

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.

POST / ASSISTANT DIRECTOR: INFORMATION SYSTEMS AND NETWORK SECURITY OFFICER, REF. NO DPE/2021/003

BRANCH: Corporate Management

SALARY: R376 596.00 per annum (Level 9)

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, Telephone (012) 431-1026

email: recruitdm@dpe.gov.za