REQUEST FOR PROPOSAL (RFP)

1. Invitation to tender

Section I: Fact Sheet	
Tender No.	CWS/KE/NBO/001/FY27
Description	Provision of reliable, secure, scalable internet connectivity and managed network services for CWS operations
Estimated Cost	Variable, based on bandwidth requirements, site location, redundancy needs, installation costs, equipment, service level commitments, and awarded pricing
Questions and Answers	Questions shall be submitted in writing to **Procurement@cwsafrica.org** or through the procurement portal. **Last Day for Questions:** 12th Nov 2026 12:00 Noon. **Questions will be answered by:** 13th Nov 2026 12:00 Noon. All questions received will be consolidated and responses will be sent to all the vendors.
Publication Date	09th November 2026
Tender Closure	16th November 2026
Submission Method	Coupa Supplier Portal

1.1 General Conditions for Tender

Church World Service invites qualified, experienced, and duly licensed Internet Service Providers (ISPs) to submit proposals for the provision of reliable, secure, scalable internet connectivity, redundancy, managed network support, performance reporting, and related advisory services. The selected provider shall support CWS in maintaining business continuity, secure connectivity, responsive support, cost-effective service delivery, and compliance with applicable telecommunications, data protection, confidentiality, and procurement requirements.

The scope shall include, but is not limited to, dedicated high-speed internet connectivity, primary and backup links, last-mile connectivity, network equipment where required, managed support, monitoring, security services, service level management, incident response, billing support, and periodic reporting. The selected ISP shall support CWS operations across designated locations.

1.2 Regulatory Compliance and Licensing in Kenya.

The bidder shall comply with all applicable laws, regulations, directives and regulatory requirements governing the provision of internet connectivity, telecommunications, cybersecurity, data protection, taxation, employment and commercial services in Kenya. The bidder shall provide evidence of valid legal registration in Kenya, current tax compliance status and all applicable telecommunications, internet service, infrastructure, network facilities or related authorizations required to deliver the proposed services. Where the bidder relies on subcontractors, wholesale providers, upstream carriers, infrastructure providers or last-mile providers, the bidder shall disclose such parties and provide evidence that they are duly authorized to provide the relevant services in Kenya.

The bidder shall ensure that all services are delivered in accordance with applicable requirements of the Communications Authority of Kenya and any other competent regulatory authority. The bidder shall immediately notify CWS in writing of any actual or threatened suspension, expiry, revocation, enforcement action, regulatory dispute or other matter that may affect the bidder's ability to provide the services. Failure to maintain required licenses, approvals, permits or regulatory compliance shall constitute a material breach of contract and may result in disqualification, suspension of award, termination or any other remedy available to CWS.

1.3 Scope of Services

The ISP shall provide end-to-end internet connectivity and managed network services in a timely, secure, auditable, and customer-focused manner. The provider shall ensure that CWS has stable connectivity, clear service records, defined escalation paths, accurate invoices, and access to technical and commercial support for service, billing, and network performance matters.

1.3.1 Estimated users

Bidders shall size the proposed solution based on the number of users, sites, applications, cloud services, video conferencing requirements and operating model confirmed during the site survey and clarification process.

1.3.2 Bandwidth range per site

Bidders shall propose appropriate bandwidth per site based on CWS operational requirements, expected user load, application usage, video conferencing, cloud services, security tools and business continuity needs. Proposed bandwidth shall be scalable without major redesign.

1.4 Detailed Scope of Internet Services.

The bidder shall provide dedicated, secure, reliable and scalable business-grade internet connectivity services for CWS Kenya operations at the locations specified in this RFP or as later confirmed by CWS.

For each service location, the technical proposal shall specify the connectivity type, primary and backup arrangements, committed information rate, maximum available bandwidth, upload and download speeds, contention ratio, public IP allocation, IPv4 and IPv6 capability, routing design, failover approach, local and international peering, expected latency, jitter and packet loss, last-mile provider, upstream provider and any fair-use, throttling, traffic shaping or service limitation. The bidder shall not apply undisclosed throttling, traffic shaping, bandwidth restriction or fair-use limitation that may affect service quality, continuity or operational performance. The bidder shall provide scalable bandwidth options and clearly state upgrade timelines, costs and technical requirements. The provider shall ensure that CWS has stable connectivity, clear service records, defined escalation paths, accurate invoices, and access to technical and commercial support for service, billing, and network performance matters. Specific service deliverables include:

1.4.1 Internet Connectivity

a) Dedicated high-speed internet services (fiber, wireless, or hybrid)
b) Primary and backup links for redundancy
c) Bandwidth scalability options
d) IPv4/IPv6 compatibility

1.4.2 Network Infrastructure

a) Supply and installation of networking equipment (routers, switches, firewalls)
b) Last-mile connectivity
c) Network configuration and optimization

1.4.3 Managed Services

a) 24/7 monitoring through a Network Operations Center (NOC)
b) Incident management and fault resolution
c) Preventive maintenance
d) Performance monitoring and reporting

1.4.4 Security Services

a) Firewall setup and management
b) DDoS protection and threat monitoring
c) Secure VPN access solutions
d) Compliance with data protection and cybersecurity standards

1.4.5 Cybersecurity and Incident Reporting.

The bidder shall maintain appropriate technical, administrative and organizational cybersecurity controls to protect CWS connectivity, systems, credentials, network traffic, configurations, service information and related data.

Controls shall include;

a) DDoS mitigation,
b) secure VPN support,
c) secure firewall configuration and management,
d) encrypted administrative access,
e) multi-factor authentication for privileged access,
f) role-based access control,
g) secure configuration management,
h) security logging and monitoring,
i) vulnerability management and remediation,
j) change management, incident detection,
k) response and escalation procedures, and abuse handling.

The bidder shall promptly notify CWS of any suspected or confirmed cybersecurity incident, breach, compromise, unauthorized access, service attack, data exposure, credential compromise or other security event that may affect CWS services. The bidder shall cooperate with CWS in investigation, containment, remediation, evidence preservation, root-cause analysis and post-incident reporting.

1.4.6 Reliability & Redundancy

a) Minimum up time of 99.5%
b) Automatic failover mechanisms
c) Disaster recovery support

1.4.7 Business Continuity, Redundancy and Disaster Recovery.

The bidder shall design and deliver a resilient internet connectivity solution that supports business continuity, minimal downtime and rapid service restoration.

The proposed solution should include;

a) Primary and backup links, with target of a minimum monthly uptime of 99.9%, and backup links with a target minimum monthly uptime of 99.5%, unless otherwise agreed in writing by CWS
b) Automatic failover,
c) Resilient upstream connectivity and, where feasible,
d) Diverse last-mile physical routes to reduce single points of failure.
e) Conducting periodic failover tests and provide documented test results showing test date, scope, outcome, issues identified, corrective actions and responsible personnel.
f) Submitting monthly service performance reports showing uptime, downtime, outages, root causes, corrective actions, capacity utilization and service improvement recommendations.

1.4.8 Customer Support

a) Dedicated account manager
b) 24/7 helpdesk support
c) Escalation framework

1.4.9 Expected Service Capacity

a) Multi-site connectivity support
b) Estimated users: West End Towers – Westlands, Nairobi (450 Users), Tana River and Marsabit (Up to 10 Users Each site)

c) Bandwidth range per site: 400 MBPS scalable - West End Towers – Westlands, Nairobi ,30 Mbps Minjila Office (Tana River County, Kenya) – YWCA office – Off Hola Road and 30 Mbps Ngurunit Office (Marsabit County, Kenya) – Kukar Joshua Residence.

See below the coordinates for Tana River and Marsabit.

Location	Site	Coordinates
Minjila, Tana River	YWCA Minjila	-2.3156883221012294, 40.108515001036935
Ngurunit, Marsabit	CWS Office	1.744401, 37.314045

d) Deliverables and Timelines

The Service Provider must meet the following minimum timelines, unless otherwise agreed during contracting:

Deliverable / Service Expectation	Minimum Timeline / Requirement
Site assessment and technical feasibility review	Within 5–10 business days after request or contract instruction
Installation and setup	Within 15–30 business days after approved purchase order, site readiness, and required access approvals
Full-service activation	Within 30 business days, subject to site readiness and third-party dependencies
Standard incident acknowledgement	Within 4 business hours or better
Critical service-impacting escalation acknowledgement	Within 1 hour, with continuous updates until resolution
Performance, utilization, and service report	Monthly, unless CWS agrees to write to a different reporting frequency.

