NORTH-EAST REGIONAL HEALTH AUTHORITY

MANAGER, ICT SECURITY (MIS/IT 6)

The **North-East Regional Health Authority (NERHA),** a statutory body under the Ministry of Health & Wellness, with responsibility for the management and delivery of Public Health Services within the parishes of St. Ann, St. Mary and Portland invites applications from suitably qualified individuals to fill the position of **Manager, ICT Security.**

Summary:

Reporting to the **Director, Information Communication Technology**, the **Manager, ICT Security** is responsible for leading and overseeing the organization's ICT security, risk management and compliance framework, ensuring the confidentiality, integrity and availability of all ICT systems and data. The role serves as the technical authority for ICT security governance and risk, providing oversight to ensure that all systems and services are designed, implemented and operated in alignment with organizational policies, regulatory requirements and recognized cybersecurity frameworks. The role also ensures that appropriate technical controls are in place to support data protection and privacy requirements.

Key Responsibility Areas:

Technical/Professional Responsibilities

Security Operations and Engineering

- Implement, configure and manage security technologies, including firewalls, intrusion detection/prevention systems, SIEM and endpoint protection solutions.
- Monitor, analyze and respond to security events and incidents, ensuring timely detection, investigation and resolution.
- Conduct vulnerability assessments and penetration testing and ensure remediation of identified risks.
- Implement and maintain technical security controls, including identity and access management, network security, endpoint protection and system hardening.
- Develop, implement and routinely test disaster recovery and cyber incident response plans.
- Lead the development and continuous improvement of ICT security architecture, standards and technical controls.
- Provide security review and approval for ICT systems, infrastructure designs and projects.

Security Governance, Risk and Compliance

- Develop, implement and maintain ICT security policies, standards and procedures.
- Lead ICT security risk management processes, including risk identification, assessment, mitigation and reporting.
- Maintain and monitor the ICT security risk register and ensure alignment with enterprise risk management.
- Ensure and enforce compliance with organizational policies, regulatory requirements and applicable cybersecurity standards.
- Conduct ICT security audits, assessments and compliance reviews and ensure timely remediation of identified issues.
- Define and monitor security performance indicators and compliance metrics
- Prepare and submit regular reports on ICT security posture, risks and compliance status.

Management/Administrative Responsibilities

- Provide leadership and strategic direction for ICT security across the organization while directly executing key security functions.
- Establish priorities and oversee execution of ICT security initiatives and programmes.
- Review and approve ICT system designs and implementations to ensure compliance with security requirements.
- Coordinate with ICT Infrastructure, Software/Database and Client Support teams to ensure integration and enforcement of security controls.
- Manage vendor relationships and support procurement, implementation and maintenance of cybersecurity solutions.
- Advise on cybersecurity risks, emerging threats and mitigation strategies to support informed decision-making.
- Promote a culture of cybersecurity awareness and lead the design, delivery and continuous improvement of security awareness and training programmes.
- Monitor emerging cybersecurity threats and technologies and guide organizational response strategies.
- Performs all other related duties and functions as may be required from time to time.

Required Competencies:

Core

- Strong leadership and ability to influence and guide ICT teams and stakeholders.
- Strategic thinking and planning aligned to organizational objectives.
- Strong analytical, problem-solving and decision-making skills with sound judgment.
- Effective communication, interpersonal and presentation skills, both written and verbal.
- Stakeholder-focused approach with the ability to work under pressure.
- Strong organizational and time-management skills with the ability to manage multiple priorities.
- Accountability and results orientation with a focus on outcomes.
- High level of integrity, professionalism and confidentiality.

Technical

- Strong knowledge of cybersecurity frameworks, standards and best practices.
- Proficiency in security technologies, including firewalls, intrusion detection/prevention systems, endpoint protection and SIEM solutions.
- Knowledge of network and infrastructure security, including segmentation, secure configuration and system hardening.
- Experience with identity and access management, including Active Directory security, LDAP and single sign-on (SSO).
- Ability to monitor, analyze and respond to security events, logs and threat intelligence.
- Experience conducting vulnerability assessments, security audits and penetration testing.
- Knowledge of application and cloud security principles.
- Understanding of risk management, compliance and security governance practices.
- Knowledge of business continuity, disaster recovery and cyber incident response planning.

Qualification & Experience:

- BSc. Degree in Computer Science, Information Technology, Cybersecurity, or a related field.
- A recognized professional certification in cybersecurity or network security (e.g., CompTIA Security+, Cisco Security, or equivalent) is required.
- At least four (4) years' relevant experience in ICT security or a related area.
- Relevant industry certification is an asset (e.g., CISSP, CISM, CEH, ISO 27001, CISA, or CRISC).
- Experience in implementing and managing ICT security controls, risk assessments and incident response activities.

Special Conditions Associated with The Job:

- May be required to work beyond normal working hours, including evenings, weekends and public holidays, in response to security incidents, system outages, or critical operational needs.
- May be required to travel.

REMUNERATION PACKAGE PER ANNUM:
Salary Scale: $5,198,035 – $6,990,779 per annum

Applications along with detailed resume should be sent no later than **2026 June 10** to:

The Director,
Human Resource Management & Development
North-East Regional Health Authority
34-38 Ocean Village Shopping Centre, Ocho Rios
St. Ann E-mail: jobs@nerha.gov.jm or Fax: (876) 795–2747
WE THANK ALL APPLICANTS FOR RESPONDING, HOWEVER, ONLY SHORT LISTED APPLICANTS WILL BE ACKNOWLEDGED.