CORRIGENDUM-1

NIT No. – EdCIL/DES/SCU/ICT/2025/01

Date: 05-03-2025

Name:

"Design, Supply, Installation, Testing, Commissioning of Equipment, Implementation and Maintenance of Smart Campus ICT Solution for SCU, Ladakh"

The following corrigendum is made to the above tender.

S. No.	Chapter No.	Page No.	Description as per Tender Document	Modified Description
1	ANNEXURE-XVI (Technical Specification For All in One Workstation)	135	Viewing Size not less than 27" diagonal with Minimum Resolution of 1920 x 1080 or better. Panel Type: Antiglare, IPS with stand.	Viewing Size not less than 23.8" diagonal with Minimum Resolution of 1920 x 1080 or better. Panel Type: Antiglare, IPS with stand.
2	ANNEXURE-XVI (Technical Specification For All in One Workstation)	135	13th Generation Processor with minimum 30 MB cache , 2.1 GHz or higher frequency .	13th Generation or higher Processor with minimum 30 MB cache , 2.1 GHz or higher frequency
3	ANNEXURE-XVI (Technical Specification For All in One Workstation)	135	Integrated USB Port: (Minimum 2 USB Type C port. and Minimum 2 USB type A port.1 dual mode display port and RJ 45 port	Integrated USB Port: (Minimum 1 USB Type C port. and Minimum 2 USB type A port.1 dual mode display port and RJ 45 port
4	ANNEXURE-XVI (Technical Specification For All in One Workstation)	135	Minimum 160 Watt or higher (Internal Power supply) upto 92% efficiency.	Minimum 160 Watt or higher (Internal Power supply) with minimum 85% efficiency.
5	General		General	Broad layout plan attached. Rest, please do proper site survey before quoting for this tender.
6	General		BOQ line item no 25 and 29	BOQ line item 25 is omitted
7	Annexure XVI	81	Each switch should also be capable to deliver additional up to 4x10/25G uplinks for	Overall core swtich soln. should be capable to deliver min. 2x10/25G uplinks for expansion or servers connectivity per switch"

			expansion or servers connectivity.	
8	ANNEXURE-XVI	81	Switch should have at least 296Gbps switching fabric performance and 214Mpps forwarding rate or better	Switch should have at least 196Gbps switching fabric performance and 150Mpps forwarding rate or better
9	ANNEXURE-XVI	82	Should support IEEE 802.1Q VLAN, 802.1p priority queues, IEEE 802.1ad, IEEE 802.1ag, 802.1ae.	Should support IEEE 802.1Q VLAN, 802.1p priority queues, IEEE 802.1ad, 802.1ae."
10	ANNEXURE-XVI	83	Access Point must support dual-band / tri-band radio with minimum 2x2 & Two spatial streams (MIMO) at all radio.	Access Point must support dual-band / tri-band radio with minimum 2x2 or higher & Two or more spatial streams (MIMO) at all radio.
11	ANNEXURE-XVI	83	Must support minimum 2x2 with two spatial streams (MIMO)	Must support minimum 2x2 or higher with two or more spatial streams (MIMO)
12	ANNEXURE-XVI	83	Access Point should support minimum 573 Mbps on 2.4GHz, 1200 Mbps on 5GHz and 2400 Mbps on 6GHz.	Access Point should support minimum 573 Mbps on 2.4GHz, 1200 Mbps on 5GHz.
13	ANNEXURE-XVI	118	The proposed NGFW appliance vendor should have security effectiveness minimum 97.4% or Block Rate minimum 97.9% in 2019 SVM NGFW report of NSS Labs. Also, OEM should feature in the top quadrant of the Security Value Map (SVM) of NSS Labs report 2019 for Next Generation Firewall (NGFW)	The proposed NGFW appliance vendor should have demonstrated high security effectiveness and threat protection in independent third-party testing such as NSS Labs (prior to 2020), MITRE ATT&CK evaluations, or ICSA Labs. The NGFW should provide advanced threat protection, deep packet inspection, and integration with leading security intelligence platforms
14	Firewall Point-26	120	The proposed firewall shall be able to create custom application signatures and categories using the inline packet capture feature of the firewall without any third-party tool or technical support.	The Proposed Firewall shall be able to create custom application signatiure and using inline packet capture feature we can capture logs without any third party tool or technical support
15	Firewall Point-32	121	Solution should have machine learning capabilities on the dataplane to analyze web page content to determine if it contains malicious JavaScript or is being	The firewall shall have machine learning capabilities to analyze web page content and determine if it contains malicious JavaScript or is being used for credential phishing. The firewall shall use inline machine

