Are you smart? Professional? Efficient? Effective? Passionate about your work?

The Government Pensions Administration Agency (GPAA) is a government component which reports to the Minister of Finance and administers funds and schemes on behalf of the National Treasury and the Government Employees Pension Fund (GEPF), the largest pension fund in Africa. It thus administers the pension affairs of approximately 1,7 million government employees and those of pensioners, spouses and dependants.

To meet the needs of our changing client base, the GPAA is modernising. In order for this modernisation to be effective, we are looking to bring bright and enthusiastic professionals from all disciplines of life, who are interested in contributing towards positive change, into our fold. If this is you, please apply for the post, detailed below:

ONE PERMANENT POSITION OF DIRECTOR: INFORMATION SECURITY MANAGEMENT IS CURRENTLY AVAILABLE WITHIN THE ICT BUSINESS UNIT AT THE GPAA

DIRECTOR: INFORMATION SECURITY MANAGEMENT

INFORMATION COMMUNICATION TECHNOLOGY

HEAD OFFICE (PRETORIA) ● Ref: DIR/IS/2026/01-1P

ALL-INCLUSIVE PACKAGE: R1 266 714 – R1 492 122 P.A. - LEVEL 13 (PERMANENT)

ROLE PURPOSE: Effectively manage the information security management service.

KEY RESULT AREAS:

The incumbent will be responsible for a wide variety of tasks which includes but are not limited to the following:

Manage the implementation of the Information Security Management strategy:

- Monitor the implementation of the operational plan for the Directorate to support the achievement of GPAA's strategic objectives
- Manage, monitor and review the Directorate policies, procedures and processes, in accordance with best practice and legislation
- Compliance and reporting in line with ISO/IEC 27001 and the applicable DPSA directive
- Manage the implementation of an effective short, medium and long-term operating strategy for the Directorate
- Conduct benchmarks on new developments in practices to improve the effectiveness and efficiency of the organisation
- Manage the provision of best practice regarding Directorate functions to all stakeholders.
- Manage the implementation of a management effectiveness and leadership strategy
- Engage in strategic relationships with relevant stakeholders to serve the interest of the organisation
- Monitor compliance with relevant legislation throughout all Directorate functions
- Analyse service delivery gaps, challenges and implement remedial action strategies
- Manage quality of service provided to internal and external customers / clients / stakeholders
- Manager the mitigation of identified risks
- Ensure information flow to and alignment with all stakeholders to ensure effective engagement
- Conduct trends analyses and forecasting.

Manage the Security of Organisational information:

- Collaborate with relevant internal and external stakeholders to identify, monitor and manage Information Security risk proactively
- Develop and manage the implementation of appropriate mitigation strategies to achieve stipulated objectives
- Ensure that GPAA is appropriately protected against unforeseen events, losses and damage, to recover Information Infrastructure where required
- Conduct operational risk assessments for the Information Security department, in line with the GPAA's risk management framework, to develop and maintain adequate internal operations controls and standards.

Oversee the operations of the business unit:

- Assess the provision of Information Security Management support and advice to line managers to ensure that line managers are fully equipped to deal with Information Security Management strategy related matters
- Drive a culture of compliance with GPAA line managers and staff to ensure greater awareness of Information Security Management policies and procedures
- Monitor compliance with relevant legislation throughout all Information Security Management functions
- Manage planning of resource requirements for the organisation to ensure sufficient resources are in place to meet service delivery demands
- Analyse service delivery gaps and challenges, define service delivery operational measures and targets, and implement remedial action strategies
- Oversee quality of service provided to internal and external customers / clients / stakeholders.
- Proactive identification and mitigation of risk.
- Establish and manage agreed budgets in consultation with the Chief Information Technology Officer and Budget Office, ensuring that costs are contained based on minimum requirements for security controls
- Manage, coordinate and oversee the daily operational activities of the subunit to ensure that it functions effectively and efficiently.
- Proactively mitigate employee relations risks
- Ensure information flow to and alignment with all stakeholders to ensure effective engagement.

