Job Title:	Information Security Specialist
Job Location:	TBC
Team:	Corporate Security
Sector:	Finance and Data
Compensation:	R1.0 - R1.5Mill+
Security Team Size:	2
Countries of Operation:	Southern Africa

Redherd is a bespoke, boutique information security and **technology** recruiting partner. Our clients and us tackle some of the most complex security requirements of the modern-day cyber security industry. We obsess about the details and the subtle intricacies of a given position, therefore only run surgical searches and only approach those who possess the skills required, to excel in specific positions. Our candidates come first, and that will always stay at the forefront. Afterall, you know what is best for you.

This prominent credit bureau in South Africa specializes in providing comprehensive credit information and data analysis services. Their expertise lies in helping businesses make informed credit decisions, prevent fraud, and ensure regulatory compliance. By offering detailed insights and analytics, they support financial institutions, retailers, and utility companies in optimizing their credit management and **safeguarding sensitive information**. This company plays a crucial role in promoting **financial responsibility** and stability within the South African financial ecosystem.

The Information Security Specialist role is pivotal in safeguarding the company's **data and systems.** This position involves designing, implementing, and managing **robust security measures** to protect sensitive information. The specialist will handle tasks such as developing security frameworks, managing technical safeguards, leading incident response efforts, and ensuring regulatory compliance. With a strong foundation in both technical security measures and legal frameworks, the role is essential in maintaining the **confidentiality, integrity, and availability** of data, thereby supporting the company's mission to foster financial responsibility and prevent fraud.

Key Responsibilities

- **Security Framework Implementation:** Develop and manage a comprehensive information security framework aligned with ISO 27001, NIST, and other standards tailored to the organization's needs.
- **Technical Safeguards:** Implement and oversee technical safeguards, including firewalls, encryption, intrusion detection systems, and access controls to protect sensitive information.
- **Incident Response and Management:** Develop and maintain an incident response plan to address security breaches or incidents swiftly and effectively, minimizing impact.
- **Vulnerability Management:** Perform regular vulnerability assessments and penetration testing to identify and mitigate security risks.
- **Data Security:** Ensure the confidentiality, integrity, and availability of all processed and stored data. Manage encryption, secure storage, and data transfer processes.
- **Security Awareness Training:** Create and deliver security awareness training programs for employees to enhance the organization's security culture.
- **Regulatory Compliance:** Collaborate with the compliance team to ensure security practices meet legal requirements, staying updated on regulatory changes.
- **Cross-functional Collaboration:** Work with various departments to ensure policies, processes, and systems are secure and legally compliant.
- **Continuous Improvement:** Regularly evaluate and enhance information security measures in response to evolving threats and regulations.

Key Responsibilities

- Extensive experience in information security, particularly within the financial or credit reporting sectors, with a solid understanding of relevant South African legislation.
- Proficiency in implementing security frameworks and technical safeguards, with certifications like CISSP, CISM, or CISA being advantageous.
- Strong background in incident response, vulnerability management, and data security.
- Knowledge of cloud computing environments and associated security challenges.
- Experience in deploying security awareness training programs.
- Excellent communication skills, capable of explaining complex security concepts to various audiences.
- Commitment to continuous learning and staying current with security technologies and legislative changes.
- Bachelor's or Master's degree in Computer Science, Information Security, or a related field, though extensive experience is highly valued.
- At least 5 years of experience in information security, particularly within financial services or credit bureau sectors.

Communication and Adaptability

- Strong interpersonal and communication skills for effective collaboration with technical and non-technical team members.
- Ability to articulate complex technical issues and solutions clearly to stakeholders.
- Commitment to continuous learning and adapting to new technologies and methodologies.
- Ability to work in a dynamic, fast-paced environment, focusing on key objectives and deadlines.

Work Environment

This role offers a hybrid work model, blending remote work with occasional on-site collaboration. Primarily remote, the position provides significant flexibility and autonomy, with periodic in-office time required for key meetings and team activities. This balance promotes face-to-face collaboration and alignment with the company's culture and goals.

What They Offer

- A competitive compensation package.
- Opportunities for professional growth in a cutting-edge technology environment.
- A dynamic team culture that values innovation and collaboration.

Company Culture

Our culture emphasizes innovation, integrity, and excellence. We foster an environment where creativity thrives, and every team member can contribute to revolutionizing the credit reporting industry. Continuous learning and career growth are encouraged within our supportive ecosystem. Join us to be part of a team that values progress, collaboration, and making a difference.