**ANNEXURE G**

**INDEPENDENT POLICE INVESTIGATIVE DIRECTORATE**

***The Independent Police Investigative Directorate (IPID) is an equal opportunity and affirmative action employer. It is our intention to promote representatively in terms of race, gender and disability within the Department through the filling of posts.***

| | | |
|---|---|---|
| **APPLICATIONS** | : | Independent Police Investigative Directorate, National Office Private Bag X941, Pretoria, 0001 or hand deliver to Benstra Building, 473 Stanza Bopape & Church Street, Arcadia, Pretoria, or email recruitment10@ipid.gov.za (Please indicate the post name and reference number on the subject line) when applying through e-mail. |
| **FOR ATTENTION** | : | Mr. DS Baloyi Tel No: (012) 399 0202 |
| **CLOSING DATE** | : | 28 November 2025 |
| **NOTE** | : | Applicants are not required to submit copies of qualifications and other relevant documents on applications but must submit Z83 and a detailed Curriculum Vitae. Applications quoting the correct reference number must be submitted on the new form Z83, obtainable from any Public Service Department or on the internet at www.gov.za/documents . Received applications using the incorrect application form (old Z83) will not be considered. Each application for employment form must be fully completed, signed and initialled by the applicant. Failure to sign this form may lead to disqualification of the application during the selection process. A recently updated, comprehensive CV as well as a fully completed and initialled new signed Z83 (Section A, B, C & D are compulsory and section E, F and G are not compulsory if CV it is attached). However, the question related to conditions that prevent re-appointment under Part-F must be answered. Non-RSA Citizens/Permanent Resident Permit Should you be in possession of a foreign qualification; it must be accompanied by an evaluation certificate from the South African Qualification Authority (SAQA) (only when shortlisted). All shortlisted candidates for SMS posts will be subjected to a technical competency exercise that intends to test relevant technical elements of the job, the logistics of which will be communicated by the Department. Applicants who do not comply with the above-mentioned requirements, as well as applications received late, will not be considered. Due to the large number of applications we envisage to receive, applications will not be acknowledged, if you have not been contacted within three (3) weeks after the closing date of this advertisement, please accept that your application was unsuccessful. Correspondence will be limited to short-listed candidates only. Therefore, only shortlisted candidate for the post will be required to submit the documents on or before the date of the interview. The successful candidate will have to undergo security vetting. His / her character should be beyond reproach. The appointment is subject to security clearance, verification of qualifications and competency assessment (criminal record, citizenship, credit record checks, qualification verification and employment verification). The Department reserves the right to fill or not fill the any advertised posts. Applicants must declare any pending criminal, disciplinary or any other allegations or investigations against them. Should this be uncovered during / after the interview took place, the application will not be considered and in the unlikely event, that the person has been appointed such appointment will be terminated. The successful candidate will be appointed subject to positive results of the security vetting process. All applicants are required to declare any conflict or perceived conflict of interest, to disclose memberships of Boards and directorships that they may be associated with. The successful candidates will be appointed on a probation period of 12 months and will be required to sign a performance agreement. The suitable candidate will be selected with the intention of promoting representivity and achieving affirmative action targets as contemplated in the Department's Employment Equity Plan. |

**OTHER POST**

| | | |
|---|---|---|
| **POST 42/77** | : | **ASSISTANT DIRECTOR: ICT SECURITY REF NO: Q9/2025/74** |
| **SALARY** | : | R468 459 per annum |
| **CENTRE** | : | National Office |
| **REQUIREMENTS** | : | An NQF level 7 qualification in ICT as recognized by SAQA or related field. 3-5 years' working experience in ICT security management. Knowledge Requirements: Knowledge and understanding of government |

regulations/prescripts/policies. Knowledge and understanding of departmental policies relating to ICT. Knowledge of Firewall systems. Knowledge on network monitoring tools. Knowledge and understanding of DMZ Zone. Knowledge of ICT audit including server room compliance standards, Knowledge of Hacking/penetration test. Knowledge of different software systems and components. Knowledge of software and hardware configurations. Knowledge of desktop, server hardware and software. Ability to evaluate documentation. Knowledge of software application systems. Knowledge of back-up and recovery systems. Knowledge of disaster recovery testing and business continuity. Understanding if ICT network infrastructure and other related matters. Skills and Competencies: Excellent written and oral communication skills. Demonstrated customer service skills and focus. Proven ability to manage multiple tasks and projects. Ability to think and act tactically. Interpersonal skills. Project management skills. Troubleshooting skills. Presentation Skills. Skill to analyse and evaluate systems, data, etc.

**DUTIES** : Coordinate ICT Security operations: Administer and monitor firewall activities, provide monthly and quarterly reports, Monitor ICT security compliance with departmental policies, procedures and prescripts, Monitor the Demilitarized Zone (DMZ) on the network and generate reports. Administer and monitor user activity on the network and reporting any violations. Protect data and system integrity: Conduct network penetration and detection/prevention tests and submit monthly reports. Conduct back-ups testing for integrity and restore purposes. Verify that all systems and equipment on the Disaster Recovery (DR) site are updated in line with the Disaster Recovery Plan (DRP). Verify that archiving of emails is properly conducted for both outgoing and incoming communications. Update software and hardware systems and equipment at the DR site. Conduct ICT security risk and Compliance: Identify and report on ICT security risks and threats and escalate complicated matters. Compile monthly and quarterly reports. Identify information assets (ICT Systems), potential threats and vulnerability. Evaluate ICT systems quarterly (software & hardware) and submit reports. Conduct market research and benchmarking on ICT security Technologies to improve services and submit reports. Document all ICT security –related changes on system/networks and implementation. Provide ICT security input for network upgrades, design and installations. Respond to security related queries and solve them. Implement systems and conduct Application Testing: Publish approved projects to the web application for processing and implementation. Test new software and applications before deployment to ensure compliance. Certify software and hardware before installation or implementation. Manage resources and Record-keeping: Conduct maintenance and awareness campaigns on ICT security matters. Update all ICT security equipment and software records in registers. Verify equipment and software for disposal to ensure compliance with policies and prescripts.

**ENQUIRIES** : Mr. T Moletsane Tel No: (012) 399 0016