Expression of Interest (EOI)
For
Wi-Fi and Networking Infrastructure in Delhi Technological University, DTU

1. Background

Delhi Technological University (formerly Delhi College of Engineering) is a non-affiliating; teaching cum research University engaged in education, research, product innovation and extension work in Applied Sciences, Engineering and Management, and is committed to foster excellence.

DTU established Wi-Fi network in its campus between 2011–2015, built on a 48-core optical fiber backbone connecting academic, administrative, and residential blocks. Over time, the network infrastructure has aged considerably — most devices are obsolete, out of warranty, and beyond support. Several areas presently have poor or no network connectivity.

DTU's rapid expansion in infrastructure and student strength demands a comprehensive refresh of the campus network to create a secure, scalable, and centrally managed Wi-Fi-enabled digital environment.

2. Objective of the EOI

The University seeks Expressions of Interest (EOI) from qualified and experienced public sector units having proven expertise in large-scale campus networking and Wi-Fi deployment right from design to supply, install, and commissioning a Next Generation Network Infrastructure. The set of objectives for assignment is to: -

- Establish a secure wired and wireless (Wi-Fi 6/6E or higher) network with complete campus coverage.
- Create a single-cluster, centrally managed LAN and WAN with high redundancy and scalability.
- Build a future-ready 40G backbone scalable to 100G, with 10G distribution and mGig wireless access.
- Ensure data security, network analytics, and threat protection through integrated cybersecurity solutions.
- Enable smart campus applications including hybrid teaching, digital learning, IoT readiness, and real-time monitoring.

3. Scope of Work

The broad scope of work includes (but is not limited to):

- Active Network Components – Core, Distribution, and Access Switches; Next Gen Firewall; Secure VPN; NAC; DNS Security; Wireless Controller; Access Points (Indoor & Outdoor); NMS; and Cybersecurity Suite.
- Passive Infrastructure – Fibre backbone extension, cabling, racks, and accessories.
- Implementation Services – Installation, commissioning, testing, and system integration.
- Network Management & Support – Centralized NMS, monitoring dashboards, and performance analytics.
- Operations & Maintenance Support – Provision of on-site resident engineers for 5 years post-installation.
- Training & Documentation – Training of DTU IT staff and preparation of technical and operational manuals.

4. Technical Highlights

To design a smart campus, DTU has defined a common understanding and vision –

Below are the capabilities envisaged to be incorporated into the Smart Campus Design: –

A. Connect the Campus

- Building a secure wired and wireless network that provides faster data transfers across the entire University for providing seamless access to the resources.
- Improve operational efficiency and reduce costs through automation.
- Reduce network complexities, increase redundancies, making a flexible and easy-to-manage network.
- Adapt the campus to allow faculties to deliver continuous learning both on-site and online.
- Create a hybrid learning environment that Increases students' access to learning through online resources & content from anywhere on the campus.

B. Facilitate Safety and Security

- Securing the network, and endpoints and providing secure web access.
- Create a safe and secure learning environment by blocking cyber-attacks.
- Protect Data, Research, and Intellectual Property by enforcing user identity-based access controls.
- Prevent unauthorized accessand enhance security through two-factor authentication (2FA).

With the vision of setting up a Smart Campus - DTU is planning to have its Campus upgraded and built with State-of-the-Art Network using 40G network backbone scalable to 100G in the future, 10G Distribution – Access network, and mGig for its wireless to get line rate performance across. The backbone shall have the capability to be upscaled between Core & Distribution in the future to meet the scalability without changing the underlying hardware.

It has been envisaged to have a 3-Tier Architecture for the network –

Network Parameters

On the active network side, it is required to have a Core, Distribution, Access Switches, Next Gen Firewall, Secure VPN access, Malware protection and threat intelligence, NAC, DNS Security Wireless Controller, Wireless Access Points for Indoor & Outdoor coverage, and NMS to manage the network infrastructure.