2. Implementation, Migration and Acceptance Testing

The bidder shall submit a detailed implementation plan covering site survey, technical design and architecture, installation schedule, equipment and materials, configuration approach, migration plan, cutover plan, rollback plan, risk management, testing, key personnel, escalation contacts, handover, training and documentation.

No installation, migration, cutover or material service change shall be undertaken without prior coordination and approval by CWS. Acceptance testing shall include connectivity testing, bandwidth testing, failover testing, latency testing, security configuration review and verification of monitoring and reporting tools.

CWS acceptance shall be subject to successful completion of agreed tests and receipt of complete as-built documentation, including network diagrams, IP addressing information, equipment inventory, service configuration details, escalation contacts, SLA reporting process and maintenance procedures.

3. Key Performance Indicators (KPIs)

a) Primary links: minimum 99.9% monthly uptime; backup links: minimum 99.5% monthly uptime, unless otherwise agreed in writing by CWS.
b) ≤ 4-hour incident response
c) ≤ 12-hour outage resolution
d) ≥ 98% service consistency
e) Monthly performance reports

4. Service Level Agreement and Service Credits

The bidder shall commit to measurable service levels for all internet connectivity and managed services, including;

a) monthly uptime,
b) incident response time,
c) incident resolution time,
d) latency,
e) packet loss,
f) jitter,
g) failover time,
h) escalation time,
i) maintenance notification period and
j) monthly reporting obligations.

The bidder shall provide a clear SLA measurement methodology, including how service availability, downtime and exclusions are calculated. Critical incidents affecting CWS business operations shall receive priority response and escalation. The contract shall include service credits or equivalent remedies for missed SLAs. Service credits shall not limit CWS's right to pursue other remedies for repeated, material or prolonged service failures. Repeated failure to meet agreed SLAs, persistent outage, failure to restore services within agreed timelines or failure to implement corrective actions may constitute grounds for termination.

5. Evaluation Criteria

5.1 Stage 1: Eligibility and Mandatory Compliance

(Bidders must meet ALL requirements to proceed to technical evaluation)

No.	Compliance Requirement	Description	Mandatory	Vendor Response
1	Complete Proposal Submission	All required documents submitted as per RFP instructions	Yes	
2	Signed Submission Documents	Proposal duly signed by authorized representative	Yes	
3	Valid Business Registration	Certificate of incorporation or registration provided	Yes	
4	Tax Compliance	Valid tax compliance certificate, where applicable	Yes	
5	ISP / Telecommunications License	Evidence of valid ISP, telecommunications, or equivalent regulatory authorization	Yes	
6	Conflict of Interest Disclosure	Signed declaration confirming no conflict or properly disclosed conflicts	Yes	
7	Sanctions and Compliance Screening	Vendor not listed under sanctions or debarment lists	Yes	
8	Acceptance of Key Tender Terms	Formal acceptance of contractual, commercial, confidentiality, and service terms	Yes	

Critical Components Evaluation

No.	Criteria	Requirement	Evaluation Method	Score
1	Licensing	Valid ISP/telecommunications license	Document verification	Pass/Fail
2	Enterprise Capability	Demonstrated ability to deliver enterprise-level services	Company profile, references	Pass/Fail
3	Infrastructure: Evidence of a minimum of 2 years' experience in supply of at least 300 Mbps symmetric speeds (uploads & downloads) to 2 organizations. Provide map or document or proof showing countrywide coverage including the site (West End Towers). Provide evidence of multiple fiber paths from the site. Show proof that the bidder has direct peering with multiple upstream internet providers (at least 3) e.g SEACOM, TEAMS, EASSY etc. The ONLY accepted connection medium is Fiber. **The supplier must provide 3 /29 Public IP blocks if intending to serve as the Primary Link and 2 /29 Public IP blocks if intending to supply the Alternate Link. This requirement is mandatory.**	Operational infrastructure in service locations	Technical proposal, site presence	Pass/Fail
4	Monitoring Capability	24/7 Network monitoring (NOC)	Technical documentation	Pass/Fail
5	Relevant Experience	Experience with NGOs, INGOs, or corporate clients	Reference checks, past projects	Pass/Fail

Summary of mandatory Pass/Fail Requirements.
Bidders must also provide valid Kenyan registration, current tax compliance, applicable Communications Authority of Kenya license or authorization, disclosure of subcontractors and upstream providers, confirmation of compliance with Kenyan laws, confirmation of compliance with data protection requirements, a complete SLA proposal, a cybersecurity approach and a business continuity and redundancy approach. Failure to submit these mandatory compliance documents may result in disqualification. Only bidders that pass Stage 1 and submit a complete mandatory technical compliance checklist under Stage 2 shall proceed to Stage 3 technical scoring.

5.2 Stage 2: Technical Compliance Checklist — Mandatory, Non-Scored

(Used to validate completeness of proposals)

1. Network Infrastructure & Availability

Requirements	Status	Comments
Minimum Service Level Agreement (SLA) uptime	Yes/No	
Direct peering with multiple upstream internet service providers	Yes/No	
Continuity and Redundancy Controls	Yes/No	
Secure configuration of network equipment	Yes/No	
Change Management Controls	Yes/No	
Power backup for customer premise equipment	Yes/No	
Monitoring, logging & alerting controls	Yes/No	
Incident Response Plan	Yes/No	
Confirm support for native, dual-stack IPv6 routing.	Yes/No	
Confirm ownership or delegation of static public IP blocks (IPv4/IPv6)	Yes/No	

2. Security & Data Protection

Requirements	Status	Comments
Supplier & Interconnection Controls	Yes/No	
Authorisation to operate as an internet service provider	Yes/No	
Compliance with existing standards (NIST/GDPR/local data privacy laws)	Yes/No	
Access Controls Policy	Yes/No	
Patch and Vulnerability Management Policy	Yes/No	
Verify active, upstream scrubbing capabilities.	Yes/No	
Verify compliance with Resource Public Key Infrastructure (RPKI) standards.	Yes/No	
Is the ISP DNS infrastructure secured against spoofing and cache poisoning.	Yes/No	

3. Performance & Quality of Service

Requirements	Status	Comments
Latency threshold	Yes/No	
Jitter threshold	Yes/No	
Packet loss threshold	Yes/No	

4. Support & Maintenance

Requirements	Status	Comments
24/7/365 Network Operations Centre support	Yes/No	
Mean Time to Repair (MTTR)	Yes/No	
Real-time bandwidth utilization and monitoring	Yes/No	

6. Stage 3: Technical Evaluation (70 Points)

Bidders shall confirm inclusion of applicable CA license or authorization, data protection approach, incident reporting procedure, failover testing approach, service credit or remediation action proposal, subcontractor disclosure, insurance evidence, business continuity plan and exit management plan.

No	Technical Criteria	Detailed Assessment Considerations	Weight (%)	Maximum Points
1	ISP Authorization, Compliance, and Regulatory Standing	Evidence of valid ISP or telecommunications licensing; compliance with applicable data protection, cybersecurity, confidentiality, procurement, and regulatory requirements.	**5%**	15
2	Relevant Experience and References	Demonstrated experience delivering internet and managed network services to NGOs, international organizations, multi-site organizations, or entities of comparable complexity; quality of references and evidence of service continuity.	**10%**	10
3	Network Design, Capacity, and Scalability	Quality of proposed architecture, bandwidth sizing, primary and backup connectivity design, last-mile approach, scalability, IPv4/IPv6 readiness, and ability to support CWS operational requirements.	**15%**	15
4	Reliability, Redundancy, and Service Levels	Uptime commitments, redundancy, failover strategy, disaster recovery support, monitoring capability, incident management, restoration targets, and service continuity controls.	**15%**	10
5	Account Management and Support Model	Dedicated account manager, helpdesk availability, Network Operations Center support, escalation contacts, response-time commitments, communication protocols, and issue resolution process.	**10%**	10
6	Security, Reporting, Billing Accuracy, and Controls	Security framework, firewall or DDoS support where applicable, VPN support, performance reports, utilization reports, invoice details, audit trail, billing controls, and error correction process.	**10%**	5
7	Implementation Readiness and Risk Management	Realistic transition plan, rollout schedule, site readiness assumptions, risk mitigation for installation delays, outages, billing disputes, network changes, and stakeholder communication.	**5%**	5
	Total Technical Score		**70%**	**70**

Minimum Technical Threshold: 49/70 i.e. bidders must score at least 49 out of 70 points in the technical evaluation to proceed to financial evaluation. Bidders scoring below 49 points shall be considered technically non-responsive and shall not proceed to financial evaluation. Technical evaluation scoring shall consider;

a) Kenya regulatory compliance and licensing,
b) network design quality and scalability,
c) redundancy and business continuity,
d) SLA strength and service credit framework,
e) cybersecurity controls,
f) data protection and confidentiality safeguards,
g) implementation and migration plan,
h) support model and escalation process,
i) experience with enterprise,
j) NGO, INGO or multi-site clients in Kenya, and
k) quality of reporting and performance management

Only bidders that meet the minimum technical threshold under Stage 3 shall proceed to Stage 4 financial evaluation.

