PUBLIC PROCUREMENT REGULATORY AUTHORITY (PPRA)
ISLAMABAD

CAREER OPPORTUNITIES

Public Procurement Regulatory Authority (PPRA), Islamabad, a regulatory body established under the PPRA Ordinance, 2002, invites applications from qualified candidates on open merit basis under the e-Procurement Project titled **"e-Pak Acquisition and Disposal System (EPADS)"** for various vacant positions purely on a **"contract basis"** on a market-based competitive remuneration as per the following details. All interested candidates are required to submit online applications through the National Job Portal (NJP) website, i.e., https://njp.gov.pk

Sr. No.	Name of Post	No. of Posts	Job Description:	Minimum Qualification & Experience	Age Limit
1.	**Chief Information Security Officer (CISO)**	01	• Lead PPRA-wide cybersecurity strategy, governance, policies, standards, and security roadmap in accordance with PISF and applicable Government requirements. • Advise senior management on cybersecurity risks, threats, priorities, and overall security posture. • Oversee cybersecurity risk management, incident response, vulnerability management, identity and privileged access security, and security compliance. • Provide security oversight for PPRA applications, data, networks, cloud and local environments, and third-party/managed security services. • Ensure application-level security, secure development practices, security assessments, and timely remediation of identified risks. • Oversee cybersecurity audits, compliance reviews, and security requirements for business continuity and disaster recovery. • Coordinate with relevant Government cybersecurity authorities, regulators, auditors, and service providers, as required. • Report cybersecurity posture, significant risks, and incidents to the Competent Authority and relevant management forums. • Perform any other cybersecurity responsibility assigned by the Competent Authority.	**Qualification:** Minimum MS (18 years of education) in Computer Science, Cyber Security, Information Security, Information Technology, Software Engineering, or Computer Engineering from an HEC-recognized high-ranked university/institution and foreign universities. Higher qualification in the relevant field shall be preferred. **Mandatory Certification:** CISM or CISSP. **Experience:** Minimum 10 years of relevant and verifiable post-qualification professional experience in information/cybersecurity, including at least 5 years in a lead/managerial cybersecurity position.	**55 Years**

Sr. No.	Name of Post	No. of Posts	Job Description:	Minimum Qualification & Experience	Age Limit
2.	**Chief Technology Officer**	01	• Strategic Planning related to Authority's Information Technology needs including computer hardware & software procurement, software licenses, cloud services, network access etc. • Create strategic plans and set timelines for evaluation, development, and deployment of all technical, web, and mobile services. Plan, suggest & make technology initiatives & investments. • Evaluate & assess the technology's impact on current & future business of the Authority. Work with top management and the leadership team to set clear priorities and preferences for IT management. • Ensure tight collaboration across departments to drive strategic initiatives, including understanding of the alignment between technology strategy and various technology road maps. • Defining short-term & long-term IT goals & determine resources to achieve them. • Determine feasibility, devise monitoring mechanism, identify legal aspects, and assess the value, impact, associated risks, competitive & strategic advantage for the IT initiatives. • Develop and manage annual and quarterly budgets. • Ensure sustainable capacity building for the Authority and related stakeholders for achieving the IT goals. • Make infrastructure decisions, ensuring technical excellence, versatility, safety, and soundness, resiliency and scalability in the architecting and engineering of product solutions, as well as managing all technical delivery. • Build quality assurance processes, security policies, user roles, SOPs & data protection mechanisms, disaster recovery plans, effective management & governance. • IT resource allocation, development & monitoring of KPIs and performance metrics to assess technological performance.	**Qualification**: Master's or Bachelor's degree with 16 years of education in information Technology / information Systems / Computer Science / Computer Engineering or related discipline from HEC recognized institution or from a reputed foreign university. **Experience**: Proven experience as a CTO/CEO or Project Manager/Project Director OR similar leadership role in lT (minimum 5 years required). Proven experience in public sector organizations in leadership roles for delivering large scale project with national/provincial level scale, scope & revenue & financial impact (minimum 5 years required). **Skills and Experience** Strategic planning and thinking abilities with a problem-solving aptitude. Leadership and organizational abilities. Excellent communication skills. Competence and solid understanding of broad technology trends, both in software, hardware and infrastructure. Understanding of budgets, project management and business planning. Good understanding of public procurement regulations, rules and guidelines. Team worker with the ability to work collaboratively with cross-functional teams and external partners.	**55 Years**