The network is required to be designed and proposed keeping the following parameters in view: –

I. **Scalability**

II. **High availability**

III. **Manageability**

IV. **Data Security**

V. **Performance**

I. Scalability

The network will be based on open standards, Open APIs, and data models, will be scalable, and will support the addition of no. of users on the Internet, as well as

Intranet. The equipment suggested is required to have provision to accommodate more ports and modules in the solution without degrading the performance. The network equipment will be selected to take care of the future needs also.

II. High Availability

The success of a network-based application heavily depends on the availability of the network. Hence network availability must be very high. Network availability relies upon many metrics including the amount of redundancy built within the network hardware device. The redundant links are to be provided till the access layer meets the desired SLA and uptime.

III. Manageability

A centralized Network Management System is required - that employs a variety of tools, applications, and devices to assist network managers in monitoring and managing the various network components including wired and wireless. Proactive level of monitoring & troubleshooting, customized reports to help in handling the user problems and monitoring the service levels respectively. The solution is to have remote troubleshooting support from anywhere to ease out the manageability. These are Easy to manage from anywhere, use automation, plug and play features to be provided from day one.

IV. Data Security

The network will be secured for data transmission. This is the most important piece within the network. To maximize security, an integrated system that includes multiple layers of logical security technology will be proposed to best ensure that the systems and services are protected. This will include access controls/segmentations / micro-segmentations at several layers. This will also include differentiated access to users based on their roles and profiles within the network with secure access.

V. Performance

All the equipment will have high performance and will cater to future needs also. When more sites/blocks/users or applications are added to the network, the response time will not be affected. To maintain the required response time, the aggregating equipment like Core, and Distribution will have high processing capabilities. The

proposed network architecture is required to be designed with having Multi-Tiered Architecture approach.

C. Proposed Solution

The campus network architecture should be based on converged IP technology from the Core Switch to the Access network. All proposed hardware like - Core Switches, Distribution Switches, WLC, Next Generation Firewalls, NAC, etc., and core backbone till the access layer is required to be designed in High Availability mode.

(i) Campus Network Solution:

- Build the Campus Network to an Intelligent high-bandwidth backbone over 40G using Campus Fabric Technology and Distribution-access on 10G connectivity while building up the entire topology on Star having redundant paths providing active-active communication.

  (Setting up 3 Tier Architecture - with Redundant Cores, redundant backbone, and redundant Distribution.) Access Switches to have redundant uplinks with Distributions.

- Setting up of wireless infrastructure in the complete campus on the latest generation high-speed network on 802.11ax WiFi6 technology and to provide coverage across the campus.
- The wireless network is to be connected to the mGig PoE infrastructure to get line-rate performance for wireless users as well.
- The wireless network should provide seamless connectivity and high signal strength across the campus in the rooms and corridors.
- The network should be highly scalable and robust, which should have a capability that reduces complexity in the network environment.
- Industry-standard Wireless architecture that shall deliver reliability, security, and scalability.
- It shall provide network-wide visibility and control in a single dashboard.
- The solution shall provide Centralized management for Wired and Wireless infrastructure for unified network management and ease of IT operations.
- The network should be designed and configured in a way thus clear network segmentations can be defined, which consists of unified policies based on users for wired as well as wireless.

- The network should have a controller-based orchestrator in the network. The network should have the capability to support the campus network as fabric and the switches to be programmable so that IT can be transformed from conventional to futuristic next-gen technology on software-defined networks in the campus-wide environment.
- The network shall support enhanced network visibility, which can gain access to threats within encrypted traffic without the need for decryption with the use of advanced analytics and Machine learning.
- The solution shall support the capability to do the endpoint compliance check and removal of infected endpoints from the network.
- The solution should have centralized dashboards which will help DTU to manage its enterprise network efficiently for both wired as well as wireless infrastructure.
- The solution should support providing policy-driven automation which reduces complexity and minimizes downtime.
- It should be easy to deploy, provision, manage, and troubleshoot the devices using automation.
- The solution must have the capability to natively integrate high-quality voice, data, and video within the network which will allow the administrators to remotely do the network troubleshooting & IT support as well as connect with the peers on video/audio calls. This solution should be Enterprise Grade and privacy & security to be well taken care of with the solution.
- The solution should have the capability to allow administrators / super users to schedule the remote sessions with other users from any device, anywhere to ease out the overall DTU campus operations during critical times along with the necessary software lic. etc. These administrators / super users to have role-based access within the complete network and solution to be scalable to meet the future requirement as well.
- Take multiple users in the remote session to help troubleshoot and fix IT issues which should be interactive in nature.
- The offered solution should have the capability to enable the IT support sessions to be recorded for later consumption.
- The solution must have the capability to remotely share the files/configs, etc. between peers.

