Position Title: IT Security Specialist

SASRIA SOC LIMITED

Sasria, a state-owned company, is the only short-term insurer in South Africa that provides affordable voluntary cover against special risks such as civil commotion, public disorder, strikes, riots and terrorism to any individual, business, government or corporate entity that has assets in South Africa.

Sasria has a dual mandate – legislative mandate that directs our day-to-day business operations, and a broader strategic mandate, like any other business in South Africa, to make a positive contribution to transforming our industry and our country, in order to make our country a better place for all her people.

Vision
Special risk covered.

Mission
To provide special risk solutions for stability in South Africa.

Core Values
The following values underpin Sasria's pursuit of its stated vision and mission:

- **Fairness -** we will treat all our stakeholders impartially and with respect, recognising our accountability to them;
- **Ethics -** we will conduct ourselves in a manner that is transparent and ethical: courageously doing what is right, honouring our commitments and communicating honestly;
- **Service Excellence –** in the performance of our work, we will consistently apply our knowledge, experience and best efforts to deliver a relevant and professional service of an exceptional standard;
- **Collaboration -** we will engage with our stakeholders, assuming positive intent, respecting diversity and working together to create uniformly positive outcomes.
- **Innovation** – we will apply thought and creativity to the application of new solutions to our and our customers' needs and requirements.

Sasria is committed to diversifying its staff profile in terms of its transformation agenda and encourages candidates from previously disadvantaged backgrounds to apply. Sasria will respond to short listed candidates. Candidates who have not been contacted within 4 weeks of the closing date can assume that their application has been unsuccessful.

ROLE DESCRIPTION

Job summary statement/purpose

To actively protect the organisations information technology assets and infrastructure from external or internal threats and ensuring compliance with statutory and regulatory requirements regarding information access, security and privacy

Key performance areas (duties & responsibilities)

1. IT Security
    - Design, configure, deploy, and maintain Sasria security infrastructure
    - Actively protect the organisations information technology assets and infrastructure from external or internal threats and ensuring compliance with statutory and regulatory requirements regarding information access, security and privacy
    - Analyse problems, recommend solutions, products, and technologies to meet business security and information security objectives
    - Recommend best security practices to achieve business objectives, advises on risk assumptions for any variances granted, and provides alternatives to achieve desired end results
    - Identify, resolve and assist in management of security threats, vulnerabilities, non-compliances and risks, focusing on application security

2. Cyber-Security (Content Filtering, etc)
    - Coordinating cybersecurity risk mitigations (including cybersecurity awareness)
    - Control and monitor a spam management solution in order to minimise the amount of spam received by the Sasria.
    - Control and monitor filtering of harmful email attachments received from external sources at the gateway (firewall).
    - Ensure and monitor filtering of harmful and non-business related email attachments received from internal and external sources at the relevant mail server.
    - Oversee and monitor filtering for all users browsing the Internet restricting access as per business requirements.
    - Monitor systems for any anomalies, proper updating, and patching
    - Identifying and minimizing information security vulnerabilities

Sasria is committed to diversifying its staff profile in terms of its transformation agenda and encourages candidates from previously disadvantaged backgrounds to apply. Sasria will respond to short listed candidates. Candidates who have not been contacted within 4 weeks of the closing date can assume that their application has been unsuccessful.

3. Firewall Monitoring and control

- Monitor gateway firewall for malicious activity and restrict network access using the firewall policy as per business requirements.
- Implement firewall solutions to properly secure the organisations data and provide consultation on all new firewall implementations, firewall configuration changes, and projects requiring security operational support
- Evaluate and monitor the firewall to prevent virus attacks from an external source.

4. Anti-Virus Management

- Scan all email from external and internal sources for viruses and malicious attachments at the Microsoft Exchange server.
- Evaluate and maintain an enterprise wide desktop-based Anti-Virus client and ensure that all clients have the most recent updates.

5. Server Controls and Encryption and Remote Access (SSL VPN)

- Control and maintain access to central server network shares as per requests from business.
- Control and maintain the server hardware and software environment.
- Control and maintain electronic certificates for relevant server in the IT environment.
- Control, admin and provide data encryption to staff as per business requirement.
- Administer and maintain a remote access system (SSL VPN) users.

6. User Support

- Provide second line support to users with any Information Security related queries within the SLA time frame.
- Overseeing and providing advanced support on open issues (e.g. customer logged tickets, incidents, projects etc.)
- Assist in incident response for any breaches, intrusions, or theft
- Coach and guide Service desk and IT support in their incident response in regards to security , and appropriately escalating issues in-line with the service management processes and procedures
- Overseeing and providing advanced support on open issues (e.g. customer logged tickets, incidents, projects etc.)

Sasria is committed to diversifying its staff profile in terms of its transformation agenda and encourages candidates from previously disadvantaged backgrounds to apply. Sasria will respond to short listed candidates. Candidates who have not been contacted within 4 weeks of the closing date can assume that their application has been unsuccessful.

- Assist the end-user, and IT in requesting security variances and implementation of subsequent configuration change requests

7. Ad hoc tasks
    - Recommend best security practices to achieve business objectives, advises on risk assumptions for any variances granted, and provides alternatives to achieve desired end results
    - Research identify and recommend improvement to capabilities and maturity of threat and vulnerability management strategy, policy, standards, processes, procedures and tools in order to deliver value to the business
    - Maintains system documentation and configuration data for regulatory and audit purposes

Qualifications and Experience:

Minimum requirements:

- A relevant diploma/degree in Information Communication Technology
- Relevant IT security certifications (CompTIA Security +, ISO 27000 ect)
- 3 - 5 years IT security experience either in public or private environment.
- Proven track record of driving innovation in their Domain expertise area.

Ideal and advantage:

- ITIL certificate ITIL
- Member of a professional body within ICT.

Knowledge

- Cybersecurity CIS Critical controls
- Enterprise Architecture
- Cyber security tools & frameworks
- Networking and IT Management

Behavioural Competencies:

- Problem solving skills with the ability to interpret and analyse data
- Ability to explore and learn new technology and processes
- Have emotional resilience
- Be able to manage relationships
- Be able to handle conflict
- Take initiatives in solving problems
- Be able to work in a team with dynamics

Sasria is committed to diversifying its staff profile in terms of its transformation agenda and encourages candidates from previously disadvantaged backgrounds to apply. Sasria will respond to short listed candidates. Candidates who have not been contacted within 4 weeks of the closing date can assume that their application has been unsuccessful.

Demographics
A South African citizen of any gender, preference will be given to an EE candidate.

Location of the role:
The role will be in Illovo, Johannesburg.

Closing Date: 30 August 2019
Send applications to: careers@sasria.co.za

Sasria is committed to diversifying its staff profile in terms of its transformation agenda and encourages candidates from previously disadvantaged backgrounds to apply. Sasria will respond to short listed candidates. Candidates who have not been contacted within 4 weeks of the closing date can assume that their application has been unsuccessful.