Sr. No.	Name of Post	No. of Posts	Job Description:	Minimum Qualification & Experience	Age Limit
			• Devise effective Communication technology strategy and relationship management with partners and stakeholders.	Diversified portfolio with a solid understanding of diverse business domains to comprehend and handle all stakeholders and entities for implementing a public procurement regime across the country.	
3.	**Application Security Engineer**	01	• Continuous monitoring and analysis of application logs, database activities, APIs, and user behavior using SIEM and application security tools to identify suspicious or anomalous activities. • Detection, analysis, and response to cybersecurity incidents related to applications, including data breaches, unauthorized data access, and misuse of sensitive procurement and financial information. • Oversight and implementation of application security controls, including secure configuration, role-based access control (RBAC), API security, encryption, and protection of sensitive data such as tender documents and bid securities. • Conducting vulnerability assessments, secure code reviews, and coordinating remediation of application-level and database-related security weaknesses in alignment with OWASP Top 10 standards. • Ensuring secure system integrations with external entities including Banks, AGPR, and other organizational systems at application and data layers. • Supporting secure software operations by coordinating with development and DevOps teams on security requirements, patches, configuration changes, and secure SDLC implementation. • Supporting compliance with applicable laws, rules, regulations, and information security frameworks such as ISO/IEC 27001. • Preparation of application and data security incident reports, audit documentation, compliance reports, and periodic security advisories for management.	**Qualification**: Minimum a Bachelor's degree (16 years of education) in Computer Science, Software Engineering, Information Technology, Cybersecurity, or a related discipline from an HEC-recognized university. **Mandatory certifications:** • CEH (Certified Ethical Hacker) • CISA (Certified Information Systems Auditor) **Experience:** • Minimum of 5 years of relevant and verifiable post-qualification experience in Application Security, Information Security, or SOC operations. • Experience in securing web applications, APIs, databases, and enterprise systems. • Hands-on experience with vulnerability assessment tools, SIEM platforms, and application security testing methodologies (SAST/DAST). • Familiarity with regulatory compliance, audit processes, and security documentation within public sector or enterprise environments.	**40 Years**

Sr. No.	Name of Post	No. of Posts	Job Description:	Minimum Qualification & Experience	Age Limit
			• Participation in security audits, assessments, penetration testing activities, and continuous improvement of application and data security controls. • Any other responsibility or task assigned by the Project Director for ensuring the seamless security of the EPADS Application.		
4.	**Security Compliance Officer**	01	• Coordinate implementation and monitoring of PISF, ISMS and applicable information security policies, standards and regulatory requirements. • Maintain cybersecurity policies, procedures, compliance matrices, risk registers and risk-treatment records. • Coordinate security control assessments, internal/external audits and maintenance of audit/compliance evidence. • Track audit findings, compliance gaps and corrective actions through closure and report status to management. • Monitor third-party and managed-service security compliance against approved contractual and security requirements. • Prepare periodic cybersecurity compliance reports, dashboards and documentation for management and relevant authorities. • Support security awareness, policy compliance and continual improvement of the information security management framework. • Perform any other cybersecurity responsibility assigned by the Competent Authority.	**Qualification:** Minimum a Bachelor's degree (16 years of education) in Cyber Security, Information Security, Computer Science, Information Technology, Information Systems, Software Engineering, or a related ICT discipline from an HEC-recognized high-ranked university/institution and foreign universities. **Preferred Certifications:** ISO/IEC 27001 Lead Implementer and/or ISO/IEC 27001 Lead Auditor, CISA, or equivalent relevant information security compliance/audit certification. **Experience:** Minimum 5 years of relevant and verifiable post-qualification experience, preferably including information security compliance, ISMS, risk assessment, security audits, control assessments, policy/procedure development and audit-evidence management.	**40 Years**
5.	**IT Assistant**	03	• Provide first-level technical and operational support to users of the Electronic Public Procurement System (EPADS) and respond to queries received through the helpdesk. • Assist users in registration, login, profile management, tender publication, bid submission, and other EPADS-related processes. • Troubleshoot and resolve routine system-related issues and escalate	**Qualification**: Bachelor's Degree (14/16 years of education) in Computer Science, Information Technology, Software Engineering, Cyber Security, Data Science/Statistics, or a related qualification from a HEC-recognized university.	**33 Years**