- The solution should have capabilities to have IP based calling and flexibility the multiple users to join from anywhere.
- The solution should have the capability to integrate with the helpdesk/ ticketing solution and provide automated trouble ticket updates to the end users. This will enable end users to get updated status of their technical support cases raised.
- The network should be intelligent and intuitive, which lowers the risks and supports providing immediate remedial actions resulting in faster response and resolution time.
- All the components should be tightly integrated, and the solution should support Network Automation, day-2 operations and Security, centralized network fabric controller designing, provisioning, and troubleshooting the network and applying policies centrally.
- It should also support micro-segmentation between multiple segments of users where we can restrict communication within the same subnet and based on policy only selective users to be allowed.

(ii) <u>Network Security Solution:</u>

- The solution should support layer-2 encryption which supports encapsulation and protection of meta-data with the highest level of encryption.
- The solution should support software defined segmentations and policy enforcement based on user identity and groups etc. with tight integration with existing AD/LDAP. The solution should be able to define users and device profiles that facilitate highly secure access and network segmentation based on its IT/business needs.
- The overall solution should have complete user access policy implementation, which can enable dynamic mapping of users and devices. It should provide end-to-end security policy enforcement. The Groups, policies, authentication, authorization, accounting (AAA) services, and endpoint profiling can be done with an NAC / AAA server integrated with a network for policy authoring workflows.
- The solution should enable a simplified guest experience for easier onboarding and administration. The solution should also be capable of BYOD for students, faculty, and staff with enterprise mobility and self-service device onboarding.

- The solution should have capabilities to detect network traffic anomalies and detect malicious behavior from encrypted transmissions without compromising security.
- Enable new threat detection before it appears in the network and extend data protection and monitoring to any campus services, anywhere.
- The solution shall support providing protection against wireless threats like rogue APs, DoS, man-in-the middle attacks, authentication, encryption cracking, etc. for wired and wireless networks.
- Solution shall be capable of advanced network security for dedicated monitoring and detection of wireless network anomalies, unauthorized access, and RF attacks. Corrective action – with integration to WLAN to enable fixing of security threats and performance issues in real-time.
- The solution should support capability that provides Location-based access and location tracking, alerts for campus staff and students if required.
- The solution shall support to host 3rd party applications / Container-based applications for IOT etc. minimum at the distribution layer.
- The network should support the capability to upgrade patches, software updates, bug fixes, software rollback, etc. without impacting the hardware forwarding in the live network.
- Similarly, the wireless network shall be able to perform staggered upgrades within the campus to make sure wireless coverage is not impacted and enough APs are running to give the necessary coverage to users even during the odd hours of updates.
- DNS is the first step in all internet connections, and it's used by nearly all connected devices. Because of this, adding security at the DNS layer allows you to block threats earlier, before a connection to your network or endpoint is ever made.
- The solution should have recursive-based security to be integrated into the network which can detect and block advanced malware regardless of the specific ports or protocols used by the malware at the gateway/internet cloud level.
- The solution should support tight integration with the DNS solution which can detect and block advanced malware like botnets, exploit kits, drive-by, phishing, etc. used for both opportunistic attacks and targeted attacks targeted for this

specific organization and must use predictive intelligence and not use static signatures or blacklists.

