DEPARTMENT OF PUBLIC ENTERPRISES

APPLICATIONS: The Department of Public Enterprises, Private Bag X15, Hatfield, 0028 or hand deliver at 80 Hamilton Street, Arcadia, Pretoria 0001, or by email stated under each post

FOR ATTENTION: Human Resources

CLOSING DATE: 06 April 2021

NOTE: Applications must be submitted on form Z83 and should be accompanied by certified copies of qualifications, ID as well as a comprehensive CV in order to be considered. It is the applicant’s responsibility to have foreign qualifications evaluated by the South African Qualification Authority (SAQA). Correspondence will be limited to successful candidates only. If you have not been contacted within 3 months after the closing date of this advertisement, please accept that your application was unsuccessful. Shortlisted candidates will be subjected to screening and security vetting to determine the suitability of a person for employment. Failure to submit the requested documents will result in your application not being considered. All shortlisted candidates for SMS posts will be subjected to a technical exercise and competency assessment. A pre-entry certificate obtained from National School of Government (NSG) is required for all SMS applications. The department reserves the right not to fill these positions. People with disabilities are encouraged to apply and preference will be given to the EE Targets of the Department.

MANAGEMENT ECHELON

POST 10/55: DIRECTOR: SECURITY AND FACILITIES MANAGEMENT REF NO: DPE/2021/001
Branch: Corporate Services

SALARY: R1 057 326 per annum (Level 13), An All-inclusive remuneration package consisting of a basic salary of 70% and a 30% flexible portion that can be structured according to the individual’s personal needs.

CENTRE: Pretoria


DUTIES: Facilitate the implementation of the MISS and MPSS in the Department. Monitor departmental compliance with the standards set out in the MISS and MPSS and facilitate the implementation of corrective action. Develop the departmental security risk register and recommend mitigation strategies. Conduct preliminary investigations. Develop and facilitate the implementation of the departmental master security management plan. Manage processes to ensure a safe working environment for employees and visitors. Manage the provisioning of VIP security services in line with the diplomatic protocols. Manage the provisioning of events security services in line with SLA requirements and facilitate corrective action. Liaise with security agencies on security threats and arrangements for the security detail of political office bearers. Provide early warning and security contingency planning advisory services to executive management. Investigate security breaches and report thereon, inclusive of reporting to the relevant security agency. Provide security assistance in liaison with SOCs Administer vetting services. Liaise with the National Security Agency and administer employee vetting processes. Provide technical support to establish the departmental security level regime. Manage the Service Level Agreement with the Landlord. Manage the provisioning of reception and switchboard services. Manage the provisioning of housekeeping services, provision of plants, water and the maintenance of the building; inclusive of all matters related to the provisioning of a healthy working environment for employees and compliance with Occupational Health and Safety Act imperatives. Manage the provisioning of Office space. Identify
and manage the financial, human and equipment resources of the Programme required to optimally support the implementation of the Unit’s Annual Performance Plan. Represent the strategic intent of the Programme as part of internal resource allocation processes. Manage and account for the utilisation of the financial resources of the Programme in line with the departmental delegations. Monitor, evaluate and account for the effective and efficient utilisation (value for money) of allocated resources. Direct, manage and account for the utilisation of the Unit’s human resources. Direct the utilisation of technology in support of the Unit’s business processes.

ENQUIRIES: Mr Benneth Baloyi Tel No: (012) 431 1029 e-mail: recruitbb@dpe.gov.za

POST 10/56: DIRECTOR: INFORMATION TECHNOLOGY (GITO) REF NO: DPE/2021/002
Branch: Corporate Management

SALARY: R1 057 326 per annum (Level 13). An All-inclusive remuneration package consisting of a basic salary of 70% and a 30% flexible portion that can be structured according to the individual’s personal needs.

CENTRE: Pretoria

REQUIREMENTS: Degree in Computer Science or Information Systems/Technology (NQF Level 7) as recognised by SAQA accompanied by minimum of 5 years’ experience of middle/ senior management. Sound knowledge of multiple IT platforms/ disciplines (ie Operating Systems, IT facilities, IT Infrastructure, Knowledge Information Management). Disaster Recovery Planning and management abilities. Exposure to Content Management and Enterprise Resource Planning Systems will be an added advantage. Strong Communication, Customer management, Financial Management, Interpersonal skills and conflict management. IT Project, Analytical and Decision making skills. Business Analysis experience to ensure implementation of business decisions. Sound knowledge of Information Technology Infrastructure Library (ITIL), Cobit and TOGAF standards.

