



Ministry of National Security

VACANCY NOTICE

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

**CYBER SECURITY & CYBERCRIME POLICY SPECIALIST (GMG/SEG 3)
CYBER INTELLIGENCE & INCIDENT RESPONSE**

SALARY SCALE: \$2,336,309.00 – \$2,777,138.00

**TRAVELLING ALLOWANCE: \$894,924.00 PER ANNUM WITH MOTOR VEHICLE;
\$362,472.00 PER ANNUM WITHOUT MOTOR VEHICLE:**

JOB PURPOSE:

Provide specialist technical input to support the development, implementation, management and improvement of the Ministry's cybercrime and cybersecurity capabilities, and policy framework, including the development of national policies, legislation and programmes in these areas of focus.

The incumbent liaises with respective partners and stakeholders and conducts research and analysis to coordinate and develop relevant national cybersecurity/ cybercrime legislative changes, policies, strategy and programmes - in close collaboration with the Ministry of Science Energy & Technology, in particular, and bona fide and recognized international partners and agencies as required; and proactive and reactive legislative, policy or programme responses to cyber-related risks, threats, breaches and recommendations identified by the MNS (or other MNS Department and Agency) Cybersecurity Incident Response Unit(s) and the Strategic Intelligence Branch.

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

KEY RESPONSIBILITIES:

- Builds relationships and an effective coordination and communication channel between the Division and relevant public and private; stakeholders, (including channels for obtaining threat feeds from regional and international bodies);
- Designs systematic processes to share tactical cyber threat intelligence at a national level;
- Communicates compliance requirements with the applicable laws and regulations;
- Undertakes research and analysis, and provides advice to the Snr. Policy Director, Cyber Intelligence & Incident Response to support the establishment of proper agreements and relationships with third parties for the supply of systems and consulting services as required;
- Maintains an in-depth knowledge of internationally accepted cybersecurity standards and frameworks, and provides expert advice/input to the departments strategy and operations;
- 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;
- Identifies and monitors environmental and market trends and pro-actively assesses impact on strategic and national ICT initiatives;
- Participates in joint public-private initiatives for cybersecurity awareness and improvement;
- Formulates, evaluates and re-appraises policy systematically;
- Develops and establishes a programme for periodic security awareness.
- Provides specialist advice to inform the establishment of strategy for addressing operational risks;
- Undertakes detailed planning and execution of risk management activities;
- Maintains effective links with other Ministries, Departments, Agencies and local and international partners;
- Works with the relevant stakeholders in the development of strategic objectives and comprehensive operational plans;
- Undertakes research, analysis and develops recommendations to support the Ministry in providing advice to other policy making entities within the Ministry of National Security, other Ministries, regulators, etc.

MINIMUM QUALIFICATION AND EXPERIENCE:

- Bachelor's Degree in Cybersecurity, Cybercrime, intelligence or equivalent;
- Minimum five (5) years' experience at the IT management level, in a lead role encompassing intelligence, cybersecurity and/or cybercrime related management and/or policy formulation;
- Experience in the design or operation of a Management System compliant with global standards (e.g. ISO/IEC 27001:2015);
- Certifications in at least three of the following (or equivalent):
 - CISM: Certified Information Security Manager
 - GSLC: GIAC Security Leadership
 - CCISO: Certified Chief Information Security Officer
 - CGEIT: Certified in the Governance of Enterprise IT
 - CISSP: Certified Information Systems Security Professional
 - CISSP-ISSMP: Information Systems Security Management Professional
 - PMP: Project Management Professional
 - CCFP: Certified Cyber Forensics Professional

SPECIFIC KNOWLEDGE & SKILLS:

- Competence with leading security standards and frameworks (NIST, ISO/IEC 27001, etc.);
- Working knowledge of a Security Operations Center (SOC);
- 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.

SPECIAL CONDITIONS ASSOCIATED WITH THE JOB:

- May be required to work beyond normal working hours and on weekends;
- May be required travel extensively locally and internationally;
- May be required to visit crime and violence-prone communities;
- May be required to meet critical deadlines within a short length of time.

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: Cyber Security & Cyber Crime Policy Specialist (GMG/SEG 3)

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