- DNS Security solution should stop threats at an earlier stage by monitoring domain name requests and cloud services to prevent phishing, malware, and ransomware attacks irrespective of user working in the office or remotely.
- DNS Security solution should help in monitoring all internet traffic across users. Block attacks earlier – before they reach the endpoint or network. It should be able to contain malware that is already inside by blocking callbacks to attacker infrastructure, Managing and blocking cloud apps, etc.
- NGFWs should be able to control traffic beyond traditional port and protocol methods to also deeply analyse and correlate applications, users, traffic, and files.
- NGFW should be able to contain known and unknown malware with NGIPS, Antimalware, and sandboxing with dynamic malware analysis.
- The security solution must enhance threat protection and maximize visibility for context-aware security along with automated risk rankings and severity flags to identify priorities for the SOC team.
- NGFW should also provide remote workers with frictionless, highly secure VPN access to the enterprise network from any device, at any time, in any location while protecting the organization.
- The solution should provide centralized visibility via a central management appliance which further helps to find and respond to threats across your organization in a much better way.
- The NGFW solution allows us to protect networks, data, users, and devices from even the most sophisticated threats while delivering consistent security policies, visibility, and improved threat response, leading to robust security everywhere needed.
- The NAC solution must ensure that only authorized (across wired, wireless, and VPN connections) users can get access to the network. The NAC solution must provide the capability to quarantine any suspicious users on the network using a single console.
- The NAC Solution should enforce network authentication and authorization for the in-scope users (where present), devices, and applications. Prevent any unauthenticated (and therefore untrusted) entities from connecting to the in-scope network.

- NAC Solution must help users to securely connect to the organization network from any device, anywhere while restricting access from non-compliant devices. Verification of device posture complies with organization security policy so that risky, unpatched, and outdated devices cannot threaten the network. No network access until endpoint trust is evaluated.

(iii) <u>IP Telephony Solution</u>

- IP EPBX Servers with active-active 1:1 redundancy even across two separate locations.
- Failover between IP EPBX Servers is in a fraction of milliseconds without any call drop.
- Centralized Control for all IP & Analog Phones.
- Collaborated with Video Conferencing Facility within as well as outside campus.
- Provides extension mobility feature.
- IP Telephony can be integrated with XML and graphics-based application servers for application accessibility.
- IP Telephony can be integrated with Microsoft Outlook, institute directory
- IP Telephony provides Instant messaging, voice mail, and presence features
- IP Telephony can be integrated with landlines, mobile, and satellite phones as well as UHF/VHF/HF radios.
- IP Telephony provides scalable architecture and new phones can be added on the same infrastructure.
- Virtual guest lectures with industry leaders, alumni, and other connected education institutes.
- Campus placement interviews
- Administrative Meetings
- Faculty trainings and virtual classes across different Institutes
- Collaboration with International Institutes and Universities under Research Initiatives and Fellowship Programmes.

