Name of Post (2)	**Senior Technical Assistant - Vulnerability Assessment & Penetration Testing – VAPT** **And** **Technical Assistant - Vulnerability Assessment & Penetration Testing - VAPT**
Pay Matrix Level	Level- 7 & Level -6
No of Positions	Level 7 – 1 no & Level 6 – 1 no
Place of Posting	Bengaluru
Reservation	Level 7- 1 OBC & Level 6- 1 OBC
Educational Qualification	**Level 7 : - Member Technical Staff B1 (MTSB1)** (a) First class Diploma in Engineering / Computer applications with and 6 years of experience in the relevant field OR (b)First Class Degree in Computer Science / Electronics / IT/ Computer applications or relevant domain and 6 years of experience in the relevant field OR © Graduate with first class and DOEACC 'B' Level with 2 years of experience in the relevant field **Level 6 : -Member Technical Staff B2 (MTS B2)** a) First Class Diploma in Engineering / Computer applications with and 3 years of experience in the relevant field OR (b) First Class Degree in Computer Science / Electronics / IT/ Computer applications or relevant domain and 3 years of experience in the relevant field OR ©Trade Certificate with NCVT where basic qualification for admission to the Course

	is Matriculation or equivalent and 9 years of experience in the relevant field OR (d) Graduate with First class and DOEACC ‘A’ Level with 4 years of experience in the relevant field.
Age	35 years as on last date of submission of application as mentioned in advt. (Relaxation according to Govt. Of India instructions)
Desired Skill set	• Knowledge of basic network concepts such as TCP/IP protocol stack • Understanding security protocols such as SNMP etc • Knowledge in Cryptography and cryptographic algorithms • Knowledge of security standards like ISO 27001, PCI DSS, India cyber security Law • Knowledge of perimeter security solutions like Firewall, IDS , IPS, UTM, WAFs and security Analysis tools • Knowledge of Network Management and Monitoring tools • Experience in vulnerability assessment and penetration testing of web applications, operating systems, network equipment, Wireless, Mobiles & Database • Familiar & hands on experience with commercial/open source VAPT tools such as NMAP, Nessus, OWAP Zap, Burp, Netparker and exploit frameworks like Metasploit • Proficiency in dedicated Linux distributions like Kali Linux and Packet analysis tools Like Wireshark • Experience and Proficiency in ethical Hacking Preferred i. Certification from SANS or Certified Ethical hacker (CEH) or Computer hacking forensic investigator (CHFI) from EC council India i. Knowledge of Python ii. Expertise in the analysis of E-mail frauds
Job Profile	• Perform vulnerability and Penetration testing. • Compliance testing for various Cyber Security standards towards implementation of security policies and controls. • Implementing and mainlining security controls by adopting International best practices • Internet traffic monitoring • IP, Domain Name, user profiles tracking using Open Source Intelligence • Carry out proactive security testing as a routine activity based on the defined policies and control structures • Conduct and ensure periodic infrastructure audits (network, servers and Systems) and investigation of any cyber violations • Analysis and assess the vulnerabilities in the infrastructure (software, Hardware, Networks) and devise the possible counter measures

	• To be part of the Blue team and red team cyber security drills • Ensure business continuity with plans for effective backup and disaster recovery plans and procedure • Ensure cyber security practices and Secure SLDC for all in-house and outsourced applications development • Implement system security engineering across the programme acquisition life cycle performing and analyzing a range of IA/ C& A assessment activities. • Responsible for the development of design process and security policies and updating the gaps in the Information Security practices to the Senior management