

## Designation: Consultant – Cyber Security

### Desired Candidate Profile:

- Should have total minimum experience of 4 years in defining/working on cyber security framework, organizational IT security policies & processes for large scale Telecom/IT Projects.
- Should have:
  - ⇒ In-depth understanding of TCP/IP, common networking ports and protocols, traffic flow, system administration, OSI model and common security elements.
  - ⇒ In-depth knowledge of security tools & system applications.
  - ⇒ Ability to coordinate with various stakeholders including vendors & field teams for resolution of security incidents.

### **A) Educational Qualification:**

- **B.E. / B.Tech** (in Electronics & Communication / Electronics & Telecommunications / Computer / Information Technology ) with first class from reputed institute / university **OR** **M.E. / M.Tech** (in Electronics & Communication / Electronics & Telecommunications / Computer / Information Technology) with first class from reputed institute / university.  
(Only Candidates having Full Time Degree will be permitted)
- **Professional Certification Related to Cyber Security** i.e. CND / ECSA / ECSS / CISSP / CEH / CompTIA Security+ / CCSP / CHFI with a valid ID verifiable on ISACA / EC-Council / CompTIA respectively.  
(NOTE: Vendor Specific Certifications like PaloAlto, Juniper, Cisco, etc. will not be considered)  
(NOTE: The certificate should not have expired before 31stDecember 2018)
- **OR** On Deputation from Central PSU.

### **B) Key Roles and Responsibilities:**

- Operations and Maintenance of Security practices in large and complex Network comprising of mix of technologies (ICT & Telecom) and products like GPON, DWDM, Router, Switches, Server, storage, NMS/EMS, etc.
- Defining strategies & policies for the deployment of information & Network security technologies.
- Ensuring Network protection by ensuring implementation of Security strategies and policies.
- Perform security audits, IT & Network security risk assessments & manage security threats.
- Implement security improvements by assessing current situation, evaluating trends & anticipating requirements.
- Work closely with manager for process and efficiency improvement within the NOC.
- Coordinate with SDC team & vendors for periodic security audit of applications.
- Analysing high volumes of logs, network data and other attack artefacts for incident investigations.
- Recommend suitable enhancements to improve information & Network security performance.
- Basic understanding of common information security management frameworks such as ISO/IEC 27001.
- Basic understanding of Telecom services and active & passive components of Telecom networks.
- Understanding of e2e life cycle of incident & problem management.
- Complying with the latest regulations and compliance requirements.

### **C) Soft Skills:**

- Should be a team player and must have good written and verbal communication skills
- Ability to liaise with various stakeholders including business team & vendors
- Problem solving and Analytical skills

### **D) Age Limit: Not more than 35 Years**

### **E) Remuneration: INR 50,000/- P.M. (Cost to Company basis) or for ITS officers on deputation, pay protection benefits will be provided**

\*\*\*\*\*\_\*\*\*\*\*