**VACANCY**

| | | |
|---|---|---|
| **REFERENCE NR** | : | **VAC01188 (Re-advertisement)** |
| **JOB TITLE** | : | **Specialist: Information System Security** |
| **JOB LEVEL** | : | **C5** |
| **SALARY** | : | **R 455 638 - R 683 457** |
| **REPORT TO** | : | **Specialist: Information System Security** |
| **DIVISION** | : | **Service Management** |
| **DEPT** | : | **SM: HOD Information Systems Security** |
| **LOCATION** | : | **SITA Erasmuskloof** |
| **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.
- Collaborate and partner with internal business representatives to recommend appropriate products so that the solutions are developed with relevant security system design specifications.
- Coordinate and provide 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, including logging of non-compliance and security incident.
- Execute activities related to the implementation, and maintenance of information security controls and services aligned to the cyber security framework, policies, standards and procedures.
- Providing skills/knowledge transfer and facilitating processes to draft Business Continuity and Disaster Recover plans.
- Evaluating Business Continuity and Disaster Recover plans on the content/completeness against set standard.
- Testing of Business Continuity and Disaster Recover plans to determine if it would satisfy the requirement to carry on with core business in an event of a disaster/major disruption and if the recovery plan addresses the successful recovery to normal business operations.
- Forensic investigations.

## Qualifications and Experience

**Minimum**: 3 years National Diploma in Computer Science or Information Technology or Network Management or a relevant discipline NQF level 6 qualification, Facilitator, Assessor and Moderator, Business Continuity Management. CISSP or CISA or industry-recognised certificate will be an added advantage.

**Experience**: 3 to 5 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:** Working knowledge of information technology security risk management, monitoring, vulnerability assessments, auditing and reporting. 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).

**Other Special Requirements**

Valid driving licence and own reliable transport.

On site working and not remote working (not working from home).

Traveling to clients and onsite execution of tasks.

Be able to interpret vulnerability assessments and provide high level as well as technical reports.

Knowledge and utilisation of vulnerability assessment software/tools.

Communication and presentation skills as training learners in a classroom setup is a requirement.

**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 egovsupport@sita.co.za OR call 080 1414 882

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

**Closing Date: 21 May 2024**

**Disclaimer**

SITA is an Employment Equity employer and this position will be filled based on the 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 the right not to make an appointment.
- The appointment is subject to getting a positive security clearance, the signing of a balance scorecard contract, verification of the applicants' documents (Qualifications), and reference checking.
- Correspondence will be entered to with shortlisted candidates only.
- CV`s from Recruitment Agencies will not be considered.