NATIONAL PENSION SCHEME AUTHORITY

EMPLOYMENT OPPORTUNITIES

The National Pension Scheme Authority (NAPSA) wishes to fill the positions indicated below. Interested applicants who meet the required competences are encouraged to apply.

The successful candidates will be expected to have demonstrable competencies relevant to the respective job.

1.0 Security Analyst - Infrastructure NC06 (One Year Contract): Head Office

1.1 Main Purpose of Job

The Security Analyst – Infrastructure is responsible for the development and implementation of the IT Security Strategy (covering Access Control, Email Security, Firewalls, Intrusion Detection Systems, Malware, Network Access Control, Vulnerability Scanning, Security Audit, Spyware, enterprise BCP and VPN) at NAPSA to ensure the availability of a safe IT platform from which to manage member funds. Additionally, the position coordinates the implementation of the section work plan to ensure the activities of the section are aligned with the strategy of the section.

.

1.2 Key Responsibilities

a) Design, implement and maintain IT security infrastructure and systems that integrate capabilities and technologies to address identified risks and enable strategic and/or tactical IT solutions that enable the business
b) Ensure the Authority's ICT infrastructure and Networks security program is delivered in line with the Approved Strategy.
c) Monitor and resolve incidents/problems within the Security infrastructure to ensure stability and availability to the Enterprise
d) On a periodic basis, extract and review existing User access control lists to all the servers and Network devices, and ensure compliance with the set standards

e) Implement and regularly update Access control and Bring-Your-Own-Device (BOYD) policies to provide guidance on the conduct of NAPSA staff in the utilisation of IT facilities for enhanced security.
f) Analyze architectural requirements, design and implement infrastructure that allows enablement of specific capabilities, solutions, or preventative/remediation controls to protect sensitive data and systems in accordance with industry standards and governance/compliance requirements
g) Ensure that endpoint devices are always up-to-date with the latest security patches
h) Research/investigate emerging IT Infrastructure security topics such as new threats, capabilities as well as explore possible solutions. This should lead to the creation or updating of policies, technology strategies, solution architecture, and vulnerability assessments done by the Authority to ensure the approach employed delivers the desired objectives.
i) Apply industry standard risk management techniques and knowledge across various capabilities to determine the effectiveness of the deployed security infrastructure/products and to create action plans that remediate identified risks
j) Conduct periodic information Security awareness to all members of staff
k) Ensure a secure business environment and protection of stakeholder value through ensuring availability, integrity and confidentiality of networks and IT Infrastructure as required by the business
l) To perform and coordinate log management through the Security events and information management (SIEM).
m) Security tool administration and support (Network/Endpoint/Threat Hunting/Investigations)
n) Report and track any security breaches detected on the Network or systems
o) Regularly review the security posture of the IT Infrastructure under the Information Technology department
p) Review and update security policies as directed by the line manager
q) Perform IT Risk assessments and report on existing/new systems
r) Maintain IT Disaster Recovery Plan and facilitate all DR planning and testing in liaison with the line manager
s) Conduct in-house vulnerability assessment of the Authority's ICT Infrastructure
t) Perform in-house quarterly Penetration Tests on the Authority's ICT Infrastructure
u) Maintain Perimeter and Inner Firewall rules and ensure they are operational at all times

1.3 Qualifications and Experience

- Grade 12 Certificate with 5 'O' levels with credit or better including Mathematics and English;
- Bachelor's Degree in Computer Science or equivalent;
- Should possess **any** of the following certifications; Cisco Certified Network Professional (CCNP) or equivalent, Certified Information Systems Security Professional (CISSP), Certified Ethical Hacker or any other relevant IT Security Certification;
- Not less than three (3) years of relevant IT experience at a similar level in an organisation of similar size.

2.0 Security Analyst - Applications NC06 (One Year Contract): Head Office

2.1 Main Purpose of Job

The Security Analyst - Applications is responsible for the development and implementation of the IT Security Strategy (covering Systems Access Control, Vulnerability Scanning, Security Audit, Application Security and enterprise BCP) at NAPSA to ensure the availability of a safe IT platform from which to manage member funds. Additionally, the position coordinates the implementation of the section work plan to ensure the activities of the section are aligned with the section strategy, and that quality standards and timelines are observed.

.

2.2 Key Responsibilities

a) Identify security shortcomings in the NAPSA application systems and recommend appropriate policies to ensure best practices and standards are complied with.
b) Report and track any security breaches on the Systems Applications
c) Regularly review security posture of all the Applications Systems under the Information Technology department
d) Review and update security policies as directed by the line manager
e) On a periodic basis, extract and review existing users access control lists from all systems
f) Perform IT Risk assessments and report on existing/new application systems
g) Maintain IT Disaster Recovery Plan and facilitate all DR planning and testing of applications systems in liaison with the line manager
h) Conduct periodic reviews on all installed Systems to ensure compliance with the set standards
i) Conduct periodic information Security awareness to all members of staff

j) Work with developers to refine security checkpoints based on the Security Standards and other industry-accepted doctrine such as NIST SP 800-115 and/or ISO 27002 security standards.
k) Use automated tools to perform source code security analyses to identify vulnerabilities and attack vectors in web applications.
l) Work with information systems analysts to refine web application penetration testing methods and breadth of security services.
m) Obtain and review all required artifacts as part of go, no go analyses at security checkpoint phases in the application development cycle.
n) Assist with periodic security risk assessments, IT security audits, and management reporting.
o) Review and coordinate changes to information security policies, procedures, standards, and audit work programs in a continuous improvement model
p) Conduct in-house vulnerability assessment of the Authority's ICT Application Systems
q) Perform in-house quarterly Penetration Tests on the Authority's ICT Application Systems
r) Maintain Application Firewall rules and ensure they are operational at all times.

3.3 Qualifications and Experience

- Grade 12 Certificate with 5 'O' levels with credit or better including Mathematics and English;
- Bachelor's Degree in Computer Science or equivalent;
- Should possess **any** of the following certifications; Certified Information Systems Management (CISM), Certified Information Systems Security Professional (CISSP), Certified Ethical Hacker or any other relevant IT Security Certification;
- Not less than three (3) years of relevant IT experience at a similar level in an organisation of similar size

TO APPLY

Your application letter should be accompanied by a CV and copies of relevant certificates and should also specify your contact address and telephone number(s).

Application letters should be addressed to:

Director Human Resources and Administration
National Pension Scheme Authority
Levy Business Park
Church Road

P.O. Box 51275
LUSAKA

The closing date of receipt of applications is ***Wednesday, 23rd September, 2020.***

PLEASE NOTE THAT:

- **ONLY APPLICANTS WHO MEET THE SPECIFICATIONS INDICATED ABOVE WILL BE SHORTLISTED.**
- **ANY FORM OF LOBBYING WILL LEAD TO AUTOMATIC DISQUALIFICATION OF THE CANDIDATE**

BE SMART, SECURE YOUR FUTURE