National Institute of Electronics and Information Technology, Delhi
Centre 2nd Floor, Parsvnath Metro Mall,
Inderlok Metro Station, Inderlok, Delhi-110052

Eligibility Criteria against the Advertisement vide no. 07/301/2023/NDL/FM for empanelment of IT Resource Persons to be deployed in specific Govt. Department in Delhi/NCR on contract basis

S. No.	Name of The Post/ No. of Positions	Essential Qualification	Consolidated Monthly Salary (Rs.)	Experience (after availing essential qualification) as on - 26-03-2023	Job Profile/ Skill Set/ Locations (probably)
01	Consultant –CE (5)	Bachelor's Degree in Technology or Engineering or equivalent in the field of Computer Science / Information Technology / Cyber Security / Electronics and Communications with atleast 60% marks in aggregate. OR M.Tech. in the field of Computer Science / Information Technology / Cyber Security / Electronics and Communications / MCA Degree, with at least 60% marks in aggregate	60,000/- to 90,000/-	Minimum 5 years experience in the required domain field in areas of Cyber Security as per detailed responsibilities and tasks defined **in para-2 (below**) Desirable: Any certificate related to Cyber security: CEH/CISSP/CISA/ OSCP or Diploma in Cyber security	Age Limit: upto 40 years **For : Delhi/NCR**

Note: The number of vacancies are tentative and can vary at any point of time as per office requirement.

Para 2- Detailed Responsibilities and Tasks

1. **Consultant (CE)**

(a) **Cyber security audit and VAPT**
- Web Application and mobile application auditing (including Android, and iOS) vulnerability assessments, Compliance audits, Code Reviews
- Source Code Security Audit; inspect the source code for security weaknesses.
- Remote Vulnerability assessment and Security Testing of Web applications.
- Static Source code Vulnerability Audit and Security Testing of websites code.
- Review of authentication, authorization, session and communication mechanisms

- Research and Development of solution to mitigate Application level attacks.
- Review of third-party libraries
- Security validation of cryptographic functions and routines
- Evaluation of tools/solutions for Vulnerability Assessment and Penetration Testing

(b) Analyst /developer/auditor (expert areas)

• Tracking of cyber threat and vulnerabilities and analysis

• Vulnerability analysis, Support for Exploit testing, writing scripts, Advisory preparation

• Preparation of guidelines, case studies and white papers

• Providing assistance to senior analysists for tracking of incidents such as website intrusions/defacements, Spam, vulnerable and open services such as open DNS, open NTP, exposed databases etc and coordinating incident response with shift teams

• Determination of operational and implementation feasibility by evaluating problem definition, requirement analysis, solution design development of the proposed solutions.

• Preparation of specifications, designs, flowcharts, layouts, diagrams of the required application/software.

• Preparation and installation of solutions by determining and designing system specifications, standards, and programming.

• Providing information by collecting, analyzing, and summarizing development and service issues.

• Providing expert guidance to external/internal developers/programmers

• Improving overall development efforts by conducting systems analysis, recommending changes in policies and procedures, recommending platforms and products, testing and approving products.

• Development of scripts/programs according to the specific requirement different internal teams such as Operations/malware analysis/ Infrastructure Management

• Leading teams for development of Scripts for aiding in Malware analysis and forensics.

• Web application and mobile application auditing

• Source code review

• Evaluation of tools/solutions for VAPT

• ISMS audits

• Auditing of Industrial Control Systems