Sr. No.	Name of Post	No. of Posts	Job Description:	Minimum Qualification & Experience	Age Limit
			complex technical matters to the concerned technical team. • Guide procuring agencies, bidders, and other stakeholders on the effective use of EPADS through telephone, email, and other designated communication channels. • Maintain records of user queries, complaints, resolutions, and escalations, ensuring timely follow-up and closure. • Prepare periodic reports on helpdesk activities, recurring issues, and user support requirements. • Perform other IT support and helpdesk-related duties assigned by the competent authority.	Relevant hands-on experience in IT support / Helpdesk will be preferred.	
6.	**IT Technician**	01	• Provide basic technical support to staff and end users and resolve routine IT-related issues. • Install, configure, repair, and maintain computers, laptops, printers, and other IT equipment. • Perform routine hardware and software troubleshooting, including operating system installation, configuration, and updates. • Assist in assembling, disassembling, upgrading, and replacing computer hardware and related components. • Conduct preventive maintenance of IT equipment to ensure smooth and uninterrupted functioning. • Maintain an updated inventory of IT equipment, accessories, and related assets, along with records of repairs and maintenance. • Identify and report recurring technical faults and refer complex issues to the concerned IT personnel. • Perform other IT maintenance and technical support duties assigned by the competent authority.	**Qualification**: i. Minimum Intermediate or equivalent qualification from a recognized Board of Education. ii. Minimum 3-6 months Diploma/Certificate in Information Technology, Computer Hardware, Networking, or a relevant technical field from a recognized institute. iii. Must possess practical knowledge of computer hardware, software installation, operating systems, troubleshooting, and routine maintenance of IT equipment. vi. Relevant hands-on experience in IT support, hardware maintenance, or technical troubleshooting will be preferred.	**30 Years**

Important instruction/information:

1. Applicant(s) should submit their application(s) only through the National Job Portal (NJP). No manual application submissions will be accepted.

2. Only shortlisted/eligible applicants will be called for Test/interview.
3. Applicants may apply for more than one post by submitting separate Application Form for each post.
4. Age relaxation has already been included in the upper age limit.
5. Applicants shortlisted for interview shall present their original educational credentials/testimonials, certifications and experience certificate(s) along with one set of attested copies at the time of interview.
6. Information provided in the Application Form of NJP will be verified, and in case of any false or forged information and fake or bogus documents, the Authority reserves the right to cancel candidature at any stage.
7. Incomplete application will not be entertained.
8. No TA/DA will be admissible for the purpose of Test/interview.
9. The Authority reserves the right to cancel the recruitment process or increase/decrease the position(s) at any stage without assigning any reason.
10. Government employees may apply through proper channel.
11. Candidates having valid Balochistan domicile are encouraged to apply.
12. Application deadline: 20-Nov-26.

HR EXPERT
Public Procurement Regulatory Authority (PPRA),
First Floor, FBC Building, Sector G-5/2, Islamabad.
Phone No. 051-9201850