Ministry of National Security

VACANCY NOTICE

Applications are invited from suitably qualified candidates to fill the post of:

SENIOR POLICY DIRECTOR, CYBER INTELLIGENCE & INCIDENT RESPONSE (GMG/SEG 5)
CYBER INTELLIGENCE & INCIDENT RESPONSE BRANCH

SALARY SCALE: $3,394,286.00 – $4,034,739.00
TRAVELLING ALLOWANCE: $1,697,148.00 PER ANNUM WITH MOTOR VEHICLE;
$678,864.00 PER ANNUM WITHOUT MOTOR VEHICLE:

JOB PURPOSE:

The incumbent is responsible for establishing and leading new and evolving MNS intelligence and cybercrime and cybersecurity capabilities, including leading on policies, legislation and programmes in these areas of focus.

The incumbent is responsible for developing, improving and managing the national intelligence sharing and use architecture, policies and programmes (across government for the purposes of national security); lead on all MNS cybercrime and cybersecurity legislation, policies and programmes and oversee the Ministry's covert Cybersecurity Incident Response team.

The duties and responsibilities include but are not limited to the following:

KEY RESPONSIBILITIES:

- Leads and manages the creation of the threat intelligence programme;
- Establishes proper agreements and relationships with third parties for the supply of systems and consulting services as required;
- Develops a comprehensive cybersecurity policy framework that is aligned to the national ICT strategy and subscribes to leading guidelines, standards, and relevant regulations;
- Provides expert technical advice, briefings and support to stakeholders on cybersecurity and cyber-policy matters;
- Leads interventions geared at strengthening cybersecurity capabilities within the national security sector;
- Leads consultation sessions with stakeholders and ensure relevant information is captured and disseminated;
- Recommends the establishment of monitoring and evaluation frameworks to evaluate the effectiveness of policies, programmes and initiatives implemented or being implemented;
- Implements mechanisms to strengthen the Ministry's monitoring and evaluation capabilities for responsibility areas;
- Leads the design and implementation of the project's monitoring and evaluation activities, including the development of the project's Monitoring and Evaluation Plan;
- Introduces and monitors data quality assessments and data improvement plans;
- Develops and leads implementation of strategies for institutional and individual capacity building on data collection, collation and reporting procedures of matters pertaining to cybersecurity;
- Undertakes detailed planning and execution of risk management activities.
- Builds relationships and an effective coordination and communication channel between the Division Head and relevant public and private stakeholders, (including channels for obtaining threat feeds from regional and international bodies);
- Provides responsive, high quality service to stakeholders by providing accurate, relevant, complete and up-to-date information;
- Recommends policy options related to cybersecurity to the Chief Technical Director: Security Risk Reform & Transformation Division for consideration;
- Leads in coordinating activities with local, regional and international entities with interests in cybersecurity;
- Represents the Ministry at local, regional and international conventions workshops and meetings relevant to cybersecurity policy issues;

MINIMUM QUALIFICATION AND EXPERIENCE:

- Master's Degree in Public Policy/Management or related discipline;
- Minimum of five (4) years' experience in a senior management leading role with at least three (2) years in complex and distinct functional units/branches
- Demonstrated experience in successfully leading several large scale transformational projects
- Experience interfacing with the leadership of key institutions in the cybersecurity area/function would be a distinct asset.

SPECFIC KNOWLEDGE & SKILLS:

- Sound knowledge of Policy Development processes;
- Knowledge of Government of Jamaica planning processes;
- Knowledge of the preparation of policy documents i.e. Cabinet Submissions/Notes;
- Strong organizational and programme management skills;
- Knowledge of relevant Laws, Government Guidelines;
- Working knowledge of scientific research processes;
- Sound knowledge of local, regional and international cybercrime, cybersecurity laws and regulations;
- Good knowledge of security standards and frameworks (NIST, ISO/IEC 27001, etc.)
- Familiarity with the cybercrime, cybersecurity and intelligence laws and regulations of Jamaica, Caribbean Region, North America and Europe
- Familiarity with security incident and event management solutions, and other solutions in the cybersecurity monitoring landscape;
- Working knowledge of a Security Operations Center (SOC)
- Intermediate project management skills;
- Sound knowledge of monitoring and evaluation principles and practices;
- Ability to conceptualize, develop, implement and monitor mechanisms to minimize organizational risks;
- Working knowledge of Microsoft Word, Excel and Power Point skills.

SPECIAL CONDITIONS ASSOCIATED WITH THE JOB:

- May be required to work beyond normal working hours and on weekends and public holidays;
- May be required travel extensively locally and internationally;
- Critical deadlines for completion of tasks;
- Typical working condition.

Interested persons should forward their applications and résumés **NO LATER THAN Friday, May 17, 2019,** to the:-

Director, Human Resource Management & Administration
Ministry of National Security
4th Floor NCB North Tower
2 Oxford Road
Kingston 5
Email: jobopp@mns.gov.jm

Subject: Senior Policy Director, Cyber Intelligence & Incident Response (GMG/SEG 5)

We thank all applicants for their interest in this career opportunity. However, please note, only short-listed candidates will be contacted