POST OF SENIOR ICT OFFICER (INFORMATION SECURITY) JG 4, 1 POST (KPC/ADVT/07/2017)

Responsible for the development a risk-based information security culture in the company. Leader of the information security function for KPC, responsible for overall corporate information security strategy, architecture, development and oversight for all utilized security technologies and services, including protection services, perimeter defenses, physical and logical access control, and profile management of all users, contractors and visitors. Enterprise-level responsibility for all data/information security policies, standards, evaluations, roles, and corporate awareness.

Key responsibilities

- Ensuring that a corporate-wide information security program is developed, documented, implemented, and maintained to protect information and information systems.
- Developing, maintaining, and issuing information security policies, procedures, and control techniques to provide direction for implementing the requirements of the information security program. Propose the draft of main information security documents – e.g., Information security policy, Classification policy, Access control policy, Acceptable use of assets, Risk assessment and risk treatment methodology, Statement of Applicability, Risk treatment plan, etc.
- Overseeing personnel with significant/privileged information security responsibilities.
- Establishing minimum mandatory risk based technical, operational, and management information security control requirements for KPC information and information systems. Ensure that all corrective actions are performed.
- Reporting any compliance failure or policy violation for appropriate disciplinary and corrective actions.
- Communicate/Train/Disseminate the benefits of information security companywide. Advise top executives on all security matters
- Report on the results of measuring the security system, propose security improvements and corrective actions, propose budget and other required resources for protecting the information
- Maintain an inventory of all important information assets. Delete the records that are not needed any more. Dispose of media and equipment no longer in use, in a secure way
- Perform risk assessment for activities to be outsourced. Perform background check for candidates for outsourcing partners. Define security clauses that must be part of an agreement.
- Security incidents management - Developing, implementing, and maintaining capabilities for detecting, reporting, and responding to information security incidents, receive information about security incidents, coordinate response to security incidents, prepare evidence for legal action following an incident, analyze incidents in order to prevent their recurrence, review logs of user activities in order to recognize suspicious behavior
- Business continuity - Coordinate the business impact analysis process and the

creation of response plans, Coordinate exercising and testing, Perform post incident review of the recovery plans
- Approve appropriate methods for the protection of mobile devices, computer networks and other communication channels.

Key Qualifications and experience
- Bachelor's degree in Computer Science, electrical/electronic engineering or equivalent.
- CISM or CISSP or CISA or any other relevant security certification is mandatory
- Membership to a relevant professional body is an added advantage.
- Minimum six (6) years post qualification experience in Information Security.

Key competencies
- Comprehensive knowledge and understanding of oil industry requirements including broad knowledge of international trends in auditing and corporate governance.
- Strong well developed written and verbal communication, intense concentration of mental and interpersonal skills including ability to conduct computerized audits/investigations and prepare relevant and quality reports
- Flexibility and responsiveness in handling and determining complaints, sound analytical skills and the ability to identify with precision the critical factors of a problem in an impartial and objective way
- Ability to maintain confidentiality of privileged information and to ensure absolute discretion and sensitivity to confidential matters
- Ability to solve complex and outstanding technical and administrative problems by generating alternative workable solutions
- Ability to deliver corporate articulated vision for change, create sense of urgency around change and motivate staff to join change effort.
- Excellent interpersonal skills and ability to manage staff of different orientation.