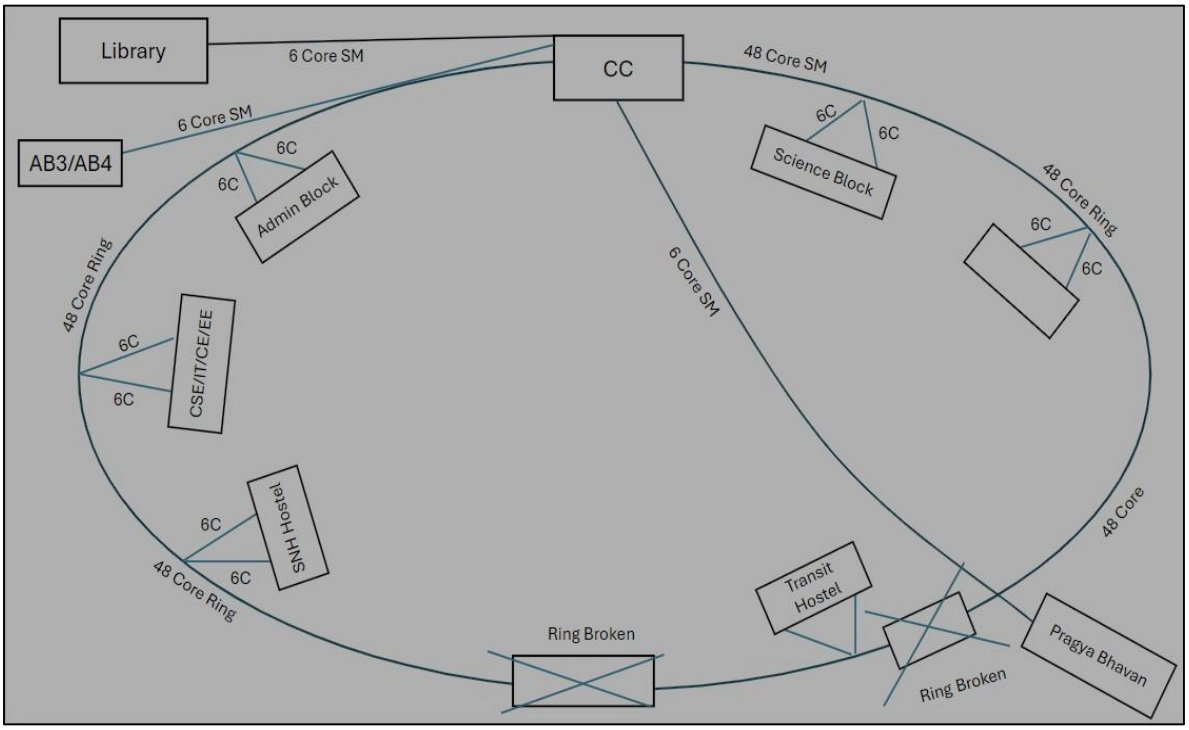
D. <u>Secure Network Solution components:</u>

- **Core Switches**
- **Distribution Switches**
- **Access Switches – Non-PoE, PoE & mGig**

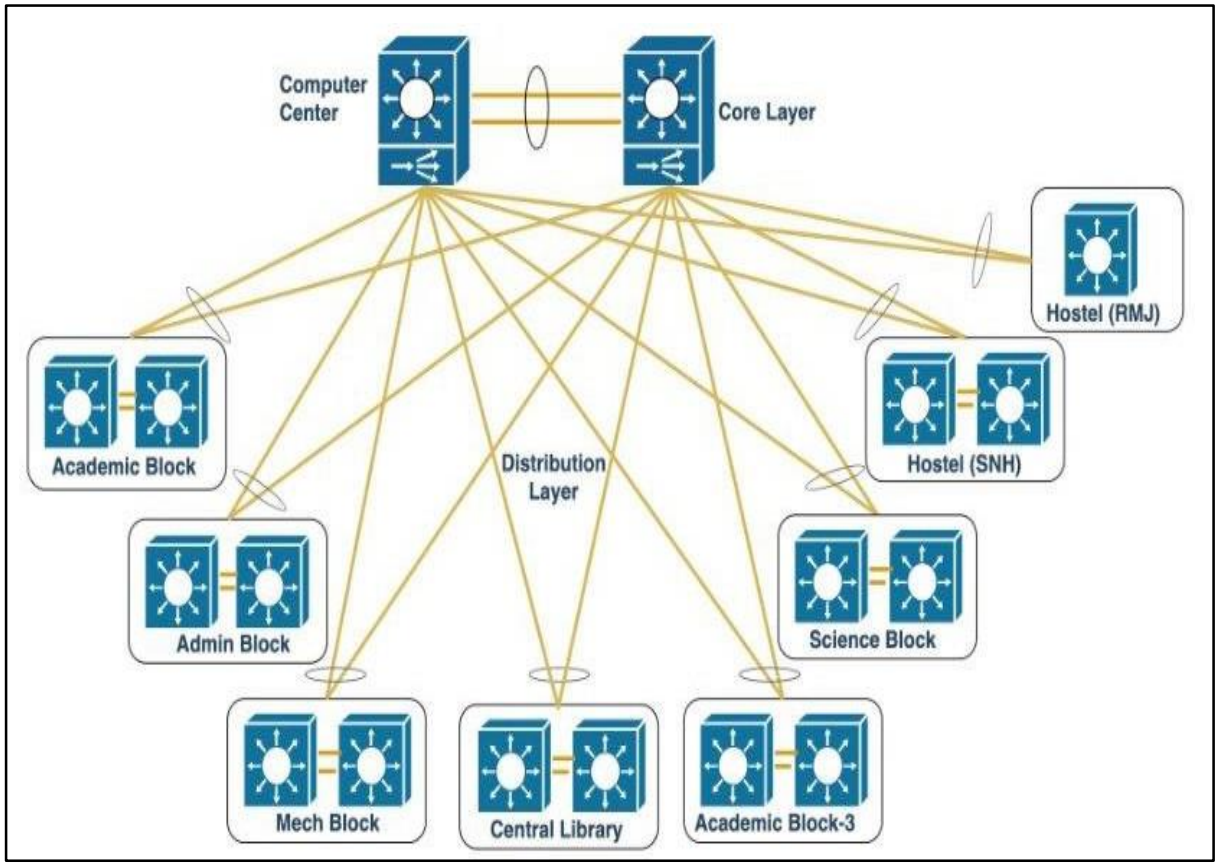
- **Indoor & Outdoor Wireless Access Points (WiFi-6)**
- **Wireless LAN Controller**
- **Network Monitoring solution**
- **Router**
- **Network Security –**
  - Next Generation Firewall
  - Malware protection and threat intelligence
  - Secure VPN
  - DNS Security
  - Network Access Control / User Identity based Access Control
  - MFA for staff
- **Unified Communication and Collaboration Solution**

