Request for Proposal on:

Mobile Backup Solution

ethio telecom™
ስትዮ ቴሌኮም™

Table of Contents

1. Background information

Ethio telecom with a strategic aspiration of being a preferred operator has been working at its full-scale towards the provisioning of competitive value adding telecom solutions and satisfying customers' expectations. To realize its vision, our company designed BRIDGE strategy and has been working hard to build best customer experience, reputable brand, deliver innovative product and services, achieve operational and technology excellence, and ultimately ensure financial growth.

Currently Ethio telecom mobile subscriber base has reached 56.45M customers (33% smartphone users and 92% of them are Android OS). It is offering a wide range of services including voice, internet, messaging along with different value-added service solely and in partnership with various service providers. Moreover, to support the digital transformation happening around the world and in our country, to address customers' needs for fast and reliable internet, Ethio telecom has recently expanded 4G LTE advanced network around the country in major cities as well as 114 towns of the country.

In line with its continuous effort to build the best service for mobile customers, Ethio telecom is planning to launch mobile backup solutions in partnership with solution providers as part of creating opportunity to our customers to protect themselves against the consequences of losing a wealth of personal and business-critical data and increase customer experience with secured and one-click step to recover all data stored on a mobile phone.

Hence, Ethio telecom wants to invite potential Mobile backup solution providers responsible for to submit their technical and commercial proposal. The main objective of the RFP is to call upon prospective who are interested to work with Ethio telecom on revenue sharing basis based on contractual agreement set.

2.   Project Objective

The main objective of the RFP is to select competent Mobile backup solution that are capable to:

- Introduce customer personal cloud storage service for ethio telecom mobile customers
- Enhance customer satisfaction with options of having a backup data from Mobile backup cloud storage

- Create opportunity to protect customers against the consequences of losing a wealth of personal and business-critical data.

- Increase customer experience with secured and one-click away from being recovered when needed.

- Create loyalty and retention of esteemed customers ahead of the coming market competition.

3.   Scope of Work

The scope of this Request for Proposal (RFP) includes:

- Providing end to end Mobile backup cloud storage solution.
- Deliver reliable end to end solution with deep technical expertise and support.
- Avail a single point for service provisioning, create easy and secure accessibility for mobile customers and provide data restore service those are subscriber contact phone number and contact name from subscriber SIMCARD and from Mobile handset contacts phone number and Name, SMS, photo, video, Music files, ringtones and any saved on mobile handset.
- Restoring service can be compatible for all types of Mobile handset that as per the consent of end users.
- Install required system solutions for the Mobile backup solution implementation and integrate the solutions with Ethio telecom infrastructure.

- Submit a product information and strategy on the potential Mobile backup areas mentioned below. The list is not intended to be exhaustive, and partners are encouraged to share additional areas that can be monetized:

    a. Mobile backup Cloud storage service
    b. SMS based back up
    c. USSD based back up
    d. Web-based based back up
    e. Application-based based back up

- Partners can submit their Mobile backup plan that can address some or all the areas above. The areas will not be restricted to the above ones and additional areas can be included depending on market potential and segment maturity.
- Partners are expected to deliver the solution, operate, and provide in life management support in collaboration with Ethio telecom.

All proposals satisfying the requirements of this Request for Proposals will be evaluated to select competitive Mobile backup the fulfil Ethio telecom requirement. This Request for Proposals, however, does not commit Ethio telecom to award a contract, to pay any costs incurred in the preparation of a proposal. Ethio telecom reserves the right to accept or reject any or all proposals received because of this request, to negotiate with all qualified partners or to cancel this Request for Proposals, if it is in the best interests of Ethio telecom to do so.

4. Project Requirements

- **Preliminary requirements**

Interested mobile backup solution service shall fulfil and provide the following engagement requirements when submitting their response proposal:

- Renewed or new trade license and commercial registration.

- Renewed or new VAS (Value Added Service) license or commitment to engage international or local business entity/ partners.

- Agreement to work with a minimum of three-year contract.

- Commit to engage international and local business entity/ partners /content providers/ for service delivery.

- Partner shall provide at least three recent client/customer references endorsing the successful implementation of the Mobile backup solution.

- Partner shall be required to allow Ethio telecom to have a site visit with the reference customer, if necessary.

4.1 Required Company Experience

The mobile backup solution shall have:

- Proven knowledge in the Mobile backup solution deployment and implementation experience with Mobile operators.

- Ability to integrate mobile cloud storage provider's system with telecom infrastructure.

- Proven ability to build, deploy and support differentiated system provider solutions that are aligned with customer needs and local market demands.

