FORM 1.5

PAPUA NEW GUINEA CUSTOMS SERVICE

JOB DESCRIPTION

1. IDENTIFICATION

AGENCY: PNG CUSTOMS SERVICE	**SYS. POS. NO:**	**REF. NO:**	
		CUIF 024	
	DESIGNATION/CLASSIFICATION: OFFICER – CYBER OPERATIONS CUS 08		
WING: OFFICE OF THE CHIEF COMMISSIONER	**LOCAL DESIGNATION:** OFFICER – CYBER OPERATIONS		
DIVISION:	**REPORTING TO:**	**SYS. POS. NO:**	**REF NO:**
INTERNAL AFFAIRS	MANAGER CYBER OPERATIONS	**CUIF 022**	
SECTION: INTENAL AFFAIRS	**LOCATION:** PORT MORESBY		

HISTORY OF POSITION

FILE REF.	DATE OF VARIATION	DETAILS

2. PURPOSE

The PNG Customs Service is responsible for protecting PNG against risks and threats to its border; facilitating the legitimate movement of people and goods; and collecting revenue for the State.

The primary responsibility of the Internal Affairs division is to investigate allegations of professional misconduct, criminal activities and policy violation committed by officers and its external stakeholders. The division functions to ensure self-governance, preserve public trust, and maintain organisation integrity.

The position of Officer Cyber Operations is responsible for monitoring, protecting, and maintaining the organization's information systems, networks, and digital assets against cyber threats. The role supports the implementation of cyber security policies, incident response activities, security monitoring, vulnerability management, and user awareness programs to ensure the confidentiality, integrity, and availability of organizational information.

3. DIMENSIONS

Financial: Is not a financial delegate but can make expenditure requests for goods and services as an Authorised Requisitioning Officer (ARO) under the Public Finance Management Act and is required to assist in the development of annual budget proposals for the division.

Staff: Is not responsible for any subordinates
Others: Is responsible for any official asset(s) allocated to the division.

4. PRINCIPLE ACCOUNTABILITIES

1. Development of strategies for the division that are in line with the organisation's goals and objectives.
2. Planning and monitoring of operational activities for the Internal Affairs division.
3. Administration of the Internal Affairs division.

5. MAJOR DUTIES

1. Security Monitoring and operations

- Monitor network, serve, and endpoint security systems.
- Identify, investigate, and respond to cyber security alerts and incidents.
- Conduct routine security reviews and log analysis.
- Escalate significant security threats to management.

2. Cyber Incident Response

- Assist in detecting, containing, and recovering from cyber incidents.
- Maintain incident records and prepare incident reports.
- Support digital evidence collection and preservation.
- Participate in cyber security investigations.

3. Vulnerability Management

- Perform vulnerability scans and security assessments.
- Monitor and track remediation activities.
- Recommend corrective actions to reduce cyber risks.
- Assist with system hardening and security improvements.

4. **Security Compliance and Governance**

- Support implementation of cyber security policies, standards, and procedures.
- Ensure compliance with government ICT and information security requirements.
- Assist in conducting security audits and risk assessments.
- Maintain cyber security documentation and records.

5. User Awareness and Training

- Promote cyber security awareness across the organization.
- Deliver basic cyber security training and guidance.
- Support phishing awareness campaigns and exercises.
- Provide security advice to staff regarding safe ICT practices.

6. **Business Continuity and Resilience**
    - Support backup and recovery processes.
    - Assist in disaster recovery planning and testing.
    - Monitor cyber risks affecting critical business systems.

7. NATURE AND SCOPE

The position of Officer Cyber Operations is responsible for monitoring, protecting, and maintaining the organization's information systems, networks, and digital assets against cyber threats. The role supports the implementation of cyber security policies, incident response activities, security monitoring, vulnerability management, and user awareness programs to ensure the confidentiality, integrity, and availability of organizational information.

WORKING RELATIONSHIP

a. Internal

Develop and maintain liaison with;

- Business Unit
- Executive Management
- Risk and Compliance Teams
- Other relevant Divisions;

b. External

Develop and maintain liaison with other external stakeholders;

- Government ICT Agencies
- Law Enforcement Agencies
- Cyber Security partners and vendors
- Internet Service Providers
- Other relevant external stakeholders

8. AUTHORITY

1. Access cyber security monitoring systems.
2. Recommend security controls and corrective actions.
3. Escalate cyber incidents in accordance with approved procedures.

9. WORK ENVIRONMENT

This is a Cyber operation position and will require the incumbent to be a team player and possess sound interpersonal and numerical skills.

10. CONSTRAINTS FRAMEWORK AND BOUNDARIES

This role will require the incumbent to maintain due diligence of all work carried out. He/she will have access to government & personal data and information that must remain confidential and secure at all times. The incumbent must also adhere to all governance policies and standard operating procedures.

This position is bound by the following Rules/Procedures.	• Code of Conduct and Ethics • Customs Administrative Orders • Customs Act & Regulations • Other Legislation enforced at the border • Public Finances Management Act • PNG Customs Service Act • Relevant Standard Operating Procedures and Policies
This position is responsible for making the following Decisions for the division.	
This position can make the following Recommendations for the Section.	• Operations Plan • Request for Resources

11. CHALLENGES

The role requires a high level of commitment and integrity, to ensure deadlines and turnaround times are met. The incumbent must be a team player, work under pressure and may be required to work after hours.

12. QUALIFICATIONS, EXPERIENCE AND SKILLS

a. Qualifications

- Diploma or Degree in Cyber Security, Information Technology, Computer Science, or related field.
- Industry certifications such as:
    - CompTIA Security+
    - Certified Ethical Hacker (CEH)
    - Microsoft Security Certifications
    - CISSP (Associate or Full)
    - GIAC Certifications

b. Knowledge

- Knowledge of network security, operating systems, and cyber threats.
- Proficient in the use of all Microsoft applications
- Valid class three (3) drivers' licence is acceptable

c. Skills

- Cyber threat analysis.
- Incident response and investigation.
- Risk assessment and problem-solving.
- Technical troubleshooting.
- Report writing and documentation.
- Attention to detail.
- Communication and stakeholder engagement.
- Ability to work under pressure during cyber incidents.

d. Work Experience

- Preferably (2-3) years' work experience in ICT or cyber security operations.
- Experience with security tools such as antivirus, firewalls, SIEM, or endpoint protection platforms.