Assistant Manager – IT Security

No of Vacancies	01
Direct Reporting to	Manager – IT Systems & Networks
Education:	Bachelors / Master's degree in Cybersecurity or related field.
Special Education	The IT Security Specialist will be responsible for protecting our information systems by designing and enforcing policies, monitoring network traffic, and active responding in case of any security threats. This role requires a proactive and analytical professional with a strong understanding of cybersecurity practices and technologies. Relevant certifications such as CISSP, CISM, CEH, CompTIA Security+, or equivalent would be a plus.
Experience	3 to 5 years of experience
Location	Karachi
Job Description:	• Security Management: Develop, implement, and maintain security protocols, policies, and procedures. • Systems & Networks Management: Hands-on grip on systems and networks management and understanding of trading systems. • Threat Analysis: Monitor network activity for security breaches and investigate violations. • Incident Response: Lead incident response efforts, conduct forensic investigations, and implement corrective actions. • Vulnerability Assessment: Perform regular vulnerability assessments and penetration tests when requested. • Compliance: Ensure compliance with industry standards and regulations (e.g., GDPR, HIPAA, ISO 27001). • Research: Research the latest information technology security trends to stay ahead of potential threats. • Security Measures Assessment: Assess the organization's security measures, such as firewalls, anti-virus software, and passwords, to identify any weak points that might make information systems vulnerable to attack. • Simulated Attacks: Perform simulated attacks to test the efficiency of security measures. • Data Protection Prioritization: Prioritize security coverage to ensure that strategically important data, such as commercial information or personal data, receives the highest levels of protection. • Cybersecurity Plan: Help to design, implement, and maintain the organization's cybersecurity plan. • Security Standards: Develop and direct implementation of security standards and best practices for the organization. • Security Tools Management: Direct the installation and use of security tools (e.g., firewalls, data encryption), to protect sensitive information. • Security Audits: Ensure that IT security audits are conducted periodically or as needed • Training: Educate staff on information security best practices and policies.

	• Risk Management: Conduct risk assessments and develop mitigation strategies. • Recommend security enhancements to IT Management.
Skills:	Proficiency in security technologies (firewalls, IDS/IPS, SIEM). Strong knowledge of network protocols, operating systems, and databases. Experience with security tools and software (e.g., Wireshark, Metasploit, Nessus).
Note:	“PMEX is an equal opportunity employer and we encourage differently abled people to apply for their relevant/suitable areas”.