DUTIES: Align the Department’s information management (including information management systems) and information technology strategy (as enabler) with the strategic direction, management plans and business processes of the Department. Support the head of department, senior management and the other users in the department in the efficient and effective utilisation of information and information technology as strategic resources to enable them to execute their functions efficiently and effectively. Manage the information technology function of the department and to ensure the establishment of sound information management systems. Establish an information plan, information technology and operational plans to give effect to the strategic direction and management plans of the Department. Develop an annual business plan and operating budget for the unit and monitor the implementation of these to ensure that business and financial targets are met. Develop departmental supporting information technology enabler policies and strategies, regulations, standards, norms, guidelines best practices and procedures. Facilitate the implementation of and adherence to the policies and strategies contained in the different plans and policies to ensure governance standards are met in the department. Promote effective management of information technology as enabler as strategic resources. Promote proper governance of ICT. Create and enabling environment for other managers to perform their functions more effectively and efficiently. Control the business agreement (BA) and service level agreements (SLAs) with SITA and/or other suppliers of information management and information technology goods and services. Utilisation of security mechanisms and ensure compliance to the relevant regulatory framework. Represent the Department at the GITO Council. Develop, implement and maintain the Risk Management strategy, as well as address risks faced by the Department.

ENQUIRIES: Mr George Malatsi Tel No: (012) 431 1117 e-mail: recruitgm@dpe.gov.za

OTHER POST

POST 10/57: ASSISTANT DIRECTOR: INFORMATION SYSTEMS AND NETWORK SECURITY OFFICER REF NO: DPE/2021/003
Branch: Corporate Management

SALARY: R376 596 per annum (Level 09)

CENTRE: Pretoria

REQUIREMENTS: Applicants must be in possession of an appropriate undergraduate qualification in Information Technology at NQF level 7 accompanied by at least 3 years’ appropriate experience at operational level. The following will be added
advantage: Cisco Certified Network Professional (CCNP), Professional Information security certification (Certified Information System Security Professional (CISSP), Certified Ethical Hacker (CEH), and ISO 27001). Excellent written and verbal communication skills. Ability to work on own initiative and as part of a team. Numerate, able to learn and assimilate new information. Commitment to working the hours required to fulfil the job, including flexibility of working. Solid knowledge of various information security frameworks. Excellent problem-solving and analytical skills. Ability to educate a non-technical audience about various security measures. Be highly analytical and effectively able to troubleshoot and prioritize needs, requirements and other issues. Keeping up to date with developments in IT security standards and threats and be committed to continuous learning and system development.

DUTIES:
Perform daily infrastructure and network monitoring, verifying the integrity and availability of all hardware, server resources, systems and key processes, reviewing system and application logs, and verifying completion of scheduled jobs such as backups. Perform regular security monitoring to identify any possible intrusions. Develop and maintain information security policy and procedures. Assess the infrastructure and information systems to identify vulnerabilities caused by weaknesses or flaws in software and hardware that could expose the infrastructure to security breaches. Evaluate the effectiveness of existing security measures, such as firewalls, password policies and intrusion-detection systems. Make recommendations to improve security based on the assessments and knowledge of current and emerging threats. Monitor network usage to ensure compliance with security policies. Perform penetration tests to find any defects. Collaborate with management and the IT department to improve security. Review Enterprise Information Security Policy which includes ICT Network Security, Application Security, Databases Security, Mobile Device Security, Bring Your Own Device, Enterprise Information Security, Patch Management, IT continuity and disaster recovery plan. Provide Tier III/other support per request. Troubleshoot and resolve complex software, hardware and related network problems. Apply OS patches and upgrades on a regular basis, and upgrade administrative tools and utilities. Perform regular security monitoring to identify any possible intrusions. Ensure implementation of security systems and solutions to monitor security across all corporate networks, computers and storage devices, to quickly identify attacks and respond to any alerts. Reinforce the importance of information security through training and awareness programs for employees.

ENQUIRIES:
Ms Dineo Masilo Tel No: (012) 431-1026 email: recruitdm@dpe.gov.za