E. Existing Passive Network Architecture – Physical Fiber Connectivity

The entire fiber backbone (48 core) shall be physically laid in Ring topology and providing star topology logically with 3 Tier Architecture - having Redundant Cores, redundant backbone, and redundant Distribution Switches.



F. Existing Passive Network Architecture – Logical Fiber Connectivity



The passive site survey to be conducted, the survey will help assess the current infrastructure, identify gaps, and determine the requirements for the proposed deployment at DTU. Based on the results of this assessment, a tentative and indicative Bill of Quantities (BoQ) to meet the project's needs to be provided. Based on available information the following data is summarized: -

	Main Campus	East Campus		
Description	**Qty/No**	**Qty**	**Total**	**Remark**
LAN Port (Existing)	4053	270	4323	
LAN Port Not Required	1549	40	1589	
AB-3, 4 APJ & VLB Hostel	923	0	923	
LAN Port Usable	1581	230	1811	
LAN Port (Additional Required)	3345	70	3415	
Nodes(Existing+New)	4926	300	5226	
Wi-Fi Point	1421	48	1469	
Total LAN Nodes (Exiting+New+Wi-Fi)	6347	348	6695	New switch to be considered for this qty.
Old Switches				All are out of warranty and support
12-Port Old Switch	9	6	15	
24-Port Old Switch	128	6	134	
48-Port Old Switch	24	2	26	

Site Survey Assumptions:

- The data point is factored as per the node's details shared by the customer for the individual department.
- All Hostels will be on Wi-Fi, 4 Wired nodes have been considered with a New Rack, and Jack Pannel.
- Use of one pair of Existing OFC cables for the Wi-Fi network.
- AB-3, AB-4, APJ Hostel, & VLB Hostel New building's additional LAN Points and Wi-Fi points have been considered.
- Existing nodes' copper Cable and Broken Fiber repair/Replacement would be checked for further estimation.
- UPS and cooling is required at each rack location.

5. Expected Deliverables of the work

- Detailed project plan, design architecture, and implementation methodology.
- Processing, procuring, installing, operationalizing and training for future operation.
- Procuring, installing operational and
- Bill of Material with make, model, and specifications.
- 5-year O&M and warranty support plan.
- Compliance to Government IT policies and IT security standards.

6. Eligibility Criteria

- The bidder should be a PSU, Govt of India undertaking or government dept. caring out deployment out deployment of Wi Fi networking.
- Minimum 5 years' experience in execution of campus-wide or enterprise-level Wi-Fi and networking projects.
- Experience in at least three projects of similar scale (₹25 crore or above) for reputed Government or Educational Institutions in last three years.
- Average annual turnover of ₹100 crore or above during the last three financial years.
- Five M.Tech and Ten B.Tech in relevant field on roll with experience of 3 years.