6.1 Stage 4: Financial Evaluation (30 Points)

No	Financial Criteria	Detailed Assessment Considerations	Maximum Points
1	Cost Competitiveness	Lowest evaluated compliant total cost for required bandwidth, installation, equipment, monthly service fees, redundancy, support charges, taxes, and any mandatory fees. The lowest priced compliant proposal receives full points; other proposals are prorated.	20
2	Cost Transparency and Commercial Clarity	Clear site-level pricing, bandwidth assumptions, installation costs, equipment costs, recurring charges, support charges, taxes, discounts, optional services, service validity, escalation costs, and price validity.	10
	Total Financial Score		**30**

6.1.1 Financial Proposal, Pricing Transparency and Total Cost of Ownership

The bidder shall submit a complete financial proposal quoted in Kenya Shillings unless otherwise approved by CWS in writing. The proposal shall have an itemized financial proposal.

Pricing shall be provided by site, service category and contract year where applicable. The bidder shall disclose all assumptions, exclusions, dependencies and conditions affecting pricing. No undisclosed charge shall be payable by CWS unless approved in writing before the cost is incurred. The financial evaluation shall consider the total evaluated cost over the full contract term.

Financial evaluation shall also consider tax clarity, pricing transparency, upgrade and scalability costs, backup and redundancy costs, service credit structure, early termination costs, transition costs and any cost necessary for full implementation and service continuity.

6.1.2 Currency and Taxes

All prices shall be quoted in Kenya Shillings unless otherwise approved by CWS in writing. Bidders shall clearly state whether prices are inclusive or exclusive of VAT, withholding tax, excise duty, levies or any other applicable taxes, duties or statutory charges.

6.1.3 Financial Scoring Formula

Financial Score = (Lowest evaluated compliant price ÷ Bidder's evaluated compliant price) × 20, plus up to 10 points for cost transparency and commercial clarity.

6.2 Stage 5: Final Evaluation and Award Recommendation

Final Score=(TechnicalScore×0.70) +(FinancialScore×0.30)

The Final Score = Technical Score + Financial Score, based on a total maximum score of 100 points, comprising 70 points for technical evaluation and 30 points for financial evaluation.

7. Confidentiality

All information contained in this RFP is confidential and shall not be disclosed without prior written consent from CWS.

8. Data Protection, Privacy and Traffic Confidentiality.

The bidder shall comply with the Kenya Data Protection Act, 2019, applicable regulations and any other applicable data protection, privacy and confidentiality requirements. The bidder shall protect all CWS data, network traffic information, logs, credentials, configurations, IP addressing information, business information and any personal data accessed or processed in connection with the services. The bidder shall process personal data only to the extent necessary to deliver the contracted services and only in accordance with documented instructions from CWS.

The bidder shall implement appropriate technical and organizational measures to protect personal data and confidential information against unauthorized access, disclosure, alteration, loss, destruction or misuse. The bidder shall promptly notify CWS of any suspected or actual personal data breach, unauthorized disclosure, loss of data, compromise of credentials or confidentiality incident.

The bidder shall not transfer, host, access or process CWS personal data outside Kenya without prior written approval from CWS and without appropriate legal, contractual and security safeguards. Upon expiry or termination, the bidder shall return, securely delete or otherwise dispose of CWS information as instructed by CWS, unless retention is required by law.

Where the bidder processes personal data on behalf of CWS, the bidder shall act only on documented instructions from CWS, ensure confidentiality of persons authorized to process the data, implement appropriate security measures, assist CWS with data subject requests and regulatory obligations, notify CWS of personal data breaches without undue delay, delete or return personal data at the end of service provision, and make available information necessary to demonstrate compliance.

9. Conflict of Interest

Bidders must disclose any real or potential conflicts of interest. Failure to disclose may result in disqualification.

10. Fraud and Anti-Corruption

a) CWS maintains zero tolerance for:
b) Fraud
c) Bribery
d) Collusion
e) Misrepresentation
f) Any violation will result in disqualification or contract termination.

11. **Financial Management, Billing, and Audit**
    The ISP shall:
    a) Submit accurate, verifiable invoices
    b) Maintain auditable records of services provided
    c) Allow CWS audit access when required
    d) Avoid overbilling or duplicate billing

12. **Payment Terms**
    Payment shall be made within **30 days** after receipt of invoice and confirmation of satisfactory service delivery.

13. **Contract Terms**
    Initial duration: two years, renewable subject to satisfactory performance, continued need, budget availability and mutual written agreement.

14. **Insurance, Liability and Indemnity.**
    The bidder shall maintain appropriate insurance coverage for the nature, scale and risk of the services provided, including professional liability or errors and omissions insurance, cyber risk insurance, general liability insurance, workers' compensation or employer's liability insurance and equipment or asset coverage where applicable. The bidder shall provide evidence of insurance upon request by CWS.

    The bidder shall be responsible for losses, damages, claims, penalties, costs or liabilities arising from breach of contract, negligence, willful misconduct, regulatory non-compliance, confidentiality breach, data protection breach, cybersecurity incident caused by the bidder, service failure or subcontractor failure.

    The bidder shall indemnify and hold CWS harmless against claims, losses, penalties, damages and reasonable costs arising from the bidder's acts, omissions, breach of law, breach of confidentiality, data incident, security failure or failure to deliver the services in accordance with the contract.

15. **Exit Management and Transition Assistance.**
    Upon expiry, termination or non-renewal of the contract, the bidder shall provide reasonable transition assistance to CWS and/or any replacement provider to ensure service continuity. Transition assistance shall include service documentation handover, network diagrams, configuration information, IP addressing information, equipment inventory, service cancellation support, migration support, coordination with a replacement provider, continuity planning, and return or secure deletion of CWS data and confidential information.

    The bidder shall not withhold transition assistance, documentation or service information due to any dispute, unless expressly permitted by law or contract. The bidder shall cooperate in good faith to minimise disruption to CWS operations during transition.

16. **Performance and Review**
    The ISP shall:
    a) Provide monthly performance reports
    b) Participate in periodic performance reviews
    c) Implement corrective actions where required

    Monthly reports shall include uptime and downtime, incident tickets opened, resolved and pending, response and resolution times, root-cause analysis for outages, corrective and preventive actions, bandwidth utilization, capacity trends, SLA compliance, security events affecting CWS services, planned maintenance and service improvement recommendations.

Where performance falls below agreed standards, the bidder shall submit and implement a corrective action plan within timelines agreed with CWS. Failure to implement corrective actions or repeated underperformance may result in service credits, withholding of payment, escalation, termination or other contractual remedies.

17. **Maintenance, Change Management and Planned Downtime.**
The bidder shall maintain all services, systems and infrastructure required to deliver reliable connectivity to CWS. Planned maintenance shall be communicated to CWS in advance and shall include the expected date, time, duration, service impact, reason for maintenance, risk mitigation measures and escalation contacts. Planned maintenance should be scheduled outside CWS core business hours unless otherwise approved by CWS.
The bidder shall not make material changes to configurations, routing, security settings, bandwidth allocation, IP addressing, service architecture or subcontractor arrangements affecting CWS without prior written approval, except where urgent action is required to mitigate a security or service continuity risk. Emergency maintenance shall be communicated to CWS as soon as reasonably practicable.

