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: pssec.moient@gov.kn

Job Description

Job Title: Security Engineer

Work Location: National ICT Centre

Division/Department: Technical Unit

Reports to: Director

Background: St. Kitts and Nevis is striving to become a digital economy; in so doing to accelerate the digital transformation agenda for Government, the Digital Services Network (DSN) is the cornerstone of this transformation to support the increase in the delivery of government digital services. The Digital Services Network (DSN) aims to revamp the current government wide area network (GWAN) structure into a fully shared and departmental-controlled network. Following a series of working sessions with department heads and lead network engineers, a consensus on the new DSN architecture was reached, outlining its benefits and requirements. The DSN have increase cybersecurity, reliable and redundant internet connections through the Internet Exchange, reduce cost in network monitoring and management. The DSN will enable the delivery of digital government services.

This DSN will include the establishment of two (2) core network sites, connecting 60 government department sites to the Edge network, four (4) core nodes on the nationwide fibre infrastructure, two (2) datacentres with capability to link with the St. Kitts and Nevis Internet Exchange. As the St. Kitts Internet Exchange Point (SKNIXP) is being integrated with the Government wide area network. The need for Network Security Engineers is critically important to maintain security across the government network.

Given that the intention for the IXP Coordinator focuses on the buildout and maintenance of the SKNIXP only, with the current direction to enhance the ICT Network Infrastructure and the need to ensure optimal performance and Cybersecurity is maintained to support additional digital services, there is need for the technical skillset of a Network Security Engineer. Security Engineers play a crucial role in Cybersecurity, working diligently to safeguard assets and mitigate risks. To accomplish this, the department will require a team of network

Administrators, Network Specialist, System administrators and Security Engineer qualified and experienced.

Description of Post: The Security Engineer is a critical post that needs to effectively design, implement and maintain robust network security solutions for the government digital services network, inclusive of the hybrid model of on-premise ICT infrastructure, data centers and hybrid cloud hosting services. It recognizes the integration of on-premises ICT Infrastructure with virtual server environment for the delivery of digital services.

Responsibilities include designing, implementing, and maintaining robust network security solutions across the whole of government (all ministries/ departments and agencies) to protect the government digital services network, systems and data. This role involves working in collaboration with the ICT technical committee or relevant committees or designated network and system administrators, Cybersecurity analyst to ensure the integrity, confidentiality, and availability of our network infrastructure in accordance with relevant Cybersecurity, ISO/IEC 27001:2022 standards and Data Privacy & Protection regulations.

Duties and Responsibilities for the post include, but are not limited to the following:

- **Strategy & Policy Development**: To contribute to the development of security strategies and policies that are aligned with Cybersecurity policies, regulations and ISO 27001 standards.

- **ICT Infrastructure & Network Security**: To improve the design and layout of the Server Room, IXP Room, Redundant Site and Data Center with enhanced Security Protocols, Network Architecture, ICT Infrastructure and Monitoring capabilities in the National ICT Centre to increase security, optimize performance for greater resilience and business continuity:
    - Network Device Audit and documentation using infrastructure management application
    - Implementing network segmentation to isolate sensitive data
    - Designing and upgrading network infrastructure resilience.
    - Modernizing and hardening Wi-Fi network infrastructure.
    - Designing and implementing security architectures for digital services and network infrastructures.
    - Securing all network devices based on vendor and industry configuration best practices.
    - Upgrading network device operating systems as guided by vendor recommendations.
    - Automating network device backup processes.
    - Monitoring network devices and alerting for network and service failures with deployed applications.

- Generating automated network performance reports using deployed applications.
- Performing network device audits and documentation using infrastructure management applications.
- Providing network support as requested by the local IT team.

- **Security Architecture**: To design a zero Trust Security Architecture for the Digital Services Network and Data Centre in collaboration with the government ministries and departments in tandem with the project team and key stakeholders.
  - Create a framework and standard for network and cloud security compliance
  - Perform risk assessment and vulnerability assessments and security audits
  - Conducting security assessments and audits to identify vulnerabilities and recommending remediation measures.
  - Monitoring network traffic for suspicious activity and responding to security incidents promptly in collaboration with the Cybersecurity Unit
  - Investigating security breaches and recommending preventive measures in collaboration with the Cybersecurity Unit
  - Preparing and maintaining documentation related to security policies, procedures, and incident reports.

- **Data Centre Security**: To plan and implement physical security, network security, data security, operational security across physical data centers and multi-cloud environments to protect applications, infrastructure, data, and users. This applies to existing data centers based on physical servers and on virtualized servers hosted with Government Private Cloud providers.

- **Technical Training:** To conduct training with the technical staff on all relevant system updates and modernization changes.

- **Emerging Technologies:** Evaluate and recommend new security solutions to improve the organization's security posture considering emerging technologies and trends in cybersecurity

- **Reporting:** Regularly reporting on the security status and threat landscape on the network to management. Recommend updates, resources, software and hardware devices to enhance the overall security posture

- **Disaster Recovery:** Contribute to the development and implementation of disaster recovery and business continuity plans to ensure the Digital Services Network and Data Centre is resilient to recover from cybersecurity incidents and other disasters.

Any other duty that may be assigned.

Education and/or Experience :

- Bachelor's degree in Computer Science, Information Technology, or a related field.
- At least 10 years' proven experience with network security or network engineering
- At least 10 years' experience working on the design and implementation of Data Centers and hybrid cloud infrastructure environment is required
- Possess certifications in Network Security which include one or more of the following: Certified Information Systems Security Professional (CISSP), Certified Information Security Manager (CISM), Certified Ethical Hacker (CEH), or CompTIA Security+.
- Strong knowledge of network protocols, firewalls, VPNs, IDS/IPS, and encryption.
- Proven hands-on experience with IPv4 and IPv6 networking
- Working knowledge and application of BGP transit peering, MPLS operations and SD-WAN security
- Experience working with Internet Exchange Points (IXPs), Wide Area Networks (GWAN) and Fibre-Option Communication, WiFi-Mesh Networking and Telecommunication Systems
- Masters' degree in Computer Science, Computer Networks, Cybersecurity, Telecommunications or related field would be an asset.
- Excellent problem-solving skills and attention to detail.
- Ability to work independently and as part of a team in a fast-paced environment.

Knowledge and Skills:

- Possess excellent communication skills with the ability to communicate technical and non-technical information to IT professional, managers and senior government officials
- Ability to perform penetration testing or to utilize the relevant digital tools to perform network security testing
- Certification in networking using security appliances including active, preventative and unified threat management systems, including Cisco (CNNA, CCNP, CCDP) and FortiNET (FCP-Network Security and FCA- CyberSecurity)
- Experience with cloud security and services for Amazon Web Services (AWS) and Microsoft Azure will be preferred.
- Knowledge of ISO 27001 standards and implementation within Data Centres
- Familiarity with regulatory requirements such as Data Protection, Cybersecurity and network protocols and security policies and standards
- Ability to prepare Technical Reports

Salary: (**K33-38) / (K39- K41)** ($64,092 - $78,768 / $82,116 - $89,952) **per annum**
The deadline for the receipt of application is **June 30th 2025**

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