**VACANCY**
**RE ADVERTISEMENT**

| | | |
|---|---|---|
| **REFERENCE NR** | **:** | **VAC00574/23** |
| **JOB TITLE** | **:** | **Senior Specialist: EUC Information System Security Operations** |
| **JOB LEVEL** | **:** | **D2** |
| **SALARY** | **:** | **R 620 597 – R 930 895** |
| **REPORT TO** | **:** | **Consultant: EUC Information System Security Operations** |
| **DIVISION** | **:** | **Service Management** |
| **DEPT** | **:** | **End User Computing** |
| **LOCATION** | **:** | **Gauteng, Numerus** |
| **POSITION STATUS** | **:** | **Permanent (Internal & External)** |

## Purpose of the job

The job will be responsible to perform compliance and vulnerability assessments, execute activities related to the implementation, and maintenance of information security controls and services aligned to the cyber security framework and attend to all logged security incidents.

## Key Responsibility Areas

- Perform ongoing monitoring of information systems and assess threats and risks to information security;
- Coordinate security awareness and training programs to increase employees ' overall understanding, reaction time and the ability to envisage the company's potential safety and compliance requirements
- Perform compliance assessments and vulnerability assessments to ensure government and citizen information is secure
- Attend to all logged security incidents
- Collaborate and partner with internal business representatives to recommend appropriate products so that the solutions are developed with relevant security system design specifications
- Execute activities related to the implementation, and maintenance of information security controls and services aligned to the cyber security framework, policies, standards and procedures
- Management and Administration.

## Qualifications and Experience

**Required Qualification**: 3-year National Diploma / Degree in Computer Science or Information Technology or a relevant discipline verified / certified @ NQF level 6 qualification.
Certifications: ITIL foundation and COBIT 5 Introduction will be an added advantage. Certified information system security professional (CISSP) or Certified Information Security Management (CISM).

**Experience**: 6-7 years Information and Communication Technology (ICT) Infrastructure or Information Security (IS) or application life cycle management which should include the following: Working knowledge of information technology security risk management; Exposure to enterprise architecture frameworks (e.g. TOGAF; GWEA; MIOS);

knowledge of governance processes and standards (e.g. ISO 27001/27002; COBIT; ITIL); Exposure to information system security technical standards (e.g.: SSL certificates, anti-virus protection, etc.); Experienced in (e.g. Service Management, Converge Communication, Risk Management, Information Technology, Applications, etc.).

## Technical Competencies Description

**Knowledge of:** Information security management frameworks, such as ISO/IEC 27001, and NIST.and security services (firewalls, proxy's, DNS, Mail relays etc.) Risk finance and risk control concepts. Enterprise risk management concepts, frameworks. Deep understanding of operational integration of security functions. Strong knowledge of security, and network architecture. Deep knowledge of security best practices, principles, and common security frameworks. Excellent written and verbal communication skills and high level of personal integrity. Knowledge of the latest IT thinking and threat modelling methods together with a creative drive. Analytical mind capable of managing numerous information sources and providing data analysis reports to senior management. Strong customer focus – able to meet the demands of internal and external customers. Excellent communication skills– providing verbal and written communication. Excellent Project management skills. Strong networking, consultation and negotiation skills. Excellent Planning & organising. Financial management. Governance processes and standards (ISO 27001/ 27002, COBIT, ITIL). Proficiency in ICT technology securing and safeguarding (operating databases, applications, IS solutions). Knowledge of Cloud, Public Cloud security best practices and monitoring of systems and services hosted in the cloud (IaaS, SaaS etc.). Network security. On-call network troubleshooting. Firewall administration. Network protocols. Routers, hubs, and switches. System administration skills. Security risk, threats and vulnerability management. Knowledge of Cloud, Public Cloud security best practices and monitoring of systems and services hosted in the cloud (IaaS, SaaS etc.). Working knowledge of Service Oriented architecture (SOA); CISSP domains support (BCM/DRM, Legal, human resource, cryptography, access control, operations, architecture, etc.). Working knowledge of Enterprise architecture framework (TOGAF; Zachman; FEAF; MODAF; GWEA Framework; MIOS). Infrastructure (DELL/ HP/ IBM) and network security configuration. Operating systems administration (UNIX, WINDOWS, Linux) or security configuration. Database and application security configuration (Oracle, ERP,

**Technical competencies:** Technical competencies.

Interpersonal/behavioural competencies: Active listening, Attention to Detail, and Continuous Learning.

## How to apply

To apply please log onto the e-Government Portal: www.eservices.gov.za and follow the following process;

1. Register using your ID and personal information;
2. Use received one-time pin to complete the registration;
3. Log in using your username and password;
4. Click on "Employment & Labour;
5. Click on "Recruitment Citizen" to create profile, update profile, browse and apply for jobs;

**Or**, if candidate has registered on eservices portal, access www.eservices.gov.za, then follow the below steps:

1. Click on "Employment & Labour;
2. Click on "Recruitment Citizen"
3. Login using your username and password
4. Click on "Recruitment Citizen" to create profile, update profile, browse and apply for jobs

For queries/support contact eRecruitmentSupport@sita.co.za

**CV`s sent to the above email addresses will not be considered.**

## Closing Date: 19 December 2022

## Disclaimer

SITA is an Employment Equity employer and this position will be filled based on Employment Equity Plan. Correspondence will be limited to shortlisted candidates only. Preference will be given to members of designated groups.

- If you do not hear from us within two months of the closing date, please regard your application as unsuccessful.
- Applications received after the closing date will not be considered. Please clearly indicate the reference number of the position you are applying for.
- It is the applicant`s responsibility to have foreign qualifications evaluated by the South African Qualifications Authority (SAQA).
- Only candidates who meet the requirements should apply.
- SITA reserves a right not to make an appointment.
- Appointment is subject to getting a positive security clearance, the signing of a balance score card contract, verification of the applicant's documents (Qualifications), and reference checking.
- Correspondence will be entered to with shortlisted candidates only.
- CV`s from Recruitment Agencies will not be considered.
- CV's sent to incorrect email address will not be considered