Job Description

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

Job Title
The Manager: Cyber Security

Job Location
Zanzibar City

Category
-

Job Type
Full Time

Job level
Manager

Industry
Facilities Management

Open to Expatriates
Only Open to Tanzanian Nationals

Minimum Requirements

Min Budget
-

Max Budget
-

Primary Industry
Facilities Management: 5 Years

Secondary Industry
-

Primary Category
-

Secondary Category
-

Certificate
-

Qualification
-

Summary

The Manager: Cyber Security is responsible for managing cybersecurity operations, ensuring effective risk management, incident response, and compliance to protect airport systems, networks, and data from cyber threats. The role oversees security monitoring, threat analysis, implementation of cybersecurity controls, vulnerability management, and access management processes. The position works closely with the Chief Information Officer, ICT teams, operational departments, and external cybersecurity partners to maintain a secure technology environment and strengthen the organization's cybersecurity posture.

Responsibilities

- Manage day-to-day cybersecurity operations to ensure continuous monitoring and protection of IT systems and networks.
- Identify, assess, and manage cybersecurity risks affecting airport systems and infrastructure.
- Lead cybersecurity incident response activities including detection, containment, investigation, and recovery.
- Oversee security monitoring activities and analyze potential threats, vulnerabilities, and attacks.
- Ensure effective implementation and maintenance of cybersecurity controls including firewalls, identity management, and access controls.
- Monitor the effectiveness of security controls and recommend improvements where required.
- Ensure compliance with internal cybersecurity policies, regulatory requirements, and security standards.
- Coordinate vulnerability assessments, penetration testing, and cybersecurity risk mitigation activities.
- Oversee identity and access management processes to ensure secure system access.
- Support cybersecurity awareness and training initiatives across the organization.
- Collaborate with ICT teams, operational departments, and external partners to ensure secure system integration and operations.
- Provide cybersecurity reports on security status, incidents, vulnerabilities, and risks to the Chief Information Officer and management.
- Escalate critical cybersecurity risks and incidents to relevant stakeholders.
- Ensure continuous improvement of cybersecurity processes, controls, and practices.
- Maintain effective cybersecurity monitoring using tools such as SIEM, IAM, firewalls, SOC tools, and network monitoring systems.

Education & Qualifications

- Bachelor’s degree in Cybersecurity, Information Technology, Computer Science, or related field.
- Additional training in cybersecurity is an added advantage.
- Professional certifications such as CISSP, CISM, CEH, CompTIA Security+, ISO 27001 Lead Implementer, or equivalent are an added advantage.
- Proficiency in both English and Swahili.

Requirements

- 5–8 years’ experience in cybersecurity, information security, or IT risk management roles.
- Experience in cybersecurity operations, monitoring, and threat management.
- Experience in risk assessment, vulnerability management, and incident response.
- Experience managing security controls including firewalls, identity management, and access controls.
- Experience with cybersecurity tools such as SIEM, IAM, SOC tools, and network monitoring systems.
- Experience coordinating vulnerability assessments and penetration testing activities.
- Experience working in critical infrastructure, aviation, or high-security environments is an added advantage.

Characteristics

- Strong knowledge of cybersecurity operations and monitoring.
- Ability to conduct risk assessments and manage vulnerabilities.
- Strong incident response and threat analysis skills.
- Knowledge of identity and access management principles.
- Strong analytical thinking and problem-solving ability.
- High attention to detail and commitment to security standards.
- Ability to make effective decisions under pressure.
- Strong communication and coordination skills.
- Ability to enforce cybersecurity controls across the organization.
- Ability to coordinate effectively with multiple departments and external partners.
- Ability to identify, escalate, and manage critical cybersecurity risks.
- Strong accountability for maintaining system and network security posture.

Reporting To

Chief Information Officer

Driving Licence

Not Required

To Apply for This Job Click Here