18. **Vendor Compliance Requirements**
    a) Vendors must:
    b) Adhere to ethical standards
    c) Comply with legal and regulatory requirements
    d) Maintain transparency in service delivery

19. **Subcontracting, Third Parties and Supply Chain Risk.**
The bidder shall disclose all subcontractors, upstream providers, infrastructure providers, last-mile providers, network operators, managed service providers and other third parties involved in delivering the services.

    The bidder remains fully responsible for all acts, omissions, performance, security, confidentiality, regulatory compliance and service continuity of its subcontractors and third parties. The bidder shall not change any material subcontractor, upstream provider or service delivery partner without prior written notification to and approval by CWS.

    The bidder shall ensure that all subcontractors and third parties comply with the same confidentiality, cybersecurity, data protection, regulatory compliance, service continuity and audit obligations applicable to the bidder. CWS may reject any subcontractor or third party that presents unacceptable legal, operational, cybersecurity, reputational or business continuity risk.

20. **Bid validity period**
Proposals shall remain valid for a minimum of 90 calendar days from the tender closing date, unless CWS requests and the bidder agrees to an extension in writing.
Bidders are responsible for ensuring that all information submitted is accurate, complete and not misleading. CWS may reject any proposal containing material misrepresentation, omission or unverifiable information.

21. **Clarification and addenda process**
All bidder questions must be submitted in writing by the deadline stated in the Fact Sheet. CWS may issue written clarifications or addenda to all participating bidders. Only written clarifications or addenda issued by CWS shall be binding. Oral statements, informal communications or individual discussions shall not amend the RFP.

22. **Late submissions**
Submissions received after the tender closing date and time may be rejected and may not be opened or evaluated, unless CWS determines that acceptance is permitted under applicable internal procurement rules and does not compromise fairness or transparency.

23. **Right to accept, reject or cancel**
    CWS reserves the right to accept or reject any proposal, waive minor informalities, request clarifications, negotiate with one or more bidders, cancel or amend the RFP, split or combine awards, or make no award, without liability to any bidder, subject to applicable procurement requirements and donor or internal approval rules.

24. **Awards are subject to due diligence and approvals**
    This contract award shall be subject to successful completion of due diligence, reference checks, sanctions and compliance screening, technical validation, contract negotiations, budget availability and all required internal or donor approvals.

25. **No reimbursement of proposal costs**
    Bidders are responsible for all costs incurred in preparing and submitting proposals, attending meetings, providing clarifications, participating in demonstrations or supporting due diligence. CWS shall not reimburse proposal costs.

    Issuance of this RFP does not constitute a commitment by CWS to award a contract or pay any costs incurred in preparing a proposal. CWS may cancel, amend, suspend or reissue the RFP at any time in accordance with applicable procurement requirements.

26. **Site survey and bidder responsibility**
    Bidders shall be responsible for verifying site feasibility, last-mile availability, installation constraints, power requirements, rooftop or building access requirements, landlord approvals, cabling routes, equipment requirements and any dependencies necessary to deliver the proposed services. Any assumptions, exclusions or dependencies must be clearly stated in the proposal.

27. **Service acceptance and start of billing**
    Billing shall not commence for any service until CWS confirms successful service activation and acceptance in writing. Acceptance shall be based on successful completion of agreed testing, receipt of required documentation and confirmation that the service is operational and meets the agreed technical and SLA requirements.

28. **Ownership and return of equipment**
    The proposal shall clearly state whether equipment is owned by CWS, leased, rented or provided as part of the managed service. The bidder shall identify responsibility for maintenance, replacement, insurance, warranty and return of equipment upon termination or expiry.

29. **Non-exclusivity**
    Any resulting contract shall not prevent CWS from procuring similar or complementary services from other providers where required for redundancy, geographic coverage, cost efficiency, risk mitigation or business continuity.

30. **Governing law and dispute resolution**
    The RFP and any resulting contract shall be governed by the laws of Kenya, unless otherwise stated in the final contract. The parties shall first attempt to resolve disputes through good-faith negotiation. If unresolved, disputes shall be handled in accordance with the dispute resolution mechanism set out in the final contract.

31. **Sanctions, Anti-Terrorism and Donor Compliance**
    Bidders, their directors, beneficial owners, key personnel, subcontractors and upstream providers must not be subject to applicable sanctions, terrorism financing restrictions, debarment, exclusion or donor prohibition. CWS may conduct screening and due diligence at any stage and may reject or terminate where compliance concerns arise.

32. **Force majeure**
Neither party shall be liable for failure or delay caused by events beyond its reasonable control, provided that the affected party promptly notifies the other party, takes reasonable steps to mitigate the impact and resumes performance as soon as practicable. Force majeure shall not excuse payment obligations for services properly delivered before the event or the bidder's obligation to implement agreed business continuity and disaster recovery measures.

33. **Submission Requirements**
a) Proposals and should include:
b) Technical proposal
c) Financial proposal
d) Required supporting documentation
e) Signed submission
- Certificate of incorporation or registration.
- Valid tax compliance certificate.
- Applicable Communications Authority of Kenya license or authorization.
- Company profile, technical proposal and financial proposal. (with clearly indicated table of content)
- Network architecture and service design.
- Business continuity and redundancy plan.
- Cybersecurity controls summary.
- Data protection and confidentiality approach.
- Implementation and migration plan.
- SLA proposal and escalation matrix.
- Evidence of relevant experience and client references.
- Subcontractor and upstream provider disclosure.
- Exit Management and Transition Assistance Plan
- Insurance certificates, where applicable.
- Signed conflict of interest declaration, vendor disclosure form and non-disclosure agreement and any other form.
- Data Protection Declaration;

34. **Submission Method**
Submit via: Coupa Procurement System

35. **Attachments to the Tender Package**
The annexes listed below form part of this tender document.
Annex 1: Vendor Information Form and Vendor Disclosure Form
Annex 2: Evaluation Criteria-Administrative and Technical Evaluation
Annex 3: Supplier code of conduct
Annex 4: Church World Service Terms & Conditions
Annex 5: Supplier Conflict of Interest Declaration Form
Annex 6: Non-Disclosure Agreement (NDA)
Annex 7: Technical Compliance Checklist;
Annex 8: Cybersecurity Questionnaire;
Annex 9: Policy Acknowledgment and Compliance Declaration
Annex 10: Pricing Offer Sheet

Annex 1: Vendor Information Form

Section 1 – Business Details

1. Business Name _____ _____
2. Physical Address _____
3. Mailing Address _____

   Email Address _____
4. Telephone Number (s) _____
5. Primary Contact _____
6. Title/Designation _____
7. Secondary Contact _____
8. Title/Designation _____

Section 2 – Registration Details

a. Registered Name _____
b. Type of Registration _____
   (Private company, close corporation, partnership, sole proprietorship, non-profit company, or other)
c. Tax Number / VAT Number _____
d. Company Officers _____

Section 3 – Goods / Services Provided

1. Is the business a manufacturer, trader/distributor, or service provider?
2. What is the main line of goods or services provided?
3. Do you wish to be considered a vendor for any other goods or services? If so, please explain.

Section 4 – Payment Terms & Method

Church World Service prefers a minimum of 30 days' credit from the date of invoice and electronic payment. Please state the credit period and preferred payment method if different from the above.

Section 5-Bank Details

Account Name	
Bank Name	
Bank branch	
Account Number	
Currency	
Branch Code	
Swift Code	

Please note that it is against Church World Service policies for staff to ask for favors of any kind from vendors. It is also against our procurement policies for any vendor to pay in cash or in kind for any favors.

Vendors are responsible for maintaining secure banking and communication controls. Church World Service shall not be liable for payments misdirected due to compromise of the vendor's systems or communications.
For this tender, vendors shall also confirm controls for protecting traveler and approved migrant personal information, including secure handling of passports, visas, manifests, payment information, special assistance needs, and other sensitive records, and shall identify the officer responsible for privacy and information security compliance.