- Professional staff with required Mobile backup domain knowledge, ability to plan, manage and execute Mobile backup solution implementation.

- Familiarity with standardization, best practices and regulations, security, and privacy around Mobile cloud storage/Mobile backup solution.

- Capability to develop an actionable roadmap that will give clear guidelines on to how implement, support, and utilize mobile cloud storage in Ethiopia by taking existing assets into consideration and market gap

4.2 Integration Requirements

Potential Mobile Backup solution provider shall comply as per the following general requirements:

General Requirement	Compliance Fully Comply/Partially Comply/ Not Comply	Remarks
Shall integrate with operator core network and business solution like BSS, AAA, GSM, LTE, IMS/SBC, NGN, PSTN and CDMA, 5G, ACS, but not limited to.		
Shall able to integrate with operator security and VAS solution like FMS, PCRF, SMS, USSD.		
Shall provide the following interface but not limited to web service, predefined protocol, JDBC, ODBC, FTP/SFTP, SSL, SOAP, REST and other And, in case the operator wishes to develop its own self-care module the solution shall provide APIs to allow this development.		
Shall integrate through DMZ of ethio telecom.		
Shall integrate operator payment Gateway.		
Shall provide data migration capability from CSP solution to on premise platform or vice versa or among CSP.		
Shall follow well defined technical migration approaches that clearly shows Pre-migration, migration and post-migration steps with data cleansing and validation at each stage if applicable.		
Shall be adaptive and customizable to future integrations and design improvements.		
Shall ensure maximum system performance and quality while implementing/enabling security mechanism at the expected level without compromising system performance. Shall adopt enterprise integration platform and interface contract design via the integration framework.		

Shall be adaptive to future experience and site design improvements protocol for integration, file exchange and others.		

4.3 Security Requirements and Guidelines

1. The solution shall ensure Confidentiality, Integrity and Availability for the information that passes through and stored. The solution provider should describe the detail.
2. The solution shall comply with the regulatory, security and legal requirements of the company and the country, it shall consider the privacy of ethio telecom customers.
3. The solution should provide mechanisms to allow its components recover from a failure or discontinuity without risk of compromising security.
4. All systems and application should consider that security application agents like, antivirus, DLP, application control, and others could be installed on them.
5. The vendor should commit to fix any security vulnerability identified in the system whether it is owned by it or third party without any precondition. If exploitation of known vulnerability happened and cause damage to Ethio telecom business, the vendor will compensate the damage.

Identity and Access Management Requirements

1. The solution shall support single sign-on, multi-factor authentication, federate identity across applications and client-side certificate authentication across the solution platform.
2. The solution shall support role-based access control (RBAC) and users and groups grant authority based on their role on the proposed service.
3. Unauthorized administrator should not be able to retrieve any password in clear text and should not be able to decrypt the encrypted/hashed password. The password encryption/hashing mechanism detail should be described.

4. The solution should provide audit capabilities with user accountability for all significant events. It should not be possible to disable the audit log of actions taken by any administrator.

Data and database Security Requirements

1. The solution should provide confidentiality, integrity and availability to data in transit, data in use, Data in the process of storage. The solution provider should describe how their solution could achieve these data privacy and security in detail.
2. The solution should be able to store sensitive data with secure and strong cryptographic algorithm. How the solution could achieve this requirement shall be described.
3. Latest version of database and database management software shall be implemented; all patches shall be implemented immediately, and system performance shall not be impacted.
4. The solution shall incorporate data security features including but not limited secured data access permission, data storage, data transmission, and data reporting.
5. The solution should confirm and prove customers as well as organizations digital privacy.

Host and end point Security Requirements

1. The solution should work in alignment with existing endpoint security without compromising performance whenever applicable.
2. The solution should support Operating system, applications, and Database Security hardening. The detail mechanism should be explained.
3. The proposed solution's operating system installed on each device should be well-known, latest version, matured (not a beta version) and must also be easy for patch update.
▪ Log Management, Reporting and Monitoring requirements

1. The solution shall generate all kind of logs like user activity log, operational logs, run logs, audit logs, security logs, interface log, and but not limited to these.

2. The proposed system should detect the absence of log generation, modification, and deletion of the log that has security implications.
3. Audit logs should be available for online review and fetching as per the company's log retention policy.

