

## **POSITION DESCRIPTION**

PNG Ports Corporation Limited

### **AM7004 - Cyber Security Officer**

**PNG Ports Corporation Limited (PNGPCL)** is a premier maritime service company in Papua New Guinea and is the largest port operator in the South West Pacific, outside Australia and New Zealand.

PNGPCL continues to develop the capacity of its workforce to deliver high-quality service to all stakeholders and is committed to attracting the highest calibre of professionals who can make a difference to the organization. PNGPCL provides a positive work environment and rewards employees who contribute to its business success.

PNGPCL is inviting exceptional candidates to apply for this key role based in Port Moresby:

#### **Cyber Security Officer**

Reporting to the Team Leader ICT Infrastructure, the Cyber Security Officer will provide support by updating the organisation information and data security and be responsible for overseeing information security, cybersecurity and IT risk management programs based on industry-accepted information security and risk management frameworks. This also includes designing and implementing security policies around the organisation's processes and procedures to safeguard information and data loss.

#### **Key Responsibilities:**

- Design strategies and defensive systems against intruders and monitor systems for unusual activities. Conduct counteractive protocols and report incidents
- Develop new layers of protection and update security systems and examine defensive systems and provide reports based on test results
- Keep updated with new trends and procedures and analyze new methods of intrusion
- Develop and implement information security standards, guidelines and procedures
- Maintain IT security controls documentation and make recommendations, create security policies and ensure they are implemented with support and mitigation during implementation
- Implement numerous security controls as part of cybersecurity remediation programs (ISO27001, Essential 8, ASD Top 35 etc)
- Responsible for the implementation of Azure and M365 cloud security solutions
- Responsible for cyber security projects and ensure they meet cybersecurity objectives
- Provide standby support for cyber security incident response and implement vulnerability assessment, configuration audit of operating systems, web server and databases
- Track vulnerabilities and collaborate with internal IT network team to ensure closure
- Take care of day-to-day operations and data structures by overseeing operational performance, conduct software upgrades, document configuration and system specification
- Conduct threat and risk analysis and provide essential suggestions. Perform research, testing, evaluation and deployment of security procedures. Responsible for designing security training materials and organize training sessions for other departments
- Collect and analyze data and assist in eliminating risk, performance and capacity issues. Collaborate and evaluate security programs for the organization
- Conduct risk assessment and business impact analysis on new systems and technologies and assist the design and development of security features for system architectures
- Take care of built-in security systems to software, hardware and components and develop unique strategies for software systems, networks, data centers and hardware.

**Expected Competencies:**

- Degree in the field of Computer Science or Information Technology, Computer Engineering or Information Systems Management. Post-Graduate qualification is desirable
- Professional certifications (Microsoft Certified Systems Administrator (MCSA), Microsoft Certified System Engineer (MCSE), and VMware Certified Professional (VCP) is desirable
- Minimum 5 years of experience in a similar role
- In-depth knowledge and experience in cybersecurity processes and protocols
- In-depth technical knowledge of server and client operating systems
- In-depth knowledge of Application Security, Information Security, Infrastructure Security, Network Security and User Education
- In-depth knowledge around cyber resilience strategy to help the organisation to reduce risks, financial impact and reputational damages
- Understanding of Information Security Policies and Standards
- Proven experience in ICT security systems planning, development and administration
- Knowledgeable in system security (intrusion detection systems) and data backup and recovery
- Experience with IT security – cloud base and on premises
- Proven analytical, evaluative and problem-solving abilities including experience in ERP systems

**This position is open to PNG citizens only.**

**APPLY NOW**

Please visit our website: <https://vanguard.com.pg/vacancies/>

Complete the application form and follow the website instructions to forward to us including a detailed CV and copy of a current police clearance certificate. We encourage applicants to request a full PD from our office to review before applying.

Alternatively, please call us on (+675) 7500 7500 or email [recruitment@vanguard.com.pg](mailto:recruitment@vanguard.com.pg)

**Applications close COB Friday 3<sup>rd</sup> March 2023**

**Only shortlisted applicants will be contacted**

To apply for this position:

- Download and complete the Application Form from <http://www.vanguard.com.pg>.
- Email the application to [recruitment@vanguard.com.pg](mailto:recruitment@vanguard.com.pg) together with a copy of your CV in MS Word format.

**Note: Do not include copies of any other documents. You will be asked to provide the originals of certificates etc if you are selected for Interview**