Name of vendor's authorized official: _____
Signature: _____
Date completed: _____

Annex 2: Evaluation Criteria-Administrative and Technical Evaluation

Eligibility and Mandatory Compliance

No	Compliance Requirement	Description	Mandatory	Vendor Response
1	Complete Proposal Submission	All required documents submitted as per RFP instructions	Yes	
2	Signed Submission Documents	Proposal duly signed by authorized representative	Yes	
3	Valid Business Registration	Certificate of incorporation or registration provided	Yes	
4	Tax Compliance	Valid tax compliance certificate, where applicable	Yes	
5	ISP / Telecommunications License	Evidence of valid ISP, telecommunications, or equivalent regulatory authorization	Yes	
6	Conflict of Interest Disclosure	Signed declaration confirming no conflict or properly disclosed conflicts	Yes	
7	Sanctions and Compliance Screening	Vendor not listed under sanctions or debarment lists	Yes	
8	Acceptance of Key Tender Terms	Formal acceptance of contractual, commercial, confidentiality, and service terms	Yes	

Critical Components Evaluation

No.	Criteria	Requirement	Evaluation Method	Score
1	Licensing	Valid ISP/telecommunications license	Document verification	Pass/Fail
2	Enterprise Capability	Demonstrated ability to deliver enterprise-level services	Company profile, references	Pass/Fail
3	Infrastructure: Evidence of a minimum of 2 years' experience in supply of at least 300 Mbps symmetric speeds (uploads & downloads) to 2 organizations Provide map or document or proof showing countrywide coverage including the site (West End Towers). Provide evidence of multiple fiber paths from the site. Show proof that the bidder has direct peering with multiple upstream internet providers (at least 3) e.g SEACOM, TEAMS,	Operational infrastructure in service locations	Technical proposal, site presence	Pass/Fail

	EASSY etc. The ONLY accepted connection medium is Fiber. **The supplier must provide 3 /29 Public IP blocks if intending to serve as the Primary Link and 2 /29 Public IP blocks if intending to supply the Alternate Link. This requirement is mandatory.**			
4	Monitoring Capability	24/7 Network monitoring (NOC)	Technical documentation	Pass/Fail
5	Relevant Experience	Experience with NGOs, INGOs, or corporate clients	Reference checks, past projects	Pass/Fail

Technical Evaluation (70 Points)

No	Technical Criteria	Detailed Assessment Considerations	Weight (%)	Maximum Points
1	ISP Authorization, Compliance, and Regulatory Standing	Evidence of valid ISP or telecommunications licensing; compliance with applicable data protection, cybersecurity, confidentiality, procurement, and regulatory requirements.	**5%**	15
2	Relevant Experience and References	Demonstrated experience delivering internet and managed network services to NGOs, international organizations, multi-site organizations, or entities of comparable complexity; quality of references and evidence of service continuity.	**10%**	10
3	Network Design, Capacity, and Scalability	Quality of proposed architecture, bandwidth sizing, primary and backup connectivity design, last-mile approach, scalability, IPv4/IPv6 readiness, and ability to support CWS operational requirements.	**15%**	15
4	Reliability, Redundancy, and Service Levels	Uptime commitments, redundancy, failover strategy, disaster recovery support, monitoring capability, incident management, restoration targets, and service continuity controls.	**15%**	10
5	Account Management and Support Model	Dedicated account manager, helpdesk availability, Network Operations Center support, escalation contacts, response-time commitments, communication protocols, and issue resolution process.	**10%**	10
6	Security, Reporting, Billing Accuracy, and Controls	Security framework, firewall or DDoS support where applicable, VPN support, performance reports, utilization reports, invoice details, audit trail, billing controls, and error correction process.	**10%**	5
7	Implementation Readiness and Risk Management	Realistic transition plan, rollout schedule, site readiness assumptions, risk mitigation for installation delays, outages, billing disputes, network changes, and stakeholder communication.	**5%**	5
	Total Technical Score		**70%**	**70**

Annex 3: Supplier Code of Conduct

1. **Introduction**

   Suppliers, contractors, and service providers ("Suppliers") are expected to uphold the highest standards of ethical conduct, integrity, and accountability in all business interactions.

   This Supplier Code of Conduct reflects a commitment to prevent:

   - Sexual exploitation and abuse (SEA)
   - Fraud and corruption
   - Abuse of power
   - Harassment and discrimination
   - Unethical business practices

   These standards are aligned with international humanitarian and development principles.

2. **Purpose**

   The purpose of this Code is to:

   - Promote ethical and responsible business practices across the supply chain
   - Protect individuals and communities from abuse and exploitation
   - Ensure transparency, fairness, and accountability in procurement and service delivery
   - Provide clear behavioral expectations for all Suppliers

   This Code serves as a mandatory requirement for all Suppliers doing business with the organization.

3. **Scope**

   This Code applies to:

   - All Suppliers, vendors, contractors, and subcontractors
   - Supplier employees, agents, and representatives
   - Any third party involved in the delivery of goods or services

   Suppliers must also ensure that their own supply chain complies with these principles where applicable.

4. **Supplier Standards of Conduct**

   1.1 **Human Rights and Respect**

   Suppliers shall:

   - Respect and uphold fundamental human rights without discrimination
   - Treat all individuals with dignity, fairness, and respect
   - Ensure their operations do not cause harm to communities or vulnerable populations
   - Comply with applicable international laws, standards, and local regulations

   1.2 **Prevention of Sexual Exploitation and Abuse (SEA)**

   Suppliers must strictly prohibit:

   - Any form of sexual exploitation or abuse, which is considered gross misconduct
   - Sexual activity with people under 18 years of age
   - Exchange of goods, services, employment, or assistance for sexual favors
   - Exploitation of vulnerable individuals or abuse of unequal power dynamics

   Suppliers are expected to:

   - Maintain a zero-tolerance approach to SEA
   - Report any suspected violations immediately
   - Promote a safe environment that prevents exploitation and abuse

   1.3 **Child Protection and Safeguarding**

   Suppliers shall maintain a child-safe environment across all operations, personnel, subcontractors, and service delivery activities.

   - Prohibit all forms of violence, abuse, neglect, exploitation, and harmful conduct involving children.

- Apply safe recruitment, supervision, and conduct standards for personnel who may interact with children.
- Immediately report child safeguarding concerns through designated reporting channels and protect children and reporters from retaliation.

1.4 **Harassment, Discrimination, and Workplace Behavior**

Suppliers shall:

- Prohibit all forms of harassment, bullying, and discrimination
- Maintain workplaces free from offensive, humiliating, or abusive conduct
- Promote inclusion, respect, and dignity
- Take appropriate disciplinary action against violations

1.5 **Fraud, Corruption, and Integrity**

Suppliers must adhere to a zero-tolerance policy toward fraud and corruption.

Suppliers shall:

- Never engage in bribery, kickbacks, or improper financial gain
- Ensure transparency in all financial transactions
- Avoid falsification of records or documents
- Protect confidential information
- Maintain accurate financial and operational records

1.6 **Ethical Business Practices**

Suppliers shall:

- Operate with honesty, transparency, and fairness
- Declare conflicts of interest (e.g., relationships with staff or decision-makers)
- Not offer or accept gifts that improperly influence decisions
- Avoid unethical profit-sharing arrangements
- Ensure fair competition in procurement processes

1.7 **Labor Standards**

Suppliers must:

- Prohibit child labor, forced labor, and exploitative labor practices
- Ensure safe and healthy working conditions
- Comply with local labor laws and international standards
- Pay fair wages and applicable taxes

1.8 **Environmental Responsibility**

Suppliers shall:

- Minimize environmental impact in operations
- Ensure goods are produced ethically and responsibly
- Avoid supplying unsafe or harmful products

1.9 **Security and Safety**

Suppliers must:

- Provide safe working environments
- Ensure compliance with applicable safety and security regulations
- Prohibit handling weapons or unsafe practices during service delivery

5. **Reporting and Compliance**
   Suppliers must report suspected misconduct, unethical behavior, safeguarding concerns, or violations immediately through designated reporting channels: Fraud@cwsafrica.org and must cooperate fully with any review, audit, or investigation.
   - Report concerns promptly using the organization's designated reporting channels or other approved contractual reporting mechanisms.
   - Preserve relevant records and provide timely information requested for investigations or compliance reviews.
   - Maintain confidentiality and prohibit retaliation against whistleblowers, affected persons, witnesses, or anyone raising a concern in good faith.

