

| TECHNICAL SPECIFICATION – High Availability Internet Connection – Secondary Link for Department of Survey   |  |  |                       |         |
|---|--|--|-----------------------|---------|
| Date:   | 4/3/2026   |  |                       |         |
| Project:  | Secondary Internet Connection for Data Centre High Availability  |  |                       |         |
| Current Provider:   | Sri Lanka Telecom – 50 Megabits per second symmetric fiber       |  |                       |         |
| Target:   | New Provider – 10 Megabits per second symmetric (Active/Passive) |  |                       |         |
| 1. Introduction   |  |  |                       |         |
| This Technical Specification defines the mandatory requirements for a secondary dedicated internet connection to operate in parallel with the existing Sri Lanka Telecom fiber line, creating a High Availability Active/Passive cluster with Zero Single Point of Failure.   |  |  |                       |         |
| Bandwidth Rationale: The secondary connection is idle under normal conditions and only activates during Sri Lanka Telecom outages. 10 Megabits per second symmetric is sufficient to sustain critical data centre operations for the duration of any failure (maximum Mean Time To Repair of 4 hours). This provides a cost-effective High Availability solution while maintaining essential services during outages. |  |  |                       |         |
| 2. Key Technical Definitions  |  |  |                       |         |
| 2.1   | Term   | Definition   | Compliance<br>Yes/ No | Remarks |
| 2.2   | Symmetric  | Upload and download bandwidth are equal. For this requirement, 10 Megabits per second symmetric means 10 Megabits per second upload and 10 Megabits per second download simultaneously.  |                       |         |
| 2.3   | Active/Passive   | Primary link (Sri Lanka Telecom) handles all traffic under normal conditions. Secondary link remains idle but automatically activates upon primary link failure.   |                       |         |
| 2.4   | Committed Information Rate                                       | Guaranteed minimum bandwidth at all times. No contention or sharing with other users.  |                       |         |
| 2.5   | Border Gateway Protocol  | Dynamic routing protocol that enables automatic failover between multiple internet connections.  |                       |         |
| 2.6   | Bidirectional Forwarding Detection                               | Protocol that detects link failures rapidly. With mutually agreed timers, can achieve sub-second detection.  |                       |         |
| 2.7   | Zero Single Point of Failure                                     | No single component, cable, or facility whose failure can cause complete loss of internet connectivity.  |                       |         |
| 3. Technical Requirements   |  |  |                       |         |
| No  | Parameter  | Requirement  |                       |         |
| 3.1   | Service Type   | Dedicated Internet Access, uncontended, 1:1 Committed Information Rate   |                       |         |
| 3.2   | Bandwidth  | 10 Megabits per second symmetric (10 Megabits per second upload / 10 Megabits per second download)   |                       |         |
| 3.3   | Redundancy Model   | Active/Passive with automatic failover (Primary: Sri Lanka Telecom, Secondary: New Provider)   |                       |         |
| 3.4   | Failover Time  | Support for Bidirectional Forwarding Detection with minimum detection time ≤1 second, subject to mutually agreed timer configuration between provider and data centre.   |                       |         |
| 3.5   | Physical Diversity (Last-Mile)                                   | The secondary link must utilize physically diverse building entry points (e.g., North vs. South) and separate lead-in conduits. Geographic Information System maps must demonstrate that the fiber path does not share a common trench or manhole with Sri Lanka Telecom for at least the first 2 kilometers from the premises. No single physical cut shall cause simultaneous failure of both links. Any shared infrastructure beyond this point must be disclosed in writing. |                       |         |
| 3.6   | International Diversity  | The bidder must demonstrate Upstream Path Diversity. While physical subsea cable overlap may exist in national gateways, the bidder must prove they utilize different Upstream Tier-1 Transit Providers (e.g., Tata, NTT, Cogent, Level 3) and a different Autonomous System path than Sri Lanka Telecom to ensure logical resiliency. Network diagram showing minimum 2 independent upstream transit providers and their Autonomous System Numbers must be provided.            |                       |         |
| 3.7   | Last-Mile Technology   | Fiber (different core or carrier from Sri Lanka Telecom) OR Licensed Wireless (only if fiber diversity proven impossible with documented evidence)   |                       |         |
| 3.8   | Routing Protocol   | Border Gateway Protocol version 4 support with our edge router. Must support Bidirectional Forwarding Detection for rapid convergence. Must not filter return path based on source Autonomous System Number. Must support static default route in addition to Border Gateway Protocol for emergency fallback configuration.  |                       |         |
| 3.9   | IP Addressing  | Option A (Preferred): Provider Independent space advertised with Data Centre's own Autonomous System Number. No Internet Protocol renumbering required ever.<br><br>Option B (Fallback): Provider Assigned space with Border Gateway Protocol conditional advertisement and documented Internet Protocol transition plan in case of provider failure.  |                       |         |
| 3.10  | Throughput   | 10 Megabits per second symmetric, 1:1 Committed Information Rate. No traffic shaping below Committed Information Rate. No microburst policing. Maximum Transmission Unit 1500 bytes mandatory. Support for 9000 byte jumbo frames is preferred but not mandatory.  |                       |         |