			used for credential phishing. Inline ML should prevent web page threats from infiltrating network by providing real-time analysis capabilities.	learning to prevent web-based threats from infiltrating the network by providing real-time analysis capabilities."
16	Firewall Point-47	122	Should have threat prevention capabilities to easily import IPS signatures from the most common definition languages Snort and Suricata	Firewall Have threat prevention capabilities where it can import or create Custom signature.
17	Firewall Point-61	124	The proposed firewall should protect against evasive techniques such as cloaking, fake CAPTCHAs, and HTML character encoding based attacks	The proposed firewall should protect against evasive techniques
18	Firewall Point-62	124	The proposed Firewall should offer advanced URL filtering capabilities including Inline Real-Time Web Threat Prevention, Anti-Evasion Measures, Multicategory Support, Real-Time Credential Theft Protection, Phishing Image Detection, Criteria Matching, Translation Site Filtering.	The proposed Firewall should offer advanced URL filtering capabilities including Inline Real-Time Web Threat Prevention, Anti-Evasion Measures, Credential theft Protection
19	Firewall Point-63	124	The solution should protect against never-before- seen phishing and JavaScript attacks inline. Solution should be capable to use both signature based and ML based signature less technology	The solution should protect unknown malicious attack. Solution should be capable to use both signature based and ML based signature less technology
20	Firewall Point-64	124	The proposed firewall should have URL or URL category base protection for user cooperate credential submission protection from phishing attack with malicious URL path	The proposed firewall should have URL or URL category base protection for user from phishing attack with malicious URL path
21	Firewall Point-65	124	The NGFW should prevent credential theft attacks by preventing users from submitting credentials to phishing sites.	The NGFW should prevent credential theft attacks to phishing sites.
22	Firewall Point-66	124	The NGFW should prevent this kind of credential theft attack (without the need of endpoint agents). Vendors should provide	The firewall shall be capable of preventing credential theft attacks without the need for endpoint agents. It shall provide features that

			features with the ability to prevent the theft and abuse of stolen credentials, one of the most common methods cyber adversaries use to successfully compromise and maneuver within an organization to steal valuable assets. It should also complement additional malware and threat 1prevention and secure application enablement functionality, to extend customer organization's' ability to prevent cyber breaches. 1.) Automatically identify and block phishing sites 2.) Prevent users from submitting credentials to phishing sites 3.) Prevent the use of stolen credentials	protect against the theft and abuse of stolen credentials. Specifically, the firewall shall have the capability to: Automatically identify and block phishing sites. Prevent users from submitting credentials to phishing sites. Prevent the use of stolen credentials
23	Firewall Point-85	126	Should support DNS sinkholing for malicious DNS request from inside hosts to outside bad domains and should be able to integrate and query third party external threat intelligence databases to block or sinkhole bad IP address, Domain and URLs	Should support DNS protection from malicious DNS request from inside hosts to outside bad domains and should be able to integrate and query third party external threat intelligence databases to block DNS attack
24	Notice Inviting Tender	5	Last and Date Time for receipt of Bids- 10.03.2025 up to 12:30 Hrs	Last and Date Time for receipt of Bids- 17.03.2025 up to 12:30 Hrs
25	Notice Inviting Tender	5	Date and Time of Opening of Technical Bids- 10.03.2025 up to 15:30 Hrs	Date and Time of Opening of Technical Bids- 17.03.2025 up to 15:30 Hrs

Sd/-

Chief General Manager (DES)

EdCIL (India) Limited