   Failure to comply with this Code may result in:
   - Contract termination
   - Disqualification from future business
   - Legal action, where applicable
6. **Supplier Acknowledgment and Commitment**
   By signing the Supplier Code of Conduct (SCC), the Supplier formally acknowledges and agrees to comply with the standards and requirements set forth herein.
   The Supplier shall:
   - Review and understand this Code and ensure alignment with all applicable requirements.
   - Confirm compliance with this Code as a condition of doing business and maintain compliance throughout the contractual relationship.
   - Ensure employees, agents, affiliates, and subcontractors are informed of, trained on, and comply with this Code.
   - Implement appropriate policies, procedures, monitoring, and oversight mechanisms to ensure ongoing adherence.
   - Cooperate with audits, assessments, or investigations and provide evidence of compliance upon request.
   - Accept accountability for non-compliance, including corrective action, suspension, contract termination, or disqualification from future business.
7. **Continuous Improvement**
   Suppliers are encouraged to:
   - Develop systems to ensure ongoing compliance
   - Train employees on ethical conduct
   - Strengthen internal controls and accountability mechanisms.
8. **Authorized Signatory**

   Supplier Name: _____
   Authorized Representative: _____
   Title: _____
   Signature: _____
   Date: _____

Annex 4: Church World Service Terms and Conditions

1. Defined Terms. Each of the following terms has been used more repeatedly in this document: Authorized Representative, Contract Number, Delivery Date, Delivery Location, Delivery Terms, Donor Terms, Goods, Packing Requirements, Pricing, and Specifications. Other terms are defined as specified throughout this Agreement.
2. Purchase and Sale of Goods. Supplier will sell to Church World Service, and Church World Service will purchase and pay for, the Goods in accordance with the terms and conditions set forth in this Agreement.
3. Specifications. The Goods must strictly comply with or exceed the Specifications. No deviation, substitution or change is permitted without Church World Service' prior written consent.
4. Purchase Order Amendments. Church World Service may suspend Supplier's performance, increase or decrease the ordered quantities, or make changes for Church World Service' reasonable business needs by written notice to Supplier (each, a "Purchase Order Amendment"). Unless mutually agreed, a Purchase Order Amendment does not apply to change the Goods timely and fully delivered and accepted before the date of the Purchase Order Amendment. If any change causes an increase or decrease in the cost of, or the time required for, Supplier's performance, an equitable adjustment may be made in the price or delivery schedule or both, if such adjustment is set forth in a Purchase Order Amendment signed by the Authorized Representative.
5. Inspection, Acceptance and Rejection.

a. All Goods will be subject to Church World Service' inspection and testing, at any time and place, including the period of manufacture/production/creation and before final acceptance. If Church World Service inspects or tests at Supplier's premises, Supplier, without additional charge, will provide all reasonable facilities and assistance for the safety and convenience of Church World Service' inspectors. No inspection or testing done or not done before final inspection and acceptance will relieve Supplier from responsibility for defects or for other failure to meet the requirements of this Agreement. Notwithstanding any prior inspections or payments made, all Goods will be subject to final inspection and acceptance at the Delivery Location within a reasonable time after delivery (but in no event, less than five business days after the date of delivery).

b. Acceptance will occur only when the Authorized Representative delivers written, signed notice of acceptance to Supplier in the form of a goods received notice ("GRN") and such notice has been signed by Supplier's representative. The GRN must include: (1) the GRN number; (2) the Contract number; (3) a description of the Goods; (4) the quantity delivered; (5) final inspection date and location; (6) quantity accepted; and (7) quantity rejected or over-shipped.

c. If any delivery, documentation or the Goods delivered do not comply with all of the terms and conditions of this Agreement, Church World Service may do one or more of the following: (1) reject such nonconforming Goods, accept conforming Goods and reduce the purchase price by such amount as Church World Service determines in good faith reflects the value to Church World Service of the accepted Goods, (2) accept such nonconforming Goods and reduce the purchase price by such amount as Church World Service determines in good faith reflects the reduced value to Church World Service of such nonconforming Goods; (3) reject all Goods; and/or (4) terminate this Agreement without any further obligation on Church World Service' part.

d. If any Goods are finally accepted, Church World Service will only pay for the quantity accepted up to the quantity specified in this Agreement. Church World Service will in no event pay for quantity above the amount provided for in this Agreement or accepted. Church World Service or its agent will hold overshipments and non-conforming shipments at Supplier's risk and expense for a reasonable time awaiting Supplier's instructions. Supplier will bear the expense of return charges, storage charges and other expenses for over-shipped quantities and Goods not accepted.

6. Packing. All Goods will be prepared for shipping and delivery and will be shipped in accordance with the Packing Requirements. Price based on weight will include net weight only. Supplier will not charge Church World Service for packaging or pre-shipping costs, such as boxing, crating, handling damage, drayage, or storage. Supplier will mark all containers with necessary handling and shipping information, Contract Number, date of shipment, and names of the consignee and consignor. A packing list, and other

documentation required for domestic or international transit, regulatory clearance or identification of the Goods will accompany each shipment.

7. Transportation, Shipment and Delivery. Shipment/transportation will be in accordance with the Delivery Terms, Delivery Date, and Delivery Location. Church World Service will not be charged for shipping, delivery, loading or unloading costs unless otherwise specified in the Delivery Terms.
8. Risk of Loss. Supplier will bear all risk of loss, damage, or destruction to the Goods, in whole or in part, occurring before final acceptance by Church World Service at the Delivery Location; provided, Church World Service is responsible for any loss caused by its gross negligence.
9. Taxes, Duties and Expenses.

a. All taxes, duties and other governmental charges with respect to the manufacture/production/creation of the Goods and the delivery of the Goods to Church World Service in accordance with this Agreement will be the liability of, and borne solely by, Supplier. If the law requires Church World Service to withhold taxes from payments to Supplier, Church World Service may withhold those taxes and pay them to the appropriate taxing authority. Church World Service will deliver to Supplier an official notice for such taxes. Church World Service will use reasonable efforts to minimize any taxes withheld to the extent allowed by law.

b. Supplier is responsible for all expenses incurred by it in performing under this Agreement.

10. Invoicing and Payment.

a. Church World Service will have no obligation to make any payment to Supplier with respect to the Goods until final acceptance in accordance with Section 4(b) and delivery of an invoice that fully complies with the requirements specified in this Agreement. Invoices may only be submitted after Supplier receives a GRN. Invoices must be submitted within 60 days of Supplier's acceptance of a GRN. Church World Service will have no obligation to pay an invoice submitted after 60 days or to pay an invoice amount that Church World Service disputes in a written notice to Supplier. Each invoice must contain or attach the following:

i. a copy of the signed GRN;
ii. supplier's name and address;
iii. description of the Goods delivered, delivery date, quantity, unit price and total price to be paid;
iv. all information necessary for Church World Service to implement payment (e.g., name of representative to address payment to, address, bank account information as applicable for the method of payment);
v. the Contract Number;
vi. packing slip number;
vii. taxes and duties (only if payable by Church World Service per the terms of this Agreement);
viii. delivery Location and Delivery Date; and (9) any other information reasonably required by Church World Service. Invoices will only be deemed received on the date they are delivered to the Authorized Representative and in full compliance with the requirements herein.

b. Church World Service will make payment within 30 days of receipt of Supplier's fully conforming invoice. Payment of an invoice will not constitute acceptance of Goods, and is subject to adjustment for errors, shortages, defects or other failure of Supplier to meet the requirements of this Agreement. Church World Service may set-off amounts owed to Church World Service against an amount Church World Service owes to Supplier or Supplier's affiliated companies, and Church World Service will provide notice to Supplier within a reasonable time after the setoff.