System Management Security requirements

1. Hardware console or management interface should be protected with a password and the default password must be changed and encrypted at deployment time.
2. Management interface of any device must be strictly secured and shall be accessed using secured protocols, such as, SSHv2, HTTPs.
3. The solution shall support latest version Secure Sockets Layer (SSL) encryption and decryption processing, SSL authentication, HTTP data compression and TCP session management.
4. A secure session like an IPsec tunnel, SSH session (SSHv2), HTTPS transport layer security (TLS1.2/TLS1.3) with approved cryptography should be used for secure access management whenever applicable. The detail should be explained.

Security Systems Integration requirements

1. The solution shall integrate with the current AD, Open LDAP to allow importing existing users and groups, when it is necessary. It shall also define, manage, refine security policies, and firewall rules based on user/group identity.
2. The solution should be capable of offering an open protocol/interface for the communication with Ethio telecom security systems such as SOC, IAM, FMS, endpoint security, firewalls, SIEM, log collectors, etc.
3. The solution shall integrate with 3rd party event collection and monitoring, with Log Insight & realize operation

Application layer security

1. The solution shall have configurable User access management including but not limited to configurable password policy, role and right management, group

management, admin account management, account storage on the database and on file.

2. To secure communications between the client and the backend server there should be a certificate check on the client-side to be ensured/approves by the organization.

3. Session expiration/timeout should be implemented to high-risk and for low-risk applications separately.

4. Provide least privilege to application users (all users should only have access to what they absolutely need and no more than that.)

Mobile application security requirement

1. All application data should be encrypted with secure encryption; whether data is at rest on the device, or in transit between the device and servers behind firewall; All information should be secured from end-to-end.

2. All application information accessed via mobile devices should be completely isolated from a user's data by creating a layer of protection around enterprise-deployed apps, to securely separate corporate data, employee's data and consumer data.

3. The mobile application should prevent redirection of its traffic to a malicious server by checking that host-name lookup with DNS resolves to a white-listed IP.

High Availability and Backup Requirements

1. The solution shall incorporate component and functional resilience and eliminate any single points of failure (both from SW, HW and service point of view).

2. All the solution elements should support software HA independent of the infrastructure layer, which is in Active/Standby redundancy or load balancing, no single failure point, no stable service is lost in software module swapping.

3. The solution shall support high and reliable storage of data which is realized by using multiple data and redundant means to ensure the reliability of user data is 99.99%. It shall provide across data center high availability for datacenter nodes.

4. The solution shall guarantee 100% service restore in case of failure.

5. The system should backup all the data including but not limited to files, folders, images, system state, databases, OS and enterprise applications and shall be carried according to the company's backup policy.
6. The solution shall provide on-demand and schedule backup service automatically.as required.
7. In addition, it shall support automatic recovery, but if a fault situation is corrected based on automatic recovery, the fault log shall be updated with the module, reason and action taken by the system

5. Commercial proposal

Interested partners must provide their commercial proposal to work with Ethio telecom as mobile backup solution for an agreed period. Specifically, the partner who seeks to work with Ethio telecom shall:

- Provide the commercial proposal including proposed revenue share for the service engagement with ethio telecom.
- Prepare a business plan, business strategy and revenue projection (for at least three year)
- Provide three-year road map in terms of the implementation of the mobile backup solution in the market with Ethio telecom.

6. Confidentiality and Public Disclosure

- Partners shall treat all information obtained from Ethio telecom which is not generally available to the public as confidential and/or proprietary to Ethio telecom.
- Partners shall exercise all reasonable precautions to prevent any information derived from such sources from being disclosed to any other person.
- If required, Ethio telecom as a government/public corporation, is subject to state and local public disclosure laws and, as such, is legally obligated to disclose to the public documents, including proposals, to the extent required by laws.

- Ethio telecom will keep the confidentiality of the documents and will not expose competitive information to third party.

7. Proposal administration

- Proposal submission

Please use the RFP template provided on this document for your side responses.

All proposals must be submitted in hardcopy to Marketing Division (Eeyor Tower, 8th floor, Room no. 807) and electronically via rfp.marketing@ethiotelecom.et till February 4, 2021.

Moreover, they shall comply with the following requirements during preparation of the Proposal:

- The Proposal and all associated correspondence shall be written in English. Any interlineations, erasures or over writings shall be valid only if they are initialed by the authorized person signing the Proposal.
- Proposals received by facsimile shall be treated as defective, invalid and rejected. Only detailed complete proposals in the form indicated above received prior to the closing time and date of the proposals shall be taken as valid.
- Partners are not permitted to modify, substitute, or withdraw Proposals after its submission. Modifications to proposals already submitted will be allowed if submitted in writing prior to the time fixed in the Request for Proposals.
- The partner shall prepare the technical proposal in hard copy along with a soft copy and sealed in a separate cover. Similarly, Commercial Proposal in hard copy along with a soft copy and sealed in a separate cover.

