

TECHNICAL CORRIGENDUM – 1
COLLABORATION SETUP OF SHARED WORK SPACE AT BN-9 IT PARK, SALT LAKE

03-07-2020

Tender No: WEBEL/EOT/COM/20-21/00010 Dated: 19-06-2020

Page No.	Existing Content	To be read as
12	BOQ Sl. No. 14: LC-LC FIBRE PATCH CORD PATCH CORD	1G Duplex Multimode 50/125 OM2 LSZH Fiber Patch Cable, LC-LC type - 3 MTR
33	Under CAT 6 UTP Cable	<i>To Include:</i> CAT6 Cable shall comply to the requirements of IEEE 802.3bt (Type 4) for 4 pair-PoE
36	Under L 2 Switch 48 Port: Number of VLAN Supported: 64 (Minimum).	Number of VLAN Supported: 1500 (Minimum).
36	Under L 2 Switch 48 Port: 512MB DRAM and 256MB Flash RAM (Minimum)	1GB DRAM and 1GB Flash RAM (Minimum).Should have minimum packet buffer 10MB
37	Under L 2 Switch 24 Port: Number of VLAN Supported: 64 (Minimum).	Number of VLAN Supported: 1500 (Minimum).
37	Under L 2 Switch 24 Port: 512MB DRAM and 256MB Flash RAM (Minimum)	1GB DRAM and 1GB Flash RAM (Minimum).Should have minimum packet buffer 10MB
44	Under Heavy Duty Multifunction Printer Specification	<i>To include:</i> Print Speed should be 35 PPM (A4) Mono & Colour or above.
47	Under 3 KVA UPS System: Intermediate DC Circuit Parameters Battery Charging max : 13A Output power factor : Unity Output voltage precision : +/- 3%	Battery Charging max : 6A Output power factor : 0.8 Output voltage precision : +/-1%

TECHNICAL CORRIGENDUM – 1
COLLABORATION SETUP OF SHARED WORK SPACE AT BN-9 IT PARK, SALT LAKE

03-07-2020

Tender No: WEBEL/EOT/COM/20-21/00010 Dated: 19-06-2020

47	Under 3 KVA UPS System: Output Parameters Output power factor : Unity Output voltage precision : +/- 3% Output voltage distortion for <2% for 100% Linear Load < 5% for 100% Non Linear Load	Output power factor : 0.8 Output voltage precision : +/-1% Output voltage distortion for <3% for 100% Linear Load < 5% for 100% Non Linear Load
42	Under Centralized network policy enforcement AAA Specification	To Include: A) Device Profiling and Visibility 1) Provide automatic detection and categorization of endpoints for security and audit demands, regardless of device type, using contextual data and use this data for optimizing access policies 2) Stored profiling data should identify device profile changes and dynamically modify authorization privileges. For example, if a printer appears as a Windows laptop, the system can automatically deny access. 3) Support passive device profiling methods such as DHCP, Span Ports, HTTP User-Agent, MAC OUI and TCP SYN-ACK handshakes 4) Support active device profiling methods such as SNMP, Subnet Scan, SSH, WMI and NMAP Scan 5) Offer a comprehensive dashboard to see the total number of endpoints, and the number by category, family and device type. B) Authentication, Authorization and Accounting (AAA) 1) Integrated scalable AAA services (authentication, authorization, and accounting) including access policy management with a complete understanding of context, such as user's role, device type, location, time of day etc. 2) User and device authentication based on 802.1X, non-802.1X, and Web Portal access methods across multi-vendor wired networks, wireless networks, and VPNs

TECHNICAL CORRIGENDUM – 1
COLLABORATION SETUP OF SHARED WORK SPACE AT BN-9 IT PARK, SALT LAKE

03-07-2020

Tender No: WEBEL/EOT/COM/20-21/00010 Dated: 19-06-2020

	<p>3) Usage of multiple authentication protocols concurrently, such as PEAP, EAP-FAST, EAP-TLS, EAP-TTLS, and EAP-PEAP-Public</p> <p>4) Fine-grained control using attributes from multiple identity stores, such as Microsoft Active Directory, Kerberos, LDAP- compliant directory, Open Database Connectivity (ODBC)- compliant SQL database, token servers, and internal databases across domains within a single policy</p> <p>5) Non-802.1X devices (such as printers, IP phones, IP cameras and IOT devices) can be identified as known, based on the presence of their MAC addresses in database, or unknown upon connecting to the network.</p> <p>6) Integrated TACACS+ server for secure authentication of device administrators, operators etc. with varied privilege levels. It should keep a track of the changes made by the logged-in user. NAC solution shall have inbuilt TACACS+ Server capability to support Device administrator secure authentication, privilege-based access and audit logging</p> <p>7) Customizable Reporting with manual or scheduled reports in PDF/CSV/HTML formats, inventory dashboard showing details of learned devices, real-time monitoring of access requests and events, proactive alerts through Email/SMS</p> <p>8) API Integration with helpdesk software allowing dynamic creation of problem tickets of any network triggered policy breaches</p> <p>9) Inbuilt utilities for interactive policy simulation and monitor mode for assessing the policies before applying to the production network</p> <p>10) Solution should support Inbuilt utilities for interactive policy simulation and monitor-only mode for assessing the policies before applying to the production network</p> <p>11) The NAC solution shall detect Virtual Machines running on the PC</p> <p>C) Guest Access Management</p> <p>1) Easy-to-use guest management solution for visitors, contractors, partners, etc. on wireless and wired networks using any type of device.</p>
--	---

TECHNICAL CORRIGENDUM – 1
COLLABORATION SETUP OF SHARED WORK SPACE AT BN-9 IT PARK, SALT LAKE

03-07-2020

Tender No: WEBEL/EOT/COM/20-21/00010 Dated: 19-06-2020

		<p>2) Guest access through captive portal with extensive branding and customization including company logos, visual imagery and optional advertisements with multimedia content to extend organization's messaging</p> <p>3) Captive portal should have mobile device awareness to automatically size for smart phones, tablets and laptops</p> <p>4) Guest self-registration through the web portal, delivering username and password directly to the visitor's Web browser, or sent via email or SMS.</p> <p>5) Customize guest access privileges to enforce bandwidth limits, access to specific resources, length of connections and set automatic account expiry after a specified number of hours or days</p> <p>6) Guest portal with Sponsor based authentication, OTP-based authentication (SMS and SMTP gateway integration) and social-login authentication</p> <p>D) Requirement Summary</p> <p>1) Hardware appliance.Should support multiple redundant mode(1+1/clustering)</p> <p>2) Licenses supporting minimum 300 concurrent sessions for AAA/Guest access /TACACS+ on Day 1. Upgradeable to 1000 concurrent sessions with the same hardware.</p> <p>E) OEM and Product Eligibility/Compliance</p> <p>1) The solution shall be Common Criteria certified for network access control (NAC) solution, under both the Network Device collaborative Protection Profile (NDcPP) and the Extended Package for Authentication Servers modules. The certificate shall be attached as reference. The NAC vendor shall be a leader or challenger in the last Gartner Magic Quadrant for NAC released in 2014</p>
--	--	--

THE ABOVE CORRIGENDUM IS A PART OF ORIGINAL TENDER DOCUMENT