JOB DESCRIPTION – DEPTUY DIRECTOR (CYBER SECURITY)

Function: Information Technology		**Reports to**: Director (Information Technology)
Location: Islamabad	**No of Posts:** 01	**Age:** Maximum **40** Years at the time of closing of advertisement.

Job Responsibilities:

- Cyber security specialists' main focus is to keep an organization's data and IT infrastructure secure, which requires a diverse set of skills and responsibilities.
- Conduct threat and risk analysis and analyze the business impact of new and existing systems and technologies to eliminate risk, performance and capacity issues. Implement vulnerability assessments and configure audits of operating systems, web servers and databases and detect patterns, insecure features and malicious activities in the infrastructure
- Perform research, testing, evaluation and deployment of security technology and procedures.
- Run diagnostics on any changes to data to verify any undetected breaches
- Develop custom systems for specialized security features and procedures for software systems, networks, data centers and hardware.
- Develop and implement information security standards, guidelines and procedures.
- Develop firewalls to secure the network infrastructure.
- Keep current with new intrusion methods and develop protection plans. Have an in-depth understanding of vulnerabilities, management systems and common security applications.
- Conduct counteractive protocols and report incidents. Offer customized risk ratings for vulnerabilities based on company policies and maintain IT security controls documentation
- Ensure compliance with IT security support policies and procedures;
- Procure necessary licenses, services required for providing on-going support function;
- Monitor the adequacy and capability of IT security system;
- Identify methods / ways to solve the existing threats and security issues;
- Supervise configuration and installation of new software and hardware;
- Conduct periodic network monitoring and intrusion detection analysis to determine if there have been any attacks on the system;
- Provide supervising role in the installation of antivirus to fortify security system;
- Responsible for the development of risk mitigation activities (physical, business and financial controls) to improve the control environment;
- Provide training to concerned department personnel and explain security risks as well as the need for using strong passwords and protecting data;
- Monitor and administer the security of organization's databases.
- Monitor change management and database logs to analyse and resolve any identified security issues.
- Manage related IT assets with respect to its identification, classification and periodic physical verification etc.
- Act as the subject matter expert for the SIEM solution and maintain SIEM operations.
- Work with teams to ensure all necessary logging sources are reporting to the SIEM.
- Develop, modify, build, implement, deploy and test SIEM correlation rules in alignment with log monitoring requirements.
- Creation of technical compliance reports from SIEM and escalate suspicious activates to concerned team members.
- Configure and administrate IT security tools in compliance with company IT security policies, procedures and guidelines.
- Conduct vulnerability scans and follow up with teams to remediate the identified loopholes.
- Administrate the accessibility of external users through two factor authentication solution.
- Research and develop methods of tracking and detecting malicious activity within a network.
- Correlate collected intelligence with malware research using Endpoint security solution to build upon a larger knowledgebase of tracked threat activity.
- Perform any other job-related duties as assigned by Management.

Job Requirements / Skill Set:

- Advanced certifications such as SANS GIAC/GCIA/GCIH, CISSP, CISA, CISM or CASP and/or SIEM-specific training and certification.
- ITIL, COBIT 5, ISO 27001 or ISO 20000 will be given preference.
- Experience with vulnerability scanning solutions.
- Ability to use logic and reasoning to identify the strengths and weaknesses of IT systems.
- A deep understanding of how hackers work and ability to keep up with the fast pace of change in the criminal cyber-underworld.
- Great awareness of cybersecurity trends and hacking techniques.

JOB DESCRIPTION – DEPTUY DIRECTOR (CYBER SECURITY)

Function: Information Technology		**Reports to**: Director (Information Technology)
Location: Islamabad	**No of Posts:** 01	**Age:** Maximum **40** Years at the time of closing of advertisement.

Qualification:

- Four (04) Years Bachelor's Degree or Masters' degree in Computer Science from HEC recognized university.

Experience:

- **Minimum 6 years** of relevant post qualification experience.