THE GOVERNMENT OF ST CHRISTOPHER AND NEVIS
Ministry of Information, Communications, Technology and Posts
P O BOX 186,
NATIONAL ICT CENTER, #3 C. A. PAUL SOUTHWELL INDUSTRIAL SITE
BASSETERRE, SAINT KITTS
TEL: (869) 465- 2521 ext 467-1281 EMAIL: technology@gov.kn

Job Description
Job Title: CYBERSECURITY COORDINATOR
Work Location: National ICT Center, C.A.P. Southwell Industrial Site
Division/Department: Department of Technology, Ministry of Information, Communications, Technology and Posts
Reports to: Director
[✓] Full-time [ ] Part-time
Description of Post: The Cybersecurity Coordinator is responsible for the management of the Cybersecurity Unit and safeguarding the organization's network infrastructure, cloud environments, and critical assets from cyber threats. This role requires advanced expertise in network security architecture, cloud security frameworks, vulnerability management, and incident response. The incumbent will work closely with IT, network, and application teams to design, implement, and maintain robust security controls that ensure confidentiality, integrity, and availability of systems and data.
Duties and responsibilities for the post include but are not limited to the following: **Governance, Management, Risk & Compliance** • Manage the Cybersecurity Unit and ensure the smooth operations of the Unit • Lead in the development of a Cybersecurity Strategy and Implementation Plan • Conduct consultations with key stakeholders, manage Cybersecurity Awareness Campaigns • Prepare reports and recommendations for the enhancement of the Cybersecurity Framework • Contribution to the strengthening of Cybersecurity policies and regulations • Liaise with regional and international organizations

- Ensure security measures comply with relevant regulations, standards, and frameworks (e.g., ISO 27001, NIST CSF, CIS Controls, GDPR, and local cybersecurity laws).
- Develop and maintain documentation for security procedures, incident response playbooks, and system hardening guides.
- Participate in security audits, compliance reviews, and certification processes.

Network Security

- Design, implement, and maintain network security solutions, including firewalls, intrusion prevention systems (IPS), intrusion detection systems (IDS), and VPNs.
- Conduct regular audits of network configurations and security controls to ensure compliance with policies and best practices.
- Monitor network traffic for suspicious activity and respond to incidents in a timely manner.
- Manage secure network segmentation, access control lists (ACLs), and Zero Trust network configurations.

Cloud Security

- Develop and enforce cloud security policies and standards for public, private, and hybrid cloud environments.
- Configure and monitor security controls for major cloud platforms (e.g., Microsoft Azure, AWS, Google Cloud).
- Implement cloud-native security solutions, such as security posture management (CSPM), cloud workload protection (CWPP), and identity and access management (IAM).
- Conduct regular cloud security risk assessments and remediation plans.

Threat Management & Incident Response

- Perform vulnerability assessments, penetration testing, and security gap analyses.
- Detect, analyze, and respond to security incidents across on-premises and cloud environments.
- Lead incident investigations and provide post-incident reporting and recommendations.
- Maintain threat intelligence awareness to proactively defend against emerging cyber risks.

Collaboration & Training

- Collaborate with all stakeholders' application development teams to embed security into system and application design.
- Provide security awareness training to staff, focusing on secure network and cloud usage.

Perform any other duties assigned

Education

- Bachelor's degree in Computer Science, Information Technology, Cybersecurity, or a related field.
- Master's degree or specialized cybersecurity certifications is required.

Professional Certifications (Preferred)

- Network Security: Cisco CCNP Security, Fortinet NSE4+, Palo Alto Networks PCNSE.
- Cloud Security: Microsoft Certified: Azure Security Engineer Associate, AWS Certified Security – Specialty, Google Professional Cloud Security Engineer.
- General Cybersecurity: CISSP, CISM, CompTIA Security+, CEH.

Experience

- A minimum of 3 years in leadership position within the field of ICT
- Minimum 5 years of experience in cybersecurity engineering, with a strong emphasis on network and cloud security.
- Hands-on experience with enterprise firewalls, intrusion detection/prevention, endpoint protection, and SIEM platforms.
- Practical knowledge of cloud security tools, identity federation, and encryption technologies.
- Proven experience in security incident response and forensic investigation.

Knowledge and Skills:

In addition to the requirements above, the post holder must have the following skills:

- Strong analytical and problem-solving skills.
- Excellent understanding of TCP/IP, DNS, HTTP/S, and routing protocols.
- Knowledge of Zero Trust principles and micro-segmentation
- Working Knowledge of use of Artificial Intelligence in Cybersecurity
- Familiarity with DevSecOps practices and secure cloud deployment pipelines.
- Strong communication skills to explain technical concepts to non-technical stakeholders.
- Understanding of Cloud Computing and be familiar working in cloud platform.
- A working knowledge of Amazon Web Services would be preferred.

Salary: K39-41 ($82,116 - $89,952) per annum

Please send applications to:

Permanent Secretary
Ministry of Information, Communications, and Technology
P O BOX 186, NATIONAL ICT CENTER,
#3 C. A. PAUL SOUTHWELL INDUSTRIAL SITE
BASSETERRE, SAINT KITTS
Email: technology@gov.kn