Terms of Reference

Position	Director (ISD)/ Chief Information Security Officer (CISO)
Number of positions	01
Nature of Employment	Contract (03 years) extendable on need & performance basis. The Commission may consider to regularize the position (after three years) subject to meeting the criteria prescribed for this purpose.
Location	Islamabad
Job Summary	Drive the overall Information security program and management system of SECP including but not limited to cyber monitoring, incident management and response, vulnerability management, governance, risk, and compliance.
Duties and Responsibilities	**Security Strategy & Resourcing:** • Understand SECP's business/IT and information security strategy and objectives, and drive information/cyber security innovation, collaboration and continuous improvement; • Establish and maintain the information security strategy to set the vision, direction and scope; • Maximize in-house and outsourced information & cyber security-related services and also establish partnerships with strategic service providers; • Define and maintain the supporting information security operating model, including the key roles and responsibilities (R&R); • Develop and execute the security sourcing strategy for resourcing: employees, contractors, consultants and vendors etc.); and • Coordinate and track the financial requirements, including resources required for the adherence with applicable information / cyber security laws, regulations and adopted standards across SECP and report adherence to the Commission. **Security Governance & Reporting** • Manage and execute security governance structures through defined forums, escalation paths and reporting risks, issues current status to appropriate stakeholders; • Define matrices based on overall business objectives, and report performance status; • Oversee Information security incident management process including but not limited to info/cyber security incident reports, corrective and preventive measures; and • Drive the required coordination within InfoSec department's functions. **Stakeholder Management:** • Manage and coordinate with department heads (HoDs) and stakeholders for both strategic and operational activities to align with SECP's security initiatives; • Align information security & cybersecurity risk management with the enterprise risk management (ERM) and optimize available resources. **Security Adherence:**

	• Oversee adherence to applicable information / cyber security laws, regulations and adopted standards including but not limited to ISO27000, SECP Act., Cyber Crime Act., IOSCO, etc. across SECP; • Oversee reporting on compliance with relevant regulatory standards, policies and local legal requirements. **Sectorial CERT:** • Establish Sectorial-CERT; • Publish Sectorial-CERT's directives, Guidelines, and Advisories; • Oversee adherence with Sectorial-CERT's directives; • Report on compliance with Sectorial-CERT's directives, Guidelines, and Advisories to Government-CERT.
Functional/Technical Competencies	Should have sound knowledge in the fields like: (a) information & cyber/cloud security, (b) enterprise security architectures, (c) frameworks such as: ISO27001/27002 /ITIL /COBIT/NIST etc., (d) governance, risk management & compliance, (e) disaster recovery & business continuity, (f) security assurance & legal/regulatory compliance, (g) privacy & data governance etc. but doesn't have to be the 'hands-on keyboard' type. **Professional Certification:** i. Preferred to have at least two (02) of the listed seven (07) certifications: (a) Certified Information Systems Manager (CISM), (b) Certified Information Systems Security Professional (CISSP), (c) Certified Governance of Enterprise Information & Technology (CGEIT), (d) Certified in Risk and Information Systems Control (CRISC), (e) Certified Information System Auditor (CISA), (f) Certified Chief Information Security Officer (CCISO). ii. Nice to have earned certifications of: (a) Certified Ethical Hacker (CEH), (b) Offensive Security Certified Professional (OSCP), (c) Offensive Security Certified Expert (OSCE), (d) Certified Expert Penetration Tester (CEPT), (e) Certified Cloud Security Professional (CCSP), (f) CISCO Certified CyberOps Professional, (g) Certified Data Privacy Solutions Engineer (CDPSE).
Qualification	• Masters' degree or 04 years bachelor degree (equivalent to 16 years of education) in Cybersecurity, Information Systems and Technology (IS&T), Computer Sciences (CS), Information Technology and Management (ITM), or Digital Forensic Science degree or other related disciplines from a reputed HEC recognized Institute / University. • In addition to above, candidate with MBA degree from a reputed HEC recognized university/Institute will be given preference.
Post Qualification Experience	• At least 15 years of post-qualification experience in related field. ***8-12 years*** *of work experience in both information technology and business concepts, including at least five* ***(05) years*** *in a management role. Proven experience in managing information security risks throughout the data life cycle.*
Age	• Maximum age should not exceed 50 years on the last date of submission of application.
Other Required Skills	• Must have larger bag of non-technical skills such as: (a) ability to lead and influence people in achieving desired goals, (b) analytical problem-solving & negotiation skills, (c) willingness to motivate and support others with mentoring and coaching aptitudes, (d) fluent in written & spoken English and Urdu with exceptional communications skills. Proficient in delivering presentations to senior management.