Engagement with GSTN would be on tenure basis. The tenure would be of 4 Years. GSTN allows multiple tenure based on the performance.

Assistant Vice President (AVP) – Cyber Security

Role	Assistant Vice President (AVP) – Cyber Security
Reporting to	Senior Vice President (SVP) - CISO
Function	Technology
Experience	12 – 14 Years

Role Description

AVP – Cyber Security will be responsible for overseeing and managing the security posture of the GST System and internal IT infrastructure at GSTN. This role includes ensuring the continuous operation of 24x7 security monitoring, incident response and management of security devices, applications and appliances in collaboration with the System Integrator's (SI) team. The AVP will drive compliance with GSTN's Information Security policies, standards and procedures while aligning with industry best practices and regulatory requirements. This position reports to the CISO of GSTN.

Key Skill Set:

1. **Enterprise Security Expertise** – Hands-on experience in designing, implementing and managing Cyber security for large-scale enterprise environments, ensuring robust security controls and risk management. Practical experience in integrating security frameworks such as NIST, ISO 27001, CIS and Zero Trust with enterprise IT infrastructure (on-Prim and Cloud) to enhance cybersecurity resilience.
2. **Security Operations Center (SOC) Leadership** – Hands-on experience in leading SOC operations, managing a 24x7 security monitoring team and establishing a secondary SOC for business continuity and threat resilience.
3. **Security Operations & SIEM Analytics** – Strong expertise in monitoring SIEM alerts, correlating threat data, identifying attack patterns and leveraging AI-driven security analytics for proactive threat detection. Practical expertise in configuring, managing and analyzing audit logs, transaction logs, SIEM platforms (e.g. Splunk, FortiSIEM, QRadar, ELK etc.) for proactive threat detection and prevention.
4. **Security Metrics & Dashboarding** – Experience in developing cybersecurity KPIs, security posture dashboards and real-time risk visibility tools to measure security effectiveness and maturity.
5. **Application & Web Security** – Strong hands-on expertise in securing web applications, APIs, microservices and cloud-native applications, with in-depth knowledge of OWASP Top 10, SANS etc. and mitigation strategies.
6. **Identity & Access Management (IAM)** – Proven experience in managing IAM solutions, Privileged Access Management (PAM), Multi-Factor Authentication (MFA), Single Sign-On (SSO) and enforcing Zero Trust principles across the enterprise.
7. **Network Security & Segmentation** – Hands-on experience in configuring and securing network infrastructure, including firewalls, VPNs, SDN, NAC and micro segmentation, with a deep understanding of routing protocols and network hardening.
8. **Endpoint & User Security** – Hands-on experience in deploying and managing Endpoint Detection & Response (EDR), Extended Detection & Response (XDR), Mobile Device Management (MDM) and insider threat monitoring solutions.
9. **Secure Configuration Management** – Strong experience in enforcing secure configurations for security appliances (firewalls, IDS/IPS, WAFs, DLP etc.), ensuring compliance with industry hardening standards.
10. **Data Encryption & Protection** – Hands-on expertise in implementing encryption techniques for data at rest, in transit and in use, including AES, RSA, TLS/SSL, tokenization and homomorphic encryption.
11. **Advanced Security Technologies** – Deep knowledge and practical experience in firewalls, NIPS, HIPS, SSL/TLS, Web Application Firewalls (WAF), Zero Trust Network Access (ZTNA), CASB and cloud security tools.
12. **Continuous Monitoring & Threat Intelligence** – Hands-on experience in configuring and managing security monitoring tools, integrating threat intelligence feeds and proactively identifying and mitigating threats.
13. **Forensics & Incident Response** – Deep knowledge of digital forensics and expertise in incident analysis, malware analysis, evidence preservation and root cause analysis for security investigations.

14. **Security Incident Management** – Hands-on experience in leading incident response, SOC operations, playbook automation and crisis management strategies, ensuring swift response to security threats.

15. **Risk Assessment & Threat Modeling** – Experience in conducting cyber risk assessments, threat modeling, attack simulations (Red Team/Blue Team exercises) and penetration testing to identify security weaknesses. Hands-on experience in analyzing enterprise-wide changes, identifying potential security risks and providing actionable insights to mitigate threats.

16. **Audit & Compliance Readiness** – Experience in drafting, implementing and enforcing security policies, SOPs and governance frameworks to ensure enterprise-wide adherence to security standards. Strong knowledge and experience in supporting internal/external audits, assessing security controls and ensuring compliance with ISO 27001, PCI-DSS, DPDPA, GIGW, RBI guidelines and other regulatory standards.

17. **Security Posture Enhancement** – Hands-on expertise in conducting security gap assessments, fine-tuning security configurations and continuously improving security posture through automation and AI-driven security analytics.

18. **Data Center & BCP/Disaster Recovery Security** – Practical experience in securing data centers (DC), BCP/Disaster Recovery (DR) sites, ensuring business continuity and resilience against cyber threats.

19. **Audit Readiness & Threat Mitigation** – Proven ability to identify, analyze and implement corrective actions for emerging threats, ensuring continuous compliance and audit readiness.

People Development

- **Talent Acquisition:** Actively participate in the recruitment and selection process to build a high-performing cybersecurity team.
- **Performance Management:** Conduct formal performance appraisals, provide constructive developmental feedback and set clear growth objectives for team members.
- **Training & Skill Development:** Identify skill gaps within the team and facilitate functional training programs through internal and external learning resources to enhance expertise and efficiency.

Key Interfaces:

External:	**Internal:**
• MSPs • System Integrators • Product and Services Vendors	• Internal Departments i.e. Services; Procurements and Contracts; Customer Service, Technology; R&D, Techn

Key Attributes & Skills:

- Educational Qualification: B.E./B.Tech in Electronics, IT, Computer Science, MCA, M.Sc. or an equivalent qualification with a minimum of 10 years of rel experience.
- Information Security Expertise: Strong experience in cybersecurity, including IT infrastructure security, application security, data protection and securit operations in large-scale IT environments—especially those leveraging open-source technologies.
- Cyber Security Operations Experience:
- Minimum 2 years of experience managing Cyber security operations in large, multi-tiered, heterogeneous IT infrastructures or data centers.
- At least 5 years of hands-on experience in 24x7 Security Operations Center (SOC) environments, handling real-time security incidents, threat managem response.
- Certifications & Frameworks: Security certifications such as CISSP, CISM, CEH or equivalent are must. A solid understanding of security frameworks like is preferred.