11. Representations, Warranties and Additional Covenants. Supplier represents and warrants to Church World Service and covenants with Church World. Service as follows:

a. Supplier has full rights and authority to enter into and perform its obligations under this Agreement. Supplier's performance will not violate any agreement or obligation between Supplier and any third party.

b. The Goods and all documentation required will meet each of the standards and specifications set forth in this Agreement. The Goods are merchantable and fit for their intended purpose, comply with all applicable law and are free from all defects in material and workmanship.

c. Supplier will deliver good and marketable title to the Goods free and clear of all liens, claims, encumbrances and interests of any other person, entity or government. The Goods will not infringe on any patent, copyright, trademark, trade secret or other proprietary right of any third party.

d. Supplier will comply with all applicable law, regulations and rules in the performance of its obligations under this Agreement.

e. Supplier has not, and will not, engage in transactions with, or provide resources or support to, individuals and organizations associated with terrorism, including those individuals or entities that appear on the Specially Designated Nationals and Blocked Persons List maintained by the U.S. Treasury (http://www.treasury.gov/resource-center/sanctions/SDN-List/Pages/default.aspx) or the United Nations Security designation list (http://www.un.org/sc/committees/1267/aq_sanctions_list.shtml).
f. Supplier will comply with and train its employees in all applicable laws against bribery, corruption, inaccurate books and records, inadequate internal controls and money-laundering, including the U.S. Foreign Corrupt Practices Act and the UK Bribery Act. Supplier has not and will not offer or give any employee, agent, or representative of Church World Service anything of value to secure any business from Church World Service or influence such person to alter the terms, conditions, or performance of any contract with or purchase order from Church World Service, including but not limited to this Agreement.
g. Supplier does not own, directly or indirectly, any other company that was competing for award of this Agreement. Supplier did not seek or obtain confidential information related to the award of this Agreement from any Church World Service employee, agent or representative. Supplier did not collude or conspire with any other individual or entity to limit competition for the award of this Agreement, to set prices being offered or in any other way to interfere with free and open competition.
h. Supplier is not owned in whole or in part, directly or indirectly, by any immediate or extended family member of any Church World Service employee, agent or representative, or, if so owned, Supplier fully disclosed such relationship and any potential conflict of interest has been waived by Church World Service.
i. Supplier shall be compliant with the CWS Child Safeguarding and Anti Human Trafficking policies.
j. Supplier is not the subject of any governmental or donor investigation and has not been debarred or suspended by any government, governmental agency or donor.

12. Confidentiality. Supplier will maintain the confidentiality of:

i. any information Church World Service provides to Supplier that Church World Service identifies as confidential;
ii. the terms and conditions of this Agreement; and
iii. non-public information regarding Church World Service' policies and practices.

Upon Church World Service' request, Supplier will return to Church World Service all confidential information provided by Church World Service to Supplier. This confidentiality obligation will survive final acceptance of the Goods, payment of the purchase price and termination of this Agreement.

13. Indemnification. Supplier will indemnify Church World Service and each of its officers, directors, employees, representatives and agents (each, an "Indemnitee"),and hold them harmless from, any and all losses, claims, damages, liabilities, any government or donor investigations, fines or penalties and related expenses (including incidental and consequential damages and reasonable attorneys' fees, whether incurred at the investigative, trial or appellate level or otherwise) incurred by any Indemnitee or asserted against any Indemnitee by any third party or by Supplier arising out of, in connection with, or as a result of this Agreement, any failure by Supplier to fully perform its obligations under this Agreement or any breach by Supplier of any of its representations and warranties under this Agreement, provided that such indemnity will not, as to any Indemnitee, be available to the extent that such losses, claims, damages, liabilities or related expenses resulted from the gross negligence or wilful misconduct of such Indemnitee. This indemnity obligation will survive final acceptance of the Goods, payment of the purchase price and termination of this Agreement.
14. Termination and Remedies. This Agreement may be terminated under the following circumstances:

a. by both Parties on mutual written agreement of the Parties;
b. by Church World Service immediately upon written notice in the event Church World Service' donor(s) terminates or withdraws funding that Church World Service would use to pay Contractor under this Agreement;
c. by either Party due to the non-terminating Party's breach of this Agreement and failure to correct such breach within 15 days' prior notice of such breach;
d. by either Party upon written notice if a force majeure event, including any not reasonably foreseeable war, insurrection, change in law or government action or inaction, strike, natural disaster or similar event, prevents the terminating Party from being able to fulfil its obligations under this Agreement; or

e. by Church World Service immediately upon written notice if Church World Service using its sole discretion determines that Contractor has or will breach any of its warranties, covenants or representations in this Agreement, in which case Church World Service may withhold any and all amounts owed to Contractor until such breach is remedied. In the event termination is due to Church World Service' breach of this Agreement, by Church World Service for Church World Service convenience, due to force majeure event, or due to loss of funding, Church World Service shall be obligated to pay Contractor for its reasonable, pro-rated costs of work completed and expenses properly incurred prior to termination.

f. If Church World Service determines that Supplier has or will breach any of its warranties, covenants or representations in this Agreement, Church World Service may, in addition to any other remedies for such breach available at law or in equity, (i) terminate this Agreement; (ii) reject any Goods delivered; (iii) return any Goods already accepted and obtain full repayment for any amount paid for such Goods; (iv) if Supplier breaches Section 10(j), withhold payment until such investigation, suspension or debarment is lifted; and (v) if Supplier breaches any of Section 10(e), (f), (g), (h) or (i), not pay for any Goods that have been accepted but that have been consumed or otherwise cannot be returned to Supplier and report the breach to Church World Service donors and appropriate governmental authorities.

15. Dispute Resolution. Any unresolved dispute or claim will be settled by arbitration administered by the International Centre for Dispute Resolution in accordance with its International Arbitration Rules. ("INTERNATIONAL DISPUTE RESOLUTION PROCEDURES") The number of arbitrators will be one. The place of arbitration will be Kenya. The language of arbitration will be English.

16. Access to Books and Records. Church World Service, its donors (including, if applicable, PRM and the Comptroller General of the United States) and any of their respective representatives will have access to any books, documents, papers and records of Supplier that are directly pertinent to this Agreement for the purpose of making audits, examinations, excerpts and transcriptions.

17. Additional Donor Terms and Conditions. The Donor Terms (if any) are incorporated in this Agreement by reference and are fully binding on Supplier and Church World Service. In the event of a conflict between the Donor Terms and this Agreement or any other document between Supplier and Church World Service, the Donor Terms will prevail.

18. Miscellaneous.

a. This Agreement and the rights and obligations of the parties hereto will be governed by and construed in accordance with the laws of Kenya, without regard to conflict of laws provisions.

b. No right or obligation under this Agreement (including the right to receive monies due) will be assigned without the prior written consent of Church World Service. Any assignment without such consent will be void. Church World Service may assign its rights under this Agreement.

c. All notices provided for herein will be in writing and will be delivered by hand or overnight courier service, email or fax in accordance with each party's contact information. Notices will be deemed to have been given when received, provided that notices sent by email or fax will be deemed received when sent (except that, if not sent during normal business hours for the recipient, will be deemed received at the opening of business on the next business day for the recipient).

d. Time is of the essence of each and every obligation of Supplier under this Agreement.

e. If any provision of this Agreement is prohibited by or invalid under applicable law, such provision will be ineffective only to the extent of such prohibition or invalidity without invalidating the remainder of such provision or any remaining provisions of this Agreement.

f. Except as otherwise provided above, this Agreement may be amended or modified only by a written document signed by both parties. This Agreement constitutes the entire contract between the parties relating to the subject matter hereof and supersedes any and all previous agreements and understandings, oral or written, relating to the subject matter hereof.

Signed:
(Being duly authorized official to sign on behalf of the Bidder)
Name: _____
Designation: _____
Organization: _____
Date: _____

Annex 5: Supplier Conflict of Interest Declaration Form

Section 1: Declaration of Conflict of Interest

I/We, the undersigned, declare that:

1. **Conflict of Interest**
    a. Neither the company nor its employees, agents, or representatives have any personal or financial interest that could improperly influence, or be perceived to influence, the procurement process with Church World Service.

2. **Relationships with CWS Staff**
    a. No employee, director, or representative of our company has a close family relationship (spouse, parent, child, sibling) or financial partnership with any CWS staff involved in procurement or contract administration.

1. **Gifts and Benefits**
    a. We have not offered, and will not offer, any gifts, favors, or benefits to CWS staff that could be construed as an attempt to influence procurement decisions.

2. **Disclosure Obligation**
    a. If any situation arises that may constitute a conflict of interest during the course of our engagement, we will immediately disclose it in writing to CWS.