Proposals and any other related documents prepared in response to this RFP will not be considered unless they are filed to the correct address within the period.

Timeline:

Action	Tentative Schedule
RFP posted	January 4, 2021
Submission deadline	February 4, 2021

- Proposal Review and Discussion.

Ethio telecom will enter discussion with any one or more applicants regarding business model, engagement approach, price, scope of services, or any other term of their proposals, and such other contractual terms, at any time prior to execution of a final contract.

RFP Template

The proposals submitted in response to this RFP must include a cover letter signed by the person authorized to issue the proposal on behalf of the company.
The proposal should also include:

- A cover letter which summarizes the response, includes areas to which response is made and indicates if supporting documentation is included in your response.
- The RFP shall be prepared shall address the following parts but not limited to:

A. General Information
- Parent company:
  o Business Name, address, telephone number, website,
  o A primary contact, including name, job title, address, telephone and email address.
- Local representative
  o Authorization letter
  o Agent information
  o Business license and taxpayer identification number (Local)

B. Company Profile

- Qualified partners should submit a company profile and experience showing but not limited to the below (as applicable)
    - o The prospective authorized Mobile backup business experience supported by a brief company profile. They shall present business experience supported by a brief company profile including but not limited to:
    - o A description of business background, including, country of origin, primary mission of business, business experience and any other information relevant to this RFP.
    - o Successful years of experiences in providing back up and telecom related services
        - o Staff resources
        - o The qualification of the management
        - o The business experience of the management and the staffs preferably in Telecom related services
    - o Track record related to the role played acted as partners into different markets
    - o Provide at least two references for the successful role carried for Mobile backup solution
- Relevant partners experience working with operators in African market is desirable.
- Mobile backup solution portfolio:
    - ❖ Partners platform, equipment and other relevant hardware and software components.
    - ❖ Service access channels: How users access to services: via internet/web / mobile client or via USSD, SMS and other if any.
    - ❖ Product offers/Service type
    - ❖ High level service/ solution architecture describing components and key integration points.

C. Project Understanding

Provide a brief narrative statement that confirms your understanding of the project, and agreement to provide required products and services as Mobile backup solution necessary to achieve the objectives of the project. Describe how your strategy and business experience will benefit the project.

Demonstrating clear understanding of Ethio telecom technical and operational requirements

- Brief baseline assessment of Ethio telecom Digital and VAS market size, roadblocks, regulations, and ecosystem, etc
- Digital and VAS roadmap and strategy for business, government, and the critical mass
- Revenue projection by category for three years
- Classification of Digital and VAS
- Assessment of current gaps in Ethio telecom related to delivery of digital and VAS offers with benchmark and gap

D. Engagement scope

Provide a proposed scope of work, including a proposal and project milestones, in accordance with "Scope of Work," of this RFP. Please make sure to include a statement regarding how you engage a diverse range of partners / content providers & stakeholders from the market at large.

Potential partners should describe in detail:

- Proposal scope, objective and how the solution will be realized.
- Product and Services to be delivered, with different business or technical environments,
- Technical and integration details
- Technology, solution, and related issues

E. Statement of Financial Capacity

- General statement of the financial condition
- most recent audited financial statements
- Disclosure of any bankruptcy filings over the past five years

F. Engaging local business entity

- Availability of local business entity that can actively be engaged.
- Readiness and capability in delivering the required services
- List of professionals for project implementation
- Proof of capability/ certification/ relevant experience

G. Commercial proposal

A. Business/ financial strategy

- Present strategic roadmap for project implementation, priority areas and a detailed look at specific recommended projects with costs projections.
- Proposed revenue share model and modality for the engagement.
- Identify opportunities for quick wins and solutions that produce rapid returns on investment for the earlier stages of implementation
- Detailed cost information for each option/alternative. The cost proposal must identify, by separate item, task and activity required for each deliverable.
- Propose Go to market strategy and Co-marketing approaches

B. Delivery time

- Propose the shortest and feasible delivery time for solution.

G. Technical proposal

- Please provide your responses to the technical compliance statement described
- Provide additional technical requirements and platform capabilities you are offering to avail during the project

H Additional information

- Case studies, solution brief /demos
- Benefits to Ethio telecom, partners and customer's/ end users
- Resource and integration requirements
- Preconditions, challenges, or areas of concern
- Any additional information on applications, solution delivery, marketing support, business models etc.