South Africa

SOUTH AFRICAN TOURISM

DATA & SECURITY IMPLEMENTATION SPECIALIST

An exciting Data and Security opportunity exists at our Head Office in South Africa, to join our Digital and Technology (DigiTech) business unit as a Data and Security Implementation Specialist. We invite applications from individuals who are passionate about promoting South Africa as a Tourism Destination and possess the required skills and experience.

Purpose of the Role

Act as subject matter expert and implementation specialist of data management and system security standards defined by the business. Perform daily data and security operations across all digital platforms and provide ongoing technical assistance, cyber security monitoring, risk management, data, and information management support to the business.

Key Performance Areas:

Systems and Information Security

- Oversee and maintain system and cyber -security across SA Tourism to safeguard Business information system assets.
- Develop and manage the data governance framework for all systems at SA Tourism.
- Develop and manage the digital channel access governance framework for all owned, earned and bought digital media channels.
- Develop and manage user platform access governance with external service providers.
- Manage the Design, Development, Implementation and Support of systems security and cybersecurity solutions across all SA Tourism network system domains (including hosted solution domains).
- Frequently review network systems (including databases) logs as per user access and activities.
- Provide user training or user awareness services on network system security requirements.
- Ensure use of systems by the organization adherence to Legislative requirements as per protection of private information and POPIA and GDPR reporting requirements.
- Confer with users to discuss issues such as computer data access needs, security violations and programming changes.
- Encrypt data transmissions and erect firewalls to conceal confidential information as it is being transmitted and to keep out tainted digital transfers.
- Monitor the use of data files and regulate access to safeguard information in computer files.
- Monitor current reports of computer viruses to determine when to update virus protection systems.

- Modify computer security files to incorporate new software, correct errors or change individual access status.
- Assist in resolving systems security and data/information related logged calls.

ICT Security Policies and Support

- Ensuring that the SAT's security policies comply with current acts and legislations.
- Develop the digital ICT security framework.
- Develop and maintain standards as per network system security configurations and settings.
- Develop and manage firewall rules and perform random vulnerability and penetration tests (internal and external).
- Manage the development, implementation and review of Information Security, User Account Management, ICT Systems Use and System Change Request Policies and Procedures.
- In partnership with ICT-Infrastructure Support team, develop policies and procedures for areas such as business continuity planning, loss prevention, fraud prevention, account management, patch management, server baselines, data backup and privacy.
- Develop emergency procedures and incident responses.
- Assist in ensuring that general Digital and ICT frameworks are implemented.
- Review existing security measures and updating security protocols as needed.

Application of System Security Standards

- Oversee the daily systems operations to identify potential system security risks and room for improvements.
- Oversee and coordinate systems security efforts across SA Tourism to ensure that security standards are met across all digital platforms:
- Ensure security is maintained and updated.
- Oversee the safeguarding of intellectual property and computer systems.
- Identify security initiatives and standards.
- Oversee the network of vendors and service providers who secure the company's assets.
- Prioritise security initiatives.
- Managing, evaluating, and resolving any physical or digital security incidents or breaches.
- Conduct audits as per vulnerability and penetration tests, to find holes in security platforms.
- Conduct user access audits across all systems.
- Assist in system change control processes and monitor project activities to ensure the system security of the projects.
- Prepare periodical reports and make presentations as required.

DigiTech Risk Management

- Presenting risk assessments and improved security policies to the Digitech team members.
- To ensure that sufficient risk management is incorporated to the DigiTech operation so that liability is minimised and or eliminated.
- Implement Digitech data governance and risk management framework.
- Identify and manage the operational risks for Digitech and make inputs to the operational Digitech Risk Register.
- Develop, implement, and report on risk mitigating measures for Digitech.

Minimum Qualifications and Experience

- A Bachelor's Degree/Diploma in Information & Communication Technology/Computer Science or related curriculum
- Project management
- ITIL Programme Certification.
- COBIT Certificate will be advantageous.
- 5-8 years of experience in systems security services management, of which three years should be in management position.
- 5-8 years of Experience in Information management applications and IT security support.
- 5-8 years of Experience in digital channel governance access management.
- 5-8 years of Experience in Database administration

Knowledge and understanding of:

- Governance, risk, and compliance.
- Project management
- Knowledge and implementation of GDPR and POPI Act.
- Systems Security (MCSE/CNNA/CISM).
- Database Administration
- Knowledge of Public Service systems.
- Relevant legislation and regulatory requirements namely, POPI Act, PFMA, Treasury Regulations and Frameworks on performance information and strategic plans.

Visit us @ www.southafrica.net

Detailed CV to be sent to : hr@southafrica.net
Closing date : 21 June 2022

Important note:

People with disabilities are encouraged to apply. Due to a large amount of correspondence we envisage receiving, only shortlisted candidates will be contacted. Should you have not heard from us Four weeks after the closing date, kindly consider your application unsuccessful. No late applications will be accepted.