| 2.1  | Term                                     | Definition   | Compliance<br>Yes/ No | Remarks |
|--|--|--|-----------------------|---------|
| 3.11   | Latency                                  | Measurement Clause: Average round-trip latency measured monthly at provider edge under normal network load. Burst exceptions due to network events shall be excluded from penalty calculations.  |                       |         |
| 3.12   | Failure Trigger                          | Performance-based (brownout) detection supported. Must not block Bidirectional Forwarding Detection, Internet Protocol Service Level Agreements, or active health probes from Data Centre edge equipment.  |                       |         |
| 3.13   | Power Resilience                         | Customer Premises Equipment must support dual power input OR external redundant power adapter with Uninterruptible Power Supply support. Equipment must be carrier-grade, suitable for 24x7 continuous operation, with minimum 5-year OEM support lifecycle.   |                       |         |
| 3.14   | Service Level Agreement Uptime           | Mandatory Minimum: 99.9 percent aggregate availability, measured at Customer Premises Equipment Ethernet handoff interface. Financial penalties for downtime.<br><br>Preferred Target: 99.99 percent aggregate availability (downtime less than 4.3 minutes per month). Bidders offering 99.99 percent will receive higher technical scoring |                       |         |
| 3.15   | Mean Time To Repair                      | Critical Fault (total link down): 4 hours from ticket creation. Degraded Fault (high latency or packet loss): 8 hours from ticket creation.  |                       |         |
| 3.16   | Monitoring Interface                     | Simple Network Management Protocol version 2c or 3 OR Read-Only Application Programming Interface providing at minimum: interface utilization, optical power levels, Border Gateway Protocol session state, Cyclic Redundancy Check errors.  |                       |         |
| 3.17   | Distributed Denial of Service Mitigation | Support for Border Gateway Protocol blackhole community or Remotely Triggered Black Hole capability. Community string documentation must be provided.  |                       |         |
| 3.18   | Customer Premises Equipment Hardware     | Make and model specified in bid. Must be new, factory-sealed, and supported for minimum 5 years. All required Small Form-factor Pluggable modules and accessories included.  |                       |         |
| 3.19   | Emergency Fallback Configuration         | Provider must support static default route configuration in addition to Border Gateway Protocol to allow emergency fallback during Border Gateway Protocol misconfiguration events.  |                       |         |
| <b>4. Bidder Declaration for Technical Specification</b>   |  |  |                       |         |
| I, the undersigned, confirm that the information provided in this Technical Specification document is true and accurate. I understand that any misrepresentation may lead to immediate disqualification or contract termination. |  |  |                       |         |
| Bidder Name:   |  |  |                       |         |
| Authorized Signatory:  |  |  |                       |         |
| Signature:   |  |  |                       |         |
| Date:  |  |  |                       |         |
| Company Seal:  |  |  |                       |         |

**Bidder's Signature :**

**Company Name & Seal :**