

JD – Director General Information Security			
Grade: NITS – 02	No of Posts: 01	Appointment Details	
		Type: Contractual	Method: Open Merit
Age: Maximum 55 years on the last date of application		Reports to: Chief Information Security Officer (CISO)	
Job Responsibilities: <ul style="list-style-type: none">▪ Lead the organization’s information security strategy and governance framework.▪ Develop and enforce enterprise-wide security policies, standards and procedures.▪ Oversee cybersecurity operations, including Security Operations Center (SOC) management.▪ Ensure compliance with regulatory, legal and industry information security standards.▪ Identify, assess, and mitigate cyber risks across systems, networks and applications.▪ Lead incident response, investigation and breach management activities.▪ Conduct security audits, risk assessments and vulnerability testing programs.▪ Oversee identity and access management, network security and cloud security controls.▪ Align security initiatives with organizational strategy and digital transformation objectives.▪ Manage third-party/vendor security risk assessments and compliance.▪ Establish disaster recovery, business continuity and crisis management plans.▪ Monitor security metrics, prepare reports and present to executive leadership and board.▪ Drive awareness, training and security culture across the organization.▪ Implement advanced threat detection, prevention, and mitigation strategies.▪ Guide technology teams on secure design, development, and deployment practices.▪ Ensure protection of sensitive data, intellectual property, and critical assets.▪ Collaborate with legal, IT, and compliance teams on security initiatives.▪ Provide executive advice on emerging threats, vulnerabilities, and security trends.▪ Lead and mentor a high-performing information security team.▪ Represent the organization in cybersecurity forums, governance boards, and audits.▪ Perform any other duty assigned by the CEO from time to time.			
Education & Experience: <ul style="list-style-type: none">▪ Master's Degree from HEC recognized universities in any of the following discipline; Computer Science, Information Technology, Cybersecurity, Information Security, Computer Engineering OR;▪ Bachelor's Degree from HEC recognized universities in any of the following discipline; Cyber Security, Systems Engineering, Computer Engineering, Network Engineering.▪ In case of Masters, a minimum of 10 years of experience. Whereas, in-case of Bachelors, a minimum of 12 years of experience.▪ At-least 3 years of leadership experience.			
Job Requirements (Skill, etc.) <ul style="list-style-type: none">▪ Extensive expertise in cybersecurity, information security management, and risk governance.▪ Strong knowledge of security frameworks such as ISO 27001, NIST, COBIT, and ITIL.▪ Ability to develop and implement enterprise-wide security strategies and policies.▪ Experience in cyber risk assessment, threat intelligence, and vulnerability management.▪ Strong leadership in managing security operations centers (SOC) and incident response teams.▪ Knowledge of data protection, privacy laws, and regulatory compliance requirements.▪ Expertise in identity and access management, network security, and cloud security.▪ Ability to oversee business continuity, disaster recovery, and crisis management planning.▪ Strong skills in third-party/vendor security assessments and risk management.▪ Experience in conducting security audits, penetration testing, and compliance reviews.▪ Ability to align security initiatives with organizational strategy and digital transformation goals.▪ Capability to train, mentor, and develop information security teams.			