7. Submission Details

Interested agencies may submit their Expression of Interest containing:

- Company Profile and Credentials.
- Summary of Similar Projects Executed in last five years with cost involved – supporting proof document will be required.
- Preliminary Technical Solution and Approach.
- Compliance to Eligibility Criteria.
- Indicative Project Timelines.
- EMD of Rs. 1.6 Cr.

- In the shape of Demand Draft/Bank Guarantee in favor of Registrar, DTU Payable at Delhi.

8. Tentative Timeline for the process of EOI:

- Pre-bid meeting – 29th Dec. 2025
- Last date of submission of EOI – 13st Jan. 2026
- Notice about shortlisted firm – 19th Jan. 2026
- Date of presentation by shortlisted firm – 27th Jan. 2026
- Date of declaration of provisional Result of EOI – 02nd Feb. 2026
- Date of filing review request by disqualified firms – 06nd Feb. 2026
- Date of declaration of final result – 12nd Feb. 2026
- Date of Issue of RFP – 27th Feb. 2026

9. EOIs shall be submitted to:

- The Chief Project Officer,
- Delhi Technological University,
- Shahbad Daulatpur, Bawana Road, Delhi – 110042.
- Email:-

10. Evaluation and Further Process

The EOIs will be evaluated by a committee constituted by DTU based on technical competence, experience, and suitability of the proposed solution. Minimum score of Eligibility criteria defined below should be equal to or more than 75 on the scale shown below:

(This scoring is applicable only for a firm which is PSU, Govt of India undertaking or government dept. caring out deployment out deployment of Wi Fi networking)

S. No	**Criteria**	**Sub criteria**	**Score**
1.	Experience	More than 5 to 10 years	20
		More than 10 years	25

2.	Turn over (average of last three years)	100 - 200 Cr / years	20
		More than 200 Cr. / years	25
3.	Number of single completed works orders of value 25 Cr. in last three years	Three	10
		For each order more above three	5 (maximum 20)
4.	No. of M. Tech with three years' experience No. of B.Tech with three years' experience	Five Three	10
	Subtotal		80
5.	Presentation on Technical Solution and Approach *		20
	Grand Total		**100**

*Only those firms will be invited for presentation who scores more than 60 as subtotal.

Shortlisted firms may be invited to present detailed solutions before the issue of a Request for Proposal (RFP).

11. Checklist for documents to be attached with expression of interest to be submitted by the firm

(this check list is to be duly filled and attached with the EOI submitted by the firm)

S. No.	**Name of document**	**Description**	**If attached, the page number**
1.	Covering letter for the EOI	With brief description about the firm, this should explicitly and unconditionally express the interest work.	

2.	EMD	In the form of Demand Draft, FD mortgaged to DTU, Bank Guarantee, Electronic Bank guarantee	
3.	Type of firm	Document showing the firm is a PSU, Govt of India undertaking or government dept. caring out deployment out deployment of Wi Fi networking.	
4.	Experience	Work orders with completion certificates showing the year of experience of the firm.	
5.	Turn over	Financial statement showing such turnover duly Certified by Chartered Accountant/ Head of accounts of the firm.	
6.	Number of single completed works orders of value 25 Cr. in last three years	Work orders not older tha three years with completion certificates showing the year of experience of the firm.	
7.	CV of M.Tech /B.Tech staff	With experience of 3 years in the field of Wi-Fi Networking.	
8.	Contact details	Address with mobile / telephone number and email.	

Signature and Stamp

12. Disclaimer

This Expression of Interest is intended only to obtain indicative responses for understanding market capabilities. It does not constitute a solicitation, commitment, or binding tender document. DTU reserves the right to amend, modify, or cancel this EOI without assigning any reason.

Issued with the approval of the Competent Authority

Delhi Technological University (DTU)

Date: ___ / ___ / 2025