

National Institute of Electronics and Information Technology, Delhi Centre

Institutional Area, 16/1-2, Pankha Road, Near Sagarpur Police Station, D Block, Janakpuri New Delhi 110058

Eligibility Criteria against the Advertisement vide no. 07/306/2023/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	Essential Qualification *	Consolidated Monthly Salary (Rs.)	Experience (after availing essential qualification) as on --04-02-2024 /Location (probably)
01.	Data Entry Operator- D	a) Graduation from recognized University b) Should possess typing Speed of not less than 35 wpm in English. c) NIELIT CCC/NIELIT IT O Level / NIELIT MAT O Level/ Min. six months Diploma in Computer Applications from Govt. University or Govt. recognized University/ Institutions	Rs.25000/- to 30000/-	3+ years Desirable: a) Experience as DEO in Govt./Semi Govt/Autonomous undertaking of Govt. b) Experience in Government projects and various roles like overall administrative duties Management of files and knowledge of Govt. rules Delhi
02.	IT Training & Support Executives – D	a)MCA/DOEACC B Level/ B.E./ B.Tech (Computer Science/ Information Technology / Electronics/ Electronics & Communication/ Electronics & Electrical/ Electronics & Telecommunication/ Electronics & Instrumentation) Or b) BCA/DOEACC IT-A Level/ BSC(IT)/ Post Graduate Diploma in Computer Application or higher	Rs. 44,900/-	For a) 2+ years For b) 3+ years Desirable: a) In-depth knowledge of Adobe/OneNote b) Excellent communication skills <u>Skill Set/Requirement:</u> Master Trainer: Providing IT support and Training in IT modules to Judicial Officers (dignitaries). Note: The candidate will have to provide training /customization at odd hours as per the requirement of dignitaries. Delhi

03.	<p>Sr. Consultant-M (Data Center Expert)</p>	<p>B.E./B.Tech(Computer Science/ Electronics/IT) OR MCA/MBA(Systems /IT) OR M.E./M.Tech (CS/IT/Electronics)</p> <p>Certified Data Center Professional (CDCP) and related certification will be a plus.</p>	Rs. 1,67,000/-	<p>Overall 10+ years in IT/Data Center related Projects. The Data Center specialist should have following key skills –</p> <ul style="list-style-type: none"> • Supervising maintenance, installation, and updates of data center systems, for both physical and software • Establishing the rules related to data accessibility and distribution • Establishing the parameters for data entry or storage of customers' data • Ensuring the safety and protection of customers' data • Managing the storage and distribution of data • Backing up data • Maintenance of equipment • Entertaining customers' inquiries and issues • Recording the installations, upgrades, and maintenance of systems or software • Creating planning for capacity changes • Upgrading hardware or software used by the organization • Researching new technologies to be utilized in the organizations • Presenting new tools that could be used to improve efficiency or cutting costs • Ensuring a safe and secure facility to protect the systems and power configuration • Planning for any probable disruptions, problems, and emergency • Troubleshooting technical or IT related issues • Configuring, managing, and analysing automated system utilized in the organization • Ensuring precautions are set in place whenever power outages or malicious attacks occurred • Ensuring the operations are in compliance with the regulations and laws. <p>Delhi</p>
-----	---	--	----------------	--

04.	Consultant –CE	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 Age Limit: upto 40 years	Rs. 60,000/- to Rs. 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 Delhi
05.	Sr. Consultant –CE	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 Age Limit: upto 40 years	Rs. 90,000/- to Rs.1,25,000/-	Minimum 10 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. Delhi
06.	Executive (HR)	a. Graduation in any stream b. Post Graduate Diploma in HRM with 60% marks Or Post Graduate Diploma in Business Management(HR) with 60% marks Or M.B.A. (HR) with 60% marks. c. Min. 6 months Diploma in Computer Application /Computer Science	Rs. 30,000/- to Rs. 36,000/-	2 years in relevant field. Delhi
07.	Junior Assistant (Exams)	10+2 with NIELIT Course on Computer Concepts (CCC) certification. Desirable: Certification in Data Entry	As per minimum wages of Labour Dept., GNCT of Delhi norms.	Minimum 1 year experience especially in examination related activities with good working knowledge of MS-Office Delhi.

Note: * The qualification of candidates must be from Govt. University or Govt. recognized University/ Institutions.

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 analysts 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

2. Sr. Consultant (CE)

(a) Senior Analyst

- Acting as resource persons for handling critical incidents and performing analytical tasks in the area of malware/artifact analysis, cyber

- forensics, threat hunting, breach investigation, operationalization of decoy systems, log analysis, correlation of incidents, analytics
- Data Scientists including operationalization of big data analytics
- Identification of new scientific techniques in incident analysis
- Tracking cyber threats, vulnerabilities reported in various systems/platforms/devices and preparation of vulnerabilities notes and advisories for publishing on website of CERT-In
- Tracking of malware threats and preparation of virus alerts for publishing on website of CERT-In
- Tracking of emerging threats, wider exploitation of vulnerabilities and new cyber-attacks and preparation of current activity for publishing on website of CERT-In
- Finding new vulnerabilities in s/w widely used in constituency , Coordination for vulnerability remediation with stakeholders
- Analysis and taking actions of reported vulnerabilities in systems/websites/networks and processes of organisations in various sectors
- Exploit writing and testing, finding and evaluating new tools/solutions in open source for using and commercial domain for procurement, creating testbeds
- Coordination 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
- Scientific ways of log analysis, attacker attribution, trends in IP masquerading (proxy, vpn etc.) , Review of analysis reports, preparing trends reports
- Preparation of guidelines and best practices to prevent recurrence of incidents and enhancing security posture of organisations in various sectors
- To make repository of publicly released incident information in specific sectors such as finance, telecom, power, transport, defence etc for keeping abreast of the current threats and achieve readiness to study and implement early responses
- Collection and analysis of relevant information, reports and data and maintain to help respond to inquiries received from stakeholders and to assist with reviews of documentation such as security architecture designs and security operation procedures
- Providing training to constituency on various areas of cyber security
- Participating in International cyber drills
- Conducting cyber drills/exercises at national level, sectoral /state level and organization level
- Handling of activities related to bilateral / multilateral agreements (MoUs) on cooperation in the area of cyber security and other coordination related tasks.

(b) 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

(c) 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 analysts for tracking of incidents such as website intrusions/defacements, Spam, vulnerable and open services such as openDNS, 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