



Job Description

9th Floor Tanzanite Park, Victoria, Dar es Salaam, Tanzania | +255 758 778 886 | info@empower.co.tz

Job Title IT Information Security Officer	Job Location Dar es Salaam	Category -
Job Type Full Time	Job level Intermediate	Industry IT & Software
Open to Expatriates Only Open to Tanzanian Nationals		

Minimum Requirements

Min Budget -	Max Budget -	Primary Industry IT & Software: 4 Years
Secondary Industry -	Primary Category -	Secondary Category -
Certificate -	Qualification -	

Summary

The IT Information Security Officer is responsible for ensuring the confidentiality, integrity, and availability of the organization's information systems. This role involves the continuous assessment, development, and implementation of security policies, procedures, and controls to protect the organisation from internal and external threats.

Responsibilities

- **Cybersecurity Strategy Development:** Advise senior management and the board on information security management, and develop an institutional methodology for managing cybersecurity risks.
- **Risk Assessment and Management:** Conduct ongoing risk assessments to identify vulnerabilities and recommend mitigation strategies. Maintain a cyber-incident response team to address potential threats.
- **Policy Formulation:** Develop and update cybersecurity policies and procedures in line with the latest regulatory requirements and industry standards. Ensure policies are approved by senior management and the board.
- **Security Monitoring:** Monitor security trends, threats, and advanced developments in the field. Stay informed about emerging attack techniques and implement relevant countermeasures.
- **Incident Response:** Analyse security incidents both locally and globally, assess their potential impact on the organisation, and implement preventive measures.
- **Security Awareness:** Develop and implement a comprehensive information security awareness program for all employees and stakeholders.
- **Compliance and Auditing:** Ensure compliance with relevant laws, regulations, and standards. Conduct regular security audits and assessments to ensure the effectiveness of security measures.
- **Collaboration and Coordination:** Work closely with IT and other departments to integrate and coordinate all security efforts. Liaise with external partners and service providers to enhance the organisation's security posture.
- **Reporting:** Prepare detailed reports for senior management and the board on the institution's cybersecurity defences levels, identified weaknesses, and required countermeasures.

Education & Qualifications

- A Bachelor's degree in Computer Science, Information Technology, or a related field.
- A Master's degree or professional certifications (CISM, CISSP, CRISC) will be an added advantage.

Requirements

- Minimum of 4 years of experience in information security, with a focus on risk management, policy development, and incident

response.

- Experience working in a financial institution or a regulated environment is preferred.

Characteristics

- Proficiency in using security tools and technologies for vulnerability assessment, penetration testing, and security monitoring.
- Strong understanding of information security domains, including cybersecurity frameworks, risk management, and incident response.
- Knowledge of regulatory requirements and industry standards for information security.
- Excellent communication skills with the ability to present complex security concepts to non-technical stakeholders.
- Strong problem-solving skills and the ability to work under pressure in a fast-paced environment.
- High level of integrity and ethical conduct.

Driving Licence

Not Required

To Apply for This Job [Click Here](#)