

EXTERNAL ADVERT

| | |
|------------------------------|---|
| Location: | Centurion |
| Division: | ESS |
| Date last modified: | February 2024 |
| Reports to: | Governance, Risk and Compliance Specialist |
| Nature of employment: | Permanent |
| Total Guaranteed Pay: | Market related |

[Information Security Specialist]

The main purpose of this role, not limited to:

- 1) Is to develop a framework and standards of operations, designing, and enforcing policies & procedures to protect TCTA's computing infrastructure from all forms of security breaches, as well as the identification of vulnerabilities and resolving them to ensure networks and data remain secure.

THE KEY PERFORMANCE AREAS OF THE ROLE IN FOCUS, ARE:

1. Information Security Services

- Development of Information Security Services capability and initiatives in support of the IT Strategy and EA Planning / Blueprinting processes.
- Advise on and ensure the effective management of information technology and business processes access and to communicate feedback to enable associated security risk management.
- Perform Vulnerability testing and scanning.
- Report on TCTA's vulnerability profile and recommendations to improve the profile.
- Analyse related information / reports to identify discrepancies and anomalies, recommend remedial action and ensure compliance to security policies and standards.
- Develop and/or align information security policies to identify and manage risk exposure.
- Mitigate risk by ensuring that proper IT security and information management measures are in place.

- Perform security audits and clean-ups to ensure accurate and up to date access within TCTA.
- Understand IT applications and infrastructure in alignment with policies and procedures.
- Document the information security principles and guidelines for application software as well as standards that should be adhered to for each product.
- Development of information security requirement specifications prior to the procurement or implementation of new systems and technology to ensure alignment between the business goals and the supporting system functionality.
- Maintain the Information Security Architectural repository to ensure consistency between applications and systems.
- Ensure currency of systems and technology by maintaining an environmental awareness.
- Provide guidelines for the development of life-cycle management strategies for systems and technology in conjunction with major stakeholders to ensure business continuity.
- Managing information security risks and issues and escalating where necessary.

2. Research

- Researching and developing leading practices for the Information Security function.
- Benchmarking and analysis of trends to optimise internal processes.
- Engaging with business units to proactively (and reactively) provide solutions, advising TCTA's management and other stakeholders in their relevant area of expertise.
- Benchmark TCTA's Information Security Architecture with Local and International best practice and applications at other organisations.

3. Project Management

- Identify strategic projects that need to be undertaken in the Information Security function.
- Preparing project definitions and detailed plans with the PMO.

- Driving and supporting the implementation of the specialised areas initiatives and strategic projects that address the needs and expectations of TCTA's stakeholders.
- Documenting functional requirements and specifications for new information security solutions.

4. Reporting

- Monitoring and reporting on progress against functional initiatives.
- Monitoring and reporting on compliance with information security policies, procedures, and controls.
- Promoting sound institutional governance, participating in required governance structures, and serving as a member on the required forums.
- Compiling reports on the functional performance at the required intervals reflecting all relevant statistics, e.g., monthly/quarterly cybersecurity report.

MINIMUM REQUIREMENTS

- B Degree or B-Tech in IT
 - 8 years' experience in Implementation and managing information security solutions in the following environments:
 - MS Windows (Sentinel, Purview, Intune, Entra, Defender, Priva, etc.)
 - Oracle EBS
 - Oracle Fusion Cloud
- Developing information security policies and procedures
- Cybersecurity event detection and investigation
- Centre for Internet Security (CIS) controls, standards, frameworks, benchmarks, etc
- Penetration tests, including ethical hacking (advantageous)
- Vulnerability assessment.
- Managing the Security Operations Centre (SOC) – added advantage
- Certified Information Systems Security Professional (CISSP)
- CISM – Certified Information Security Manager
- CISA – Certified Information Systems Auditor - preferable
- CDPSE – Certified Data Privacy Solutions Engineer - preferable
- CompTIA Security+ - preferable
- Certified Ethical Hacker (CEH) - preferable

- GIAC Security Essentials Certification (GSEC) - preferable
- Systems Security Certified Practitioner (SSCP) - preferable

Please email your CV accompanied by a Cover Letter to careers@tcta.co.za the subject should be the position title. For enquiries, please contact Nangamso Magocoba on Nmagocoba@tcta.co.za

TCTA's approved Employment Equity Plan and Targets will be considered as part of the recruitment process. As an Equal Opportunities employer, the organisation actively encourages and welcome people with various disabilities to apply;

If you have not been contacted within 30 days after the closing date, please accept that your application was unsuccessful.

All appointments shall be subject to Competency Assessments.

A detailed job profile is available on request.

Closing date: 04 March 2024

UNITY – GROWTH – EXCELLENCE – INTEGRITY - RESPECT