DEPARTMENT OF COMMUNICATION AND INFORMATION

JOB DESCRIPTION

1. IDENTIFICATION

	POSN. NO: **PMU**	**REF. NO:** PMU
DEPARTMENT: Information and Communication Technology	**DESIGNATION/CLASSIFICATION:** Manager Computer Emergency Response Team (CERT)	
OFFICE/AGENCY: Digital Government & Information Delivery Wing	**LOCAL DESIGNATION:** Manager Computer Emergency Response Team (CERT)	
DIVISION: Cyber Security	**IMMEDIATE SUPERVISOR:** Executive Manager	**POS. NO:**
BRANCH: Cyber Security	**HIGHEST SUBORDINATE** Deputy Secretary	
SECTION:	**LOCATION** Waigani	

HISTORY OF POSITION

FILE NO.	DATE OF VARIATION	DETAILS
PMU	30/03/2023	Short Term Contract

2. PURPOSE

The CERT Manager will be responsible for leading and managing the Computer Emergency Response Team, ensuring the effective detection, prevention, and mitigation of cybersecurity threats and incidents for critical infrastructure and services across all public bodies

3. DIMENSIONS

The CERT Manager will oversee the CERT team and coordinate efforts to protect digital government infrastructure, systems, and data from cybersecurity threats and incidents.

4. PRINCIPAL ACCOUNTABILITIES

The CERT Manager will be accountable for the successful operation of the Computer Emergency Response Team, ensuring that cybersecurity measures align with the strategic objectives of the digital government initiatives.

5. MAJOR DUTIES

- Lead and manage the CERT team, ensuring effective detection, prevention, and mitigation of cybersecurity threats and incidents
- Develop and implement cybersecurity policies, procedures, and best practices
- Coordinate incident response activities, ensuring timely and effective resolution
- Collaborate with internal and external stakeholders to share threat intelligence and enhance cybersecurity measures
- Conduct regular vulnerability assessments and penetration tests to identify and address potential security risks
- Provide training and guidance to department staff on cybersecurity best practices
- Monitor and evaluate the effectiveness of cybersecurity measures and recommend improvements as needed

6. NATURE AND SCOPE

6.1 WORKING RELATIONSHIPS

Internal

Internal: Work closely with colleagues within the Digital Government and Information Delivery Wing, particularly the cyber analysts within the NCSC

External

External: Liaise with external stakeholders, including government agencies, private sector partners, and vendors, to share threat intelligence, coordinate incident response efforts, and enhance cybersecurity measures.

6.2 WORK ENVIRONMENT

The CERT Manager will work in an office setting, with occasional travel to other locations as required by cybersecurity needs.

7.0 CONSTRAINTS FRAMEWORK AND BOUNDARIES

Rules and Procedures

Adhere to departmental policies, guidelines, and best practices in cybersecurity and incident response management.

Decision
Make decisions regarding cybersecurity measures and incident response priorities within the scope of assigned responsibilities and in line with departmental guidelines and objectives.

Recommendations
Provide recommendations on cybersecurity solutions, tools, and processes to improve the department's cybersecurity posture.

8.0CHALLENGES

Key Challenges for the Job include:

- Balancing the need for security with the demands of digital government projects
- Staying current with the rapidly changing landscape of cybersecurity threats and technology
- Ensuring effective communication and coordination among diverse stakeholders

9.0 QUALIFICATIONS, EXPERIENCES AND SKILLS

9.1Qualifications

Qualifications: A Bachelor's degree in Computer Science, Information Technology, or a related field. Relevant cybersecurity certifications, such as CISSP, CISM, or GIAC, are highly desirable.

9.2 Knowledge

Knowledge: Strong knowledge of cybersecurity principles, methodologies, and tools. Familiarity with digital government initiatives and policies is an asset.

9.3Skills

Skills: Excellent leadership, problem-solving, analytical, and communication skills. Ability to work effectively in a team and independently.

9.4Experience

Work Experience: At least 5 years of relevant experience in cybersecurity, with a focus on incident response and management, preferably in a government or public sector setting.