Manage and facilitate business partnering:

- Assist line managers to prepare business cases and budgets for new projects relating to provision of organisational information, motivating project viability and value to the GPAA
- Provide Information Security support and advice to the Technology COE with regard to relevant IT solutions or problems raised by managers.
- Contribute to Client meetings, demonstrating Information Security capability when required.
- Establish sound working relationships with various third-party service providers, monitoring achievement of agreed service levels.

Manage and develop the capacity requirements plan:

- Perform Information Security budget and expenditure reconciliations for the Technology COE to ensure prudent financial management of the department.
- Assist Technology COE to develop and report on cost of Information Security per employee to optimise and manage cost of service provided
- Motivate for additional financial and staff resources to meet business requirements
- Assess IT infrastructure requirements so that Information Security processes and procedures run smoothly
- Manage third party contracts sufficiently to ensure maximum return of benefits to the organisation.

Continuously manage the improvement of processes and procedures:

- Track new developments in the industry to improve the effectiveness and efficiency of the Information Security function in the GPAA
- Identify areas of improvement to meet organisational needs
- Formulate process and technological improvement solutions to enhance efficiencies
- Work in conjunction with relevant departments to implement changes, providing and integrated service
- Manage project implementation evaluating progress in terms of set objectives.
- Execute IS governance requirements to ensure compliance with best practices.

Manage all the resources in the Directorate:

- Ensure the development and management of staff within the Directorate
- Implement and maintain a relevant management approach to support effective business results within the Directorate
- Develop and sustain a culture of high performance, professionalism and integrity to support overall quality of service delivery
- Ensure control of budgeting and expenditure process in line with strategic objectives and relevant legislation
- Ensure the effective utilisation of all resources (including IS, Assets, Infrastructure, etc.) within the Directorate.

QUALIFICATIONS AND EXPERIENCE:

- A relevant degree / BTech in Computer Science / Information Technology / Cyber Security (NQF level 7) or equivalent qualification as recognised by SAQA with 5 years' experience in middle / senior management level in Performing IT management or cyber security with a strong background in incident management, risk management and security architecture
- Computer literacy which includes a good working knowledge of Microsoft Office products.

KNOWLEDGE AND COMPETENCIES:

- Knowledge of Benefits administration
- Knowledge of relevant Legislative requirements and GPAA policies and procedures.
- Industry knowledge
- Knowledge of Financial management including budgeting and forecasting
- Knowledge of Pension Fund regulations and rules
- Strategic capability and compliance management
- Knowledge of relevant systems
- Cloud and wireless security
- Security frameworks, standards and technologies
- Programme, risk and project management
- People management and empowerment
- Compliance frameworks and controls best practices
- Anti-virus, anti-spam, internet filtering and patch management tools
- Intrusion detection/prevention systems
- System technology security testing (vulnerability scanning and penetration testing)
- Documenting security architecture and plans
- Service excellence
- Respect, integrity, transparency and courtesy.

#DISCLAIMER

- **It is mandatory to email your application (comprehensive CV and new Z83, duly completed and signed) to Recruit1@gpaa.gov.za quoting the reference number in the subject heading of the email (failure to adhere to this will result in application/s being declined.**
- **Applicants are encouraged to attach supporting documentation such as ID, all qualifications and driver's license (where applicable) – no need to be certified, as this assists in the turnaround time of the recruitment process**
- **For salary levels 11 – 15, the inclusive remuneration package consists of a basic salary, the State's contribution to the Government Employees Pension Fund and a flexible portion in terms of applicable rules.**
- **Senior Management Service (SMS) applicants will be required to undergo a Competency Assessment as prescribed by DPSA.**
- **All candidates shortlisted for SMS positions will be required to undergo a technical exercise which intends to test the relevant technical elements of the job.**
- **One of the minimum requirements for SMS is the pre-entry certificate for SMS (Nyukela). For more details on the pre-entry course visit: https://www.thensg.gov.za/training-course/sms-pre-entry-programme/**

Closing date: 30 January 2026 before 12h00 noon. No late applications will be accepted.

