



higher education
& training
Department:
Higher Education and Training
REPUBLIC OF SOUTH AFRICA

Ehlanzeni TVET College Corporate Centre


29 Bell Street, NELSPRUIT.
Private Bag X11297 NELSPRUIT 1200
Tel: 013-752-7105/5817/7527/5070/4752 Fax: 013-752-4902



To: SUPPLY CHAIN UNIT
From: SPECIFICATION COMMITTEE
SUBJECT: Specification for Internet Backup Line

ITEM NUMBER	COMPLETE PRODUCT DESCRIPTION/SPECIFICATION/SCOPE OF WORK	PRODUCT QUANTITY																				
1.	<div>1. Technical Specifications</div> <div>A. Core Requirements</div> <table><tr><th>Parameter</th><th>Specification</th></tr><tr><td>Technology</td><td>Dedicated fibre-optic connection is required as the primary medium. Wireless or LTE may only be used as a temporary backup during outages or in areas where fibre is not immediately available.</td></tr><tr><td>Bandwidth</td><td>Minimum of 200 Mbps symmetrical bandwidth (upload and download), with capability to scale up to 500 Mbps as needed.</td></tr><tr><td>Uptime SLA</td><td>Guaranteed minimum uptime of 99.95% per month, excluding periods of scheduled and approved maintenance.</td></tr><tr><td>Failover Time</td><td>Automatic failover to the backup link must occur within 2 minutes of primary link failure detection.</td></tr><tr><td>Latency / Jitter</td><td>End-to-end network latency must be ≤ 30 milliseconds, with jitter not exceeding 5 milliseconds under normal operating conditions.</td></tr></table> <div>B. Monitoring & Management</div> <table><tr><th>Requirement</th><th>Specification</th></tr><tr><td>Non-Disruptive Installation</td><td><div>- Service provider must ensure a seamless deployment with no interruption to existing services.</div><div>- All implementation work must be carried out during off-peak hours (between 19:00–05:00 or on weekends) unless otherwise approved in writing by the college’s IT department.</div><div>- A detailed Risk Mitigation Plan must be submitted, outlining rollback steps and including evidence of past implementations conducted without client service disruption.</div></td></tr><tr><td>Monitoring Tools</td><td><div>- A real-time monitoring platform must be provided, displaying live statistics including uptime, latency, packet loss, and bandwidth usage.</div><div>- The tool must support configurable alerts via SMS and/or email for threshold breaches.</div></td></tr><tr><td>Change Management</td><td><div>- All planned maintenance or infrastructure changes must be communicated at least 72 hours in advance.</div><div>- Written approval from the College IT department is required for all changes that may impact service availability.</div></td></tr></table> <div>C. Security Requirements</div>	Parameter	Specification	Technology	Dedicated fibre-optic connection is required as the primary medium. Wireless or LTE may only be used as a temporary backup during outages or in areas where fibre is not immediately available.	Bandwidth	Minimum of 200 Mbps symmetrical bandwidth (upload and download), with capability to scale up to 500 Mbps as needed.	Uptime SLA	Guaranteed minimum uptime of 99.95% per month, excluding periods of scheduled and approved maintenance.	Failover Time	Automatic failover to the backup link must occur within 2 minutes of primary link failure detection.	Latency / Jitter	End-to-end network latency must be ≤ 30 milliseconds, with jitter not exceeding 5 milliseconds under normal operating conditions.	Requirement	Specification	Non-Disruptive Installation	<div>- Service provider must ensure a seamless deployment with no interruption to existing services.</div> <div>- All implementation work must be carried out during off-peak hours (between 19:00–05:00 or on weekends) unless otherwise approved in writing by the college’s IT department.</div> <div>- A detailed Risk Mitigation Plan must be submitted, outlining rollback steps and including evidence of past implementations conducted without client service disruption.</div>	Monitoring Tools	<div>- A real-time monitoring platform must be provided, displaying live statistics including uptime, latency, packet loss, and bandwidth usage.</div> <div>- The tool must support configurable alerts via SMS and/or email for threshold breaches.</div>	Change Management	<div>- All planned maintenance or infrastructure changes must be communicated at least 72 hours in advance.</div> <div>- Written approval from the College IT department is required for all changes that may impact service availability.</div>	Must be installed in all 8 Sites
Parameter	Specification																					
Technology	Dedicated fibre-optic connection is required as the primary medium. Wireless or LTE may only be used as a temporary backup during outages or in areas where fibre is not immediately available.																					
Bandwidth	Minimum of 200 Mbps symmetrical bandwidth (upload and download), with capability to scale up to 500 Mbps as needed.																					
Uptime SLA	Guaranteed minimum uptime of 99.95% per month, excluding periods of scheduled and approved maintenance.																					
Failover Time	Automatic failover to the backup link must occur within 2 minutes of primary link failure detection.																					
Latency / Jitter	End-to-end network latency must be ≤ 30 milliseconds, with jitter not exceeding 5 milliseconds under normal operating conditions.																					
Requirement	Specification																					
Non-Disruptive Installation	<div>- Service provider must ensure a seamless deployment with no interruption to existing services.</div> <div>- All implementation work must be carried out during off-peak hours (between 19:00–05:00 or on weekends) unless otherwise approved in writing by the college’s IT department.</div> <div>- A detailed Risk Mitigation Plan must be submitted, outlining rollback steps and including evidence of past implementations conducted without client service disruption.</div>																					
Monitoring Tools	<div>- A real-time monitoring platform must be provided, displaying live statistics including uptime, latency, packet loss, and bandwidth usage.</div> <div>- The tool must support configurable alerts via SMS and/or email for threshold breaches.</div>																					
Change Management	<div>- All planned maintenance or infrastructure changes must be communicated at least 72 hours in advance.</div> <div>- Written approval from the College IT department is required for all changes that may impact service availability.</div>																					

	Component	Specification	
	Managed Firewall	The solution must include a managed firewall with the following capabilities: - Intrusion Detection and Prevention Systems (IDS/IPS). - DDoS protection with minimum 10 Gbps mitigation capacity. - Monthly vulnerability assessments and reporting.	
	Data Sovereignty	All routing and processing of internet traffic must remain within the territorial boundaries of South Africa. No traffic is to transit through foreign countries at any stage.	
			Standard Industry Rate


 Mr EM Mbuyane
 Principal

09/06/202