Terms of Reference

Position	**Joint Director SOC**
Number of positions	01
Nature of Employment	• Appointment shall be made on a contractual basis for a term of three (3) years, extendable based on organizational need and performance. The Commission may consider regularization of this position after completion of three years, subject to fulfilment of the criteria prescribed for this purpose.
Location	• Islamabad
Duties and Responsibilities	• To Lead the Security Operations Centre (SOC) which is a facility to detect, analyse, and respond to cyber security events and incidents using a combination of technology solutions and a strong set of processes. • Responsible for team & vendor management, overall use of resources in 24x7 shifts and initiation of corrective action where required • Creation of regular SOC SOPs/reports, dashboards for SOC operations • Co-ordination with stakeholders, build and maintain positive working relationships with them. • Various stakeholder's management including vendor, principal, senior management and regulated entities with respect to SOC • Build, maintain and continually improve SOC maturity • Establish operational foundations, defining metrics and KPIs to drive governance, quality, and efficiency. • Experience of SOC maturity assessments with various maturity models • Any other task assigned by the Line Manager or HoD
Functional/Technical Competencies	• Ability to handle large SOC teams, work in pressure with 24x7 responsibility • Hands on experience of working in large SIEM / SOAR environment. • Sound knowledge of IT infrastructure and networking. • Good knowledge of Cybersecurity concepts and solutions like Firewalls, DLP, AV/EDR/XDR, IPS/IDS, MDM, IAM, APIs and others. • Certifications & trainings like CHFI/GCIH/CISSP and similar will be an advantage
Qualification	• Master's/Bachelor's degree (equivalent to 16 years of education) in Cybersecurity, Computer Science, Information Technology, Software Engineering, Electrical, Computer, or Telecom Engineering, or related disciplines from an HEC-recognized university/institute.
Experience	• A minimum of 10 years of post-qualification experience in IT, Information Security, or SOC operations, including at least 6 years of experience in SOC operations, of which a minimum of 3 years must be as head of the SOC function.
Age	• The maximum age should not exceed 45 years on the last date of submission of the application.
Other Required Skills	• Proficient in Microsoft Office • Excellent communication skills • Good at analysis and problem solving • Be able to work independently and as a team