Contact persons: Enquiries may be directed to Felicia Mahlaba on 012 319 1455.

TAKE NOTE OF THE DISCLAIMER MENTIONED ON EACH ADVERT. It is mandatory that applications which consist of a signed Z83 and comprehensive CV be emailed to the respective email addresses indicated on each advert. Ensure that you use the correct inbox/email. Applications send to the incorrect inbox will be deemed a regret. Ensure to sign your Z83 before you scan it. Please use your signature or valid e-signature and not your name written in block/typed print. A Z83 not signed will be deemed a regret. From 1 January 2021, a new application for employment (Z83) form will be effective and if the old Z83 is used, it will be deemed a regret. Should an individual wish to apply for a post after 1 January 2021, he/she will be required to submit the new application for employment form which can be downloaded at www.dpsa.gov.za-vacancies or http://www.gpaa.gov.za Requirements: Applications must be submitted on the new form Z83 as indicate above (signed and scanned). The relevant reference number must be quoted on all documentation and on the subject heading of the email. An application should consist of (a) a comprehensive and detailed CV (specifying all experience and duties, indicating the respective dates MM/YY as well as indicating references with full contact details) and (b) a duly completed Z83 (refer to Circular No 19 of 2022 in this regard) only. Failure to submit the above documents will result in the application not considered and deemed a regret. The candidate must agree to the following: Shortlisted candidates must avail themselves for a virtual or in-person panel interview at a date and time determined by the GPAA. Note that certain information contained in the application (CV and Z83) may be verified through the request for official documents and or other methods of verification and proof (when shortlisted). The certification of all supporting documents will be expected of the shortlisted candidates only. Applicants must note that pre-employment checks and references will be conducted once they are short-listed and the appointment is also subject to a positive outcome on these checks, which include but not limited to: security clearance, security vetting, qualification/study verification, citizenship verification, financial/asset record check, previous employment verification and criminal record. Applicants will be required to meet vetting requirements as prescribed by Minimum Information Security Standards. It is the applicant's responsibility to have foreign qualifications evaluated by the South African Qualifications Authority (SAQA). Correspondence will only be conducted with the short- listed candidates. If you have not been contacted within six (6) months after the closing date of this advertisement, please accept that your application was unsuccessful. The candidate must take note of: It is the GPAA's intention to promote equity (race, gender and disability) through the filling of this post(s) with a candidate whose transfer / promotion / appointment will promote representativeness in line with the numerical targets as contained in GPAA's Employment Equity Plan. For applications on salary levels 11 – 15, the inclusive remuneration package consists of a basic salary, the state's contribution to the Government Employees Pension Fund and a flexible portion in terms of applicable rules. SMS will be required to undergo a Competency Assessment as prescribed by DPSA. All candidates shortlisted for SMS positions will be required to undergo a technical exercise that intends to test the relevant technical elements of the job. One of the minimum requirements for SMS is the pre-entry certificate. For more details on the pre-entry course visit: https://www.thensg.gov.za/training-course/sms-pre-entry-programme/ The GPAA reserves the right to utilize practical exercises/tests/competency assessments for non-SMS positions during the recruitment process (candidates who are shortlisted will be informed accordingly) to determine the suitability of candidates for the post(s). The GPAA reserves the right to cancel the filling/not to fill a vacancy that was advertised during any stage of the recruitment process. The successful candidate will have to sign and annual performance agreement and will be required to undergo a security clearance.

the gpaa

Department:
Government Pensions Administration Agency
REPUBLIC OF SOUTH AFRICA

| YOUR BENEFITS our responsibility |