Section 2: Supplier Confirmation

I/We certify that the information provided above is true and complete to the best of our knowledge.

Authorized Representative Name: _____

Title/Position: _____

Signature: _____

Date: _____

Company Name: _____

Annex 6: Non-Disclosure Agreement (NDA)

Our Ref; CWS/KE/NBO/001/FY27

Date: _____

Procurement Unit, CWS Africa

Dear Sir,

RE: CONFIDENTIALITY & NON-DISCLOSURE UNDERTAKING.

We refer to the above matter and to the tender for the provision of ..... services, reference number CWS/KE/NBO/001/FY27

We acknowledge that during the course of provision of ....., we shall have access to and be entrusted with confidential information. In this letter, Confidential Information shall mean all information or material that has or could have commercial value or other utility in the business or prospective business of Church World Service. Confidential Information also includes all information of which unauthorized disclosure could be detrimental to the interests of Church World Service, whether or not such information is identified as Confidential Information by Church World Service.

In consideration of you making Confidential Information available to us, we hereby irrevocably and unconditionally undertake to you:

1. That we shall hold in confidence any and all Confidential Information disclosed, and further agree not to disclose Confidential Information to third parties or to otherwise use Confidential Information, except with the express written consent from yourselves or as permitted under paragraph 3 below.
   That we shall use the Confidential Information solely for the provision of internet services and not for any other purpose.
2. That this undertaking shall not prohibit disclosure of Confidential Information;
   2.1. To our **Staff/Partners/Directors/Agents** who need to know such Confidential Information to assist with the Implementation. To this end, we shall endeavor to ensure that such **Staff/Partners/Directors/Agents** have been specifically informed of the confidentiality of the Confidential Information and have agreed to be bound by the terms of this undertaking or have entered into an agreement of similar scope and obligations with ourselves to protect our proprietary and/or the confidential information.
   2.2. To the extent that such disclosure is required to be disclosed pursuant to law, court order or any requirement by any regulatory authority. In this regard, we shall promptly give notice to yourselves and provide you with sufficient time to assert any exclusions or privileges that may be available by law.
3. That upon termination of the cooperation between the parties and/or at your request, we hereby agree and undertake to return to yourselves any written information and all materials which contain and/or constitute part of the Confidential Information, and not to keep any copy thereof.
4. That this undertaking shall not apply to Confidential Information which:
   4.1. Is in the public domain as of the effective date of this undertaking, or legitimately comes into the public domain through no fault of ours.
   4.2. Is demonstrated to have been known to us prior to the date of this undertaking and was not acquired, directly or indirectly, from yourselves or from a third party under a continuing obligation of confidentiality.
   4.3. Is demonstrated to have been rightfully received by us after disclosure under this undertaking from a third party who did not require the same to hold it in confidence or limit its use, and who did not acquire it, directly or indirectly, from yourselves under a continuing obligation of confidentiality.
   4.4. Is demonstrated to have been independently developed by our personnel who had no substantive knowledge of any information provided by yourselves.

5. That we acknowledge that the Confidential Information will not form a basis of any contract between ourselves and yourselves.
6. That we warrant that we are acting as Principal in this matter, and not as agent or broker for any person, company or firm.
7. That no failure or delay by you in exercising any right, power or privilege under this undertaking shall operate as a waiver thereof, nor shall single or partial exercise thereof or the exercise of any other right, power or privilege.
8. That by issuing this undertaking, we shall be deemed not only to have accepted and confirmed the foregoing undertaking, terms and conditions as set forth hereinabove but also to have acknowledged and confirmed that we are solely liable and responsible for full compliance with the said undertaking, terms and conditions.
9. That this Undertaking shall be governed and construed in accordance with the laws of Kenya and any dispute arising from it shall be subject to the jurisdiction of the Kenyan Courts.

Yours Faithfully,

Signed:
(Being duly authorized official to sign on behalf of the Bidder)

Name: _____

Designation: _____

Organization: _____

Date: _____

Annex 7: Technical Compliance Checklist;

1. **Network Infrastructure & Availability**

Requirements	Status	Comments
Minimum Service Level Agreement (SLA) uptime	Yes/No	
Direct peering with multiple upstream internet service providers	Yes/No	
Continuity and Redundancy Controls	Yes/No	
Secure configuration of network equipment	Yes/No	
Change Management Controls	Yes/No	
Power backup for customer premise equipment	Yes/No	
Monitoring, logging & alerting controls	Yes/No	
Incident Response Plan	Yes/No	
Confirm support for native, dual-stack IPv6 routing.	Yes/No	
Confirm ownership or delegation of static public IP blocks (IPv4/IPv6)	Yes/No	

2. **Security & Data Protection**

Requirements	Status	Comments
Supplier & Interconnection Controls	Yes/No	
Authorisation to operate as an internet service provider	Yes/No	
Compliance with existing standards (NIST/GDPR/local data privacy laws)	Yes/No	
Access Controls Policy	Yes/No	
Patch and Vulnerability Management Policy	Yes/No	
Verify active, upstream scrubbing capabilities.	Yes/No	
Verify compliance with Resource Public Key Infrastructure (RPKI) standards.	Yes/No	
Is the ISP DNS infrastructure secured against spoofing and cache poisoning.	Yes/No	

3. **Performance & Quality of Service**

Requirements	Status	Comments
Latency threshold	Yes/No	
Jitter threshold	Yes/No	
Packet loss threshold	Yes/No	

4. **Support & Maintenance**

Requirements	Status	Comments
24/7/365 Network Operations Centre support	Yes/No	
Mean Time to Repair (MTTR)	Yes/No	
Real-time bandwidth utilization and monitoring	Yes/No	

Annex 8; Cybersecurity Questionnaire

This questionnaire is designed to evaluate the cybersecurity posture of our internet service providers. Please answer each question honestly to assist us in ensuring third-party risk management and operational security.

1. **Governance & Management**
   1.1. Do you have a formal Information Security , privacy or acceptable use policy approved by management?

   1.2. Is there a designated individual responsible for information security (e.g., CISO)?

2. **Network Security**
   2.1. Do you perform regular vulnerability assessments or penetration testing on your public-facing infrastructure?

   2.2. How are your management interfaces secured against unauthorized access?

3. **Incident Response**
   3.1. Do you maintain a documented Incident Response Plan?

   3.2. How are clients notified in the event of a significant service outage or data breach?

4. **Physical, Logical & Infrastructure Security**
   4.1. What physical access controls are implemented at your critical data centres/POP sites?

   4.2. EDR/XDR on servers and workstations; anti-malware; secure configuration and perimeter.?

   4.3. Do you have redundant power and networking paths to ensure service continuity?

5. **Compliance & Auditing**
   5.1. Have you implemented any recognized frameworks (e.g., ISO 27001, SOC 2, NIST)?

   5.2. Are you audited against any recognized frameworks (e.g., ISO 27001, SOC 2, NIST)?

   5.3. Do you conduct annual security assessments or penetration testing of your core network?

Annex 9: Policy Acknowledgment and Compliance Declaration

We, _____ hereby acknowledge that we have received, reviewed, and understood the following CWS policies:

- Child Safeguarding Policy
- Protection from Sexual Exploitation, Abuse and Harassment (PSEAH) Policy
- Anti-Human Trafficking Policy

We confirm that our organization, employees, subcontractors, and representatives will comply with the requirements and standards contained in these policies throughout the duration of any contract awarded by CWS.

Company Name: _____

Authorized Representative: _____

Position: _____

Signature: _____

Date: _____

Annex 9:Price Offer Sheet

Price Offer Sheet

Item Description	Quantity	Unit of	Unit Price	Total Price
400 Mbps Primary Link CWS offices located at West End Towers, Westlands, Nairobi	1	Service		
400 Mbps Secondary Link CWS offices located at West End Towers, Westlands, Nairobi	1	Service		
30 Mbps Primary Link, CWS Office Minjila Office (Tana River County, Kenya) – YWCA office	1	Service		
30 Mbps Primary Link CWS office Ngurunit Field Office (Marsabit County, Kenya) – Kukar Joshua Residence	1	Service		
Total before tax:				
VAT (if applicable)				
Total:				

Company Name:	
Name of Representative:	
Title:	
Signature:	
Date:	

Tender #:	