

## NATIONAL DEPARTMENT OF HEALTH

*It is the Department's intension to promote equity (race, gender and disability) through the filing of this post with a candidate whose transfer /promotion / appointment will promote representivity in line with the numeric targets as contained in our Employment Equity plan.*

**APPLICATIONS:** The Director-General, National Department of Health, Private Bag X399, Pretoria. 0001. Hand delivered application may be submitted at Reception (Brown Application Box), Dr AB Xuma Building, 1112 Voortrekker Rd, Pretoria Townlands 351-JR or should be forwarded to recruitment@health.gov.za quoting the reference number on the subject e-mail

**FOR ATTENTION:** Ms M Shitiba

**NOTE:** All short-listed candidates will be subjected to a technical exercise that intends to test relevant technical elements of the job, the logistics of which will be communicated by the Department. Following the interview and technical exercise for SMS posts, the selection panel will recommend candidates to attend a generic managerial competency assessment (in compliance with the DPSA Directive on the implementation of competency-based assessments). The competency assessment will be testing generic managerial competencies using the mandated DPSA SMS competency assessment batteries. Applications should be submitted on the new Z83 form obtainable from any Public Service department and should be accompanied by a CV only (previous experience must be comprehensively detailed). The Z83 must be fully completed (in line with DPSA Practice note), failure to comply will automatically disqualify the applicant. Applicants are not required to submit copies of qualification and other relevant documents on application. Certified copies of qualifications and other relevant documents will be requested prior to the final selection phase. Applications should be on one PDF format (If emailed). Applications received after the closing date and those that do not comply with the requirements will not be considered. It is the applicant's responsibility to have foreign qualifications and national certificates (where applicable) evaluated by the South African Qualification Authority (SAQA). Please note by responding to the advertisement, you consent to the collection, processing, and storing of your Personal Information in accordance with the Protection of Personal Information Act (POPIA). Your information will be used solely for the purpose of this promotion and will not be shared with third parties without prior consent unless required by law. The Department reserves the right not to fill the posts. The successful candidate will be subjected to personnel suitability checks and other vetting procedures. Applicants are respectfully informed that correspondence will be limited to short-listed candidates only. If notification of an interview is not received within three (3) months after the closing date, candidates may regard their application as unsuccessful. The Department will not be liable where applicants use incorrect/no reference number(s) on their applications.

**POST** : **DEPUTY DIRECTOR: ICT SECURITY (REF NO: NDOH 27/2026)**

**SALARY** : An all-inclusive remuneration package of R896,436 per annum [basic salary consists of 70% or 75% of total package], salary package will be structured according to Middle Management Service guidelines.

**CENTRE** : Directorate: Information Communication Technology, Pretoria.

**REQUIREMENTS** : A Grade 12 certificate and NQF 7 qualification in Information Technology/ Information Security or Computer Systems as recognized by SAQA. ITIL foundation and COBIT certification and any accreditation (Security+, CISA, CISSP, CISM, CRISK) will be an advantage. At least three (3) years' of IT experience as Assistant Director or equivalent level as well as supervisory experience. Experience in an Information Security role, in working with legal audit and compliance staff, developing and maintaining policies, procedures, standards and guidelines as well as experience in information security management frameworks, such as International standards Organization (ISO) 2700x/ the IT Infrastructure Library (ITIL) / Control Objectives for Information & Related Technology (COBIT) frameworks. Knowledge of ICT Governance,

Risk, Security, Compliance and Continuity methodologies and practices, IT Infrastructure Lifecycle Management and ICT Networks (LAN & WAN technologies). Knowledge of ICT Controls and ICT System Development, Backup, Restore, Disaster Recovery and Archiving. Knowledge and understanding of relevant legal and regulatory requirements, such as DPSA Corporate Governance of ICT Policy Framework, Cloud Security Policy, Government Wide Enterprise Architecture etc. Knowledge/Certification on COBIT methodology. Knowledge of ISO 27000 standard, ISO 22301, ISO 38500 and ISO 31000 will be an added advantage. Good communication (verbal and written), analytical, project management, policy development, people management, problem solving and decision making, planning and organizing and computer skills (MS office package). A valid driver's license.

**DUTIES**

: Provide strategic support in alignment with business goals and management of resources. Develop, implement, and monitor a strategic, comprehensive departmental information security and IT risk management program to ensure that the integrity, confidentiality, and availability of information is owned, controlled or processed by the department. Provide ICT security support and maintain compliance with security standards and minimizing of risks. Manage outsourced vendors that provide information security functions for compliance with contracted service-level agreements. Provide architecture/engineering support in designing, implementing, and maintaining robust, scalable, and secure systems. Consult with IT and security staff to ensure that security is factored into the evaluation, selection, installation and configuration of hardware, applications and software. Provide security liaison role by ensuring that security policies, compliance, and risk management are integrated into all ICT activities. Assist resource owners and IT staff in understanding and responding to security audit failures reported by auditors. Manage personnel and various security initiatives/projects to ensure alignment with organizational goals, compliance, and audit.

**ENQUIRIES**

: Mr A Mabuza at tel no: 012 395 8647

**CLOSING DATE**

: 15 April 2026