Va.No.PNCC2025.06

Vacancy Announcement

*It is the policy of Palau National Communications Corporation (PNCC) that qualified Republic of Palau Citizens be given **EQUAL EMPLOYMENT** OPPORTUNITY for employment consideration, with other country nationals utilized in positions for which qualified Republic of Palau Citizens are not available.*

Open Date: AUGUST 27, 2025	Close Date: SEPTEMBER 10, 2025
Position Title	**CYBERSECURITY SPECIALIST** **"FULL TIME CONTRACTUAL EMPLOYMENT"**
Salary Range	**Commensurate with Experience**

DUTIES SUMMARY:

PNCC is seeking a highly motivated and skilled Cybersecurity Specialist to lead and strengthen our cyber defense capabilities. This role offers an excellent opportunity to apply advanced cybersecurity knowledge, gained through both academic study and hands-on industry experience, to protect the Republic of Palau's largest telecommunications network.

The Cybersecurity Specialist will be responsible for monitoring, analyzing, and improving PNCC's security posture across IT, IP networking, and critical telecom infrastructure. The role blends technical expertise with strategic thinking, requiring someone who can implement security best practices, work collaboratively across departments, and continually evolve our defenses in response to emerging threats.

We are looking for a self-starter who is passionate about cybersecurity, eager to apply their Master's-level knowledge in a real-world telco environment, and keen to learn from PNCC's experienced technical and operational teams.

KEY DUTIES AND RESPONSIBILITIES:

Cybersecurity Monitoring & Threat Detection

- Monitor PNCC's IT and network environments for potential threats, vulnerabilities, and suspicious activity.
- Utilize SIEM, intrusion detection/prevention systems, and other monitoring tools to identify security incidents in real time.
- Collaborate with the NOC, IT, and IP networking teams to respond to security alerts and incidents.

Incident Response & Investigation

- Lead and coordinate the incident response process, ensuring rapid containment and resolution of security events.
- Conduct post-incident analysis to identify root causes and recommend remediation.
- Maintain and improve PNCC's incident response playbooks.

Security Architecture & Policy Development

- Review and strengthen PNCC's security policies, standards, and procedures.
- Work closely with the IT and IP networking teams to design secure architectures for systems, networks, and applications.
- Ensure that new systems and upgrades are evaluated for security risk before deployment.

Vulnerability Management

- Perform vulnerability assessments and penetration tests to identify security weaknesses.
- Work with technical teams to prioritize and implement remediation measures.
- Keep up to date with the latest vulnerability disclosures and threat intelligence.

Awareness & Training

- Support cybersecurity awareness programs for PNCC staff.
- Attend cybersecurity conferences
- Provide technical training and guidance to IT/networking teams to improve security practices.

Compliance & Best Practices

- Ensure PNCC is aligned with relevant international standards (e.g., NIST CSF, ISO 27001).
- Assist in preparing for and responding to cybersecurity audits and compliance checks.

QUALIFICATION REQUIREMENTS

EDUCATION AND EXPERIENCE:

- Master's degree in Cybersecurity (or related discipline).
- Several years of hands-on IT and networking experience, ideally in a telecommunications or enterprise environment.
- Solid understanding of cybersecurity principles, threat landscapes, and security best practices.
- Knowledge of common attack vectors, intrusion detection systems, firewalls, and endpoint protection tools.
- Experience with coding or scripting (e.g., Python, PowerShell, Bash) for automation and analysis.
- Strong problem-solving and analytical skills.
- Excellent communication and teamwork abilities.

Desirable:

- Experience with telecom-specific security issues (e.g., SS7/Diameter security, mobile core network protection).
- Familiarity with cloud security principles and hybrid infrastructure security.
- Relevant security certifications (e.g., CompTIA Security+, CISSP, CEH, GIAC).
- Experience participating in incident response exercises or real-world security incidents.

LICENSES AND OTHER REQUIREMENTS:

Possession of a valid Republic of Palau's driver's license.

HOW TO APPLY:

EMPLOYMENT APPLICATION FORMS ARE AVAILABLE AT THE PNCC HUMAN RESOURCES OFFICE LOCATED IN NGERUSAR, AIRAI STATE AND THE PNCC KOROR BUSINESS OFFICE (KBO) LOCATED IN DOWNTOWN KOROR ACROSS FORMER PALAU NATIONAL CONGRESS BUILDING OR SEND RESUMES TO THE FOLLOWING ADDRESS:

HUMAN RESOURCES OFFICE
PALAU NATIONAL COMMUNICATIONS CORPORATION
P.O. BOX 99 – ONE AIRPORT ROAD
KOROR, REPUBLIC OF PALAU 96940
EMAIL: mchin@pnccpalau.com