an accurate and consistent basis.
- The solution should support policy conditionality based on data attributes like content, classification, recipients, sender, author, filename, path, IP address, MAC address, modification date, file type, and location.
- The solution should interact and educate users about proper data handling at the exact time they are creating, handling, sharing or saving files.
- The solution should support policy conditionality based on data attributes like content, classification, recipients, sender, author, filename, path, IP address, MAC address, modification date, file type, and location.
- The solution should enable the classification of Word, Excel, PowerPoint - documents, Outlook - messages, calendar items from within from within Word, Excel, PowerPoint, and Microsoft Outlook and should labels over the files that have been classified using the solution.
- The solution should provide the ability to prompt users to enter a justification when overriding a policy warning.
- The solution should suggest a classification based on content but should allow user to change the classification if required by taking a justification for the same and recording it in logs.
- The solution should support users to enforce data retention and disposition tags, including date fields while classifying information especially sensitive information which can result in increased liability if stored longer.
- The solution should support dynamic/tailored classification selections based on the user's Active Directory attributes or groups. For example - HR AD group alone should have an additional label (personal data).
- 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.
- The solution should support the use of automated classification for any classification field. These classification values can be assigned based on content, context, and/or user identity (e.g. user role).
- The solution should support the ability to ask users to confirm an automated classification value (also called "suggested classification").

- The solution should support the ability to scan for certain keywords and regular expressions and set the classification accordingly.
- The solution should generate metadata for all file types, including persistent, embedded metadata for many non-Office files, including PDF, TXT, Visio, Project, images, and multimedia files.
- The solution should support ability to add customizable visual markings in email and documents (e.g. font, size, color, and content).
- The solution should support real time automatic classification of files when its downloaded and saved to specific folders (e.g. Downloads, My Documents, Desktop) and the classification should be based on file content, file type, file size, file name, file path and combination of any of these parameters.
- The solution should support Machine Learning Categorization to help predict different categories of documents, providing classification suggestion or automation on unknown content in documents and email.
- The solution should have the ability to enforce obtaining consent from end users while handling sensitive information and capture the same in the meta data. For example - If consent has to be taken for given MS office document containing PCI then tool should prompt the user to capture consent.
- The solution should provide the ability to allow user to manually classify file attachment(s) directly within MS Outlook when composing an email without the need to open the attachment and without classifying the original source file.
- The solution should allow users to click a button to run a policy check before sending an email or continuing to compose or save a document. This enables the user to run a content scan without having to do a scan on every Save.

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 recognised jurisdiction
(ii) Tax compliance certificate (or its equivalent) that is valid in accordance with any legally recognised 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 recognised 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 speciality
(vi) List of Directors (Name, ID Number/passport number, Nationality, Telephone and physical address
(vii) Britam Non-Disclosure Agreement (document to be provided to accompany this RFP)
(viii) Britam Supplier Code of Conduct (document to be provided to accompany this RFP)
(ix) Britam 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 Britam.
- Briefly highlight the profiles and technical qualifications of key staff to be involved in the project where necessary – experience in IFRSs, accounting, actuarial, risk, IT, etc. is highly recommended.
- Statement summarizing the benefit to Britam 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 an insurance company in Africa of the same or bigger, size and operation with Britam.

By responding to this Tender the service provider confirms that they have no objection to Britam 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 5th floor Britam Centre, Upper Hill, Nairobi.

RFP FOR PROVISION OF DATA PROTECTION PROGRAM & DLP SYSTEM IMPLEMENTATION SERVICES – BRITAM HOLDINGS Plc

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

The Head of Procurement
Britam Head Office
Mara / Ragati Road Junction, Upper Hill
P. O. BOX 30375 – 00100 NAIROBI

And marked at the top **"DO NOT OPEN BEFORE DECEMBER 6TH 2022, 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. Britam 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 Britam 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

Britam will not make any payments in advance. Britam will issue an LPO for all services required and the LPO will be paid 30 days from receipt of invoices in arrears.
Britam will not accept partial deliveries and neither will it make partial payments.

6 BRITAM SUPPLIER CODE OF CONDUCT

6.1 GENERAL

This Code is applicable to all Britam suppliers (hereinafter "Supplier" or "Suppliers") and their employees (be they temporary, casual or permanent) and sub-contractors throughout the world. Britam requires all Suppliers to conduct their business dealings with Britam 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 Britam, 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 Britam Supplier. Britam shall have the right to terminate any Supplier's contract for failure to comply with the provisions of this Code. Britam 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 Britam employee or any other person including officials, employees, or representatives of any government or public or international organisation, or to any other third party for the purpose of obtaining or retaining business with Britam. For the avoidance of doubt Britam 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 Britam 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 Britam 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 Britam.

Britam 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.

6.2.2.3 Conflicts of Interest

No supplier shall enter into a financial or any other relationship with a Britam employee that creates a conflict of interest for Britam. A conflict of interest arises when the material personal interests of the Britam 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 Britam 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 Britam or if a bribe or other inducement is requested from a Supplier by any Britam employee or any other person with the promise of influencing Britam's position as far as that Supplier is concerned or if the Supplier feels that a conflict of interests exists with one of Britam's employees then all pertinent details should be reported in confidence to the following Contact Address

Procurement procurement@britam.com

6.2.5 Variations

Britam reserves the right to vary this Code at any time.