Ministry of Trade, Co-operatives, Small and Medium Enterprises and Communications

JOB DESCRIPTION

MTCSMEC 63/2024: DIRECTOR COMPUTER EMERGENCY RESPONSE TEAM (CERT) - DEPARTMENT OF COMMUNICATIONS

Corporate Information

1. Position Level:	Band K
2. Salary Range	$ 59,945.18 - $76,852.80 (Step 1 – Step 4)
3. Duty Station:	Suva
4. Reporting Responsibilities	a) Reports to the Director-General (Digital Government Transformation, Cybersecurity and Communications) b) Liaises with Permanent Secretary, Heads of Department, Government Agencies, Ministry Staff, other development partners, global CERTs and private sector stakeholders. c) Subordinates: All staff of the CERT

POSITION PURPOSE

The National Computer Emergency Response Team (CERT) Director plays a crucial role in enhancing the national cybersecurity posture. This position is responsible for establishing and leading the CERT, ensuring its effective operation in line with the National Cybersecurity Strategy. This position will fully establish and lead the team which works to prevent, respond to, recover from and mitigate cybersecurity threats. This position is responsible for developing and implementing policies, procedures, and processes. The CERT Director will be required to coordinate with the relevant Ministries and stakeholders, and to share the Government's cyber vision and to solicit their involvement in achieving higher levels of cyber resilience. The Director will ensure that CERT Fiji has the technical and operational capability to leverage the international network of CERTs and CERT organisations and to contribute to our global commitment for a safe and secure cyberspace.

KEY RESPONSIBILITIES

The position will achieve its purpose through the following key duties:

Leadership and Management:

- Establish, maintain, and enhance relationships with relevant stakeholders including across government, academia, private sector, civil society and counterpart CERTs.
- Oversee, supervise and supports the CERT team, fostering a collaborative and efficient work environment.
- Ensures service level commitments and the timely delivery of CERT services and initiatives to meet CERT constituent.
- Proactively identify, manage, and mitigate risks associated with cybersecurity incidents.

- Create and maintain an Incident Response Plan and develop and ensure adherence to all related laws, policies and guidelines.
- Manage the CERT's budget effectively, staying within allocated resources and achieving established goals.
- Deliver briefings to senior government officials and relevant stakeholders.

Strategic Planning and Development:

- Develop and implement the strategic direction for the CERT, aligning with international best practices, the national cybersecurity strategy and the CERT Study Report.
- To advise on the resource allocation for the CERT
- Create and implement policies, procedures, and processes for incident response and management.
- Develop technical security materials to raise cyber awareness and preparedness for security incidents.
- Analyse reports and relevant information to propose strategic and technical recommendations for improving the national cybersecurity posture.

Collaboration and Information Sharing:

- Represent Fiji at regional and international events, forums and activities
- Collaborating with national and international CERTs, law enforcement and policy agencies, and CERT constituents to share threat intelligence and coordinate cyber incident responses.
- Produce periodic high quality ad-hoc reports on the operations of the CERT

Training and Development:

- Deliver training to staff on emerging cybersecurity trends and threats.
- Conduct regular incident drills to simulate various cyber threats and enhance team response capabilities.
- Develop training materials, including those tailored to the Fiji context, on security awareness and incident response.
- Build trust and understanding of CERT functions and objectives with key stakeholders
- Any other duties as reasonably requested by the Supervisor

KEY PERFORMANCE INDICATORS

Performance will be measured through the following indicators:

- Implement and maintain effective operational policies, processes, and procedures for incident response and management within defined timelines in line with the National Cybersecurity Strategy and other national strategies, policies and laws
- Develop and implement a strategic plan for the continuous improvement of the CERT, aligned with international best practices within the defined timeframe.

- Timely implementation of the national cybersecurity strategy and other strategies related to the functions of the CERT.
- Proactive identification and mitigation of cybersecurity risks, as they are detected to avoid system breaches and service interruption.
- Effectively communicate complex technical information to audiences with varying levels of technical knowledge, fostering understanding and collaboration for involved stakeholders.
- aligned with the National Cybersecurity Strategy.
- Prepare and present clear and concise reports outlining the CERT's activities, performance metrics, and progress towards achieving established goals to the Director General regularly.
- Regularly monitor the effectiveness of the CERT's activities, including response times, incident resolution rates, and stakeholder satisfaction.
- Ensure an integrated response to cyber security events and ensuring that the strategic approach and management of CERT's incident response capability and supporting infrastructure is successful
- Engages with the Cyber Security Community, Senior Government officials and Senior Executives within Public and Private organisations to ensure the CERT's relationships, mission and future requirements are able to be met
- Builds and maintains effective relationships and partnerships with national and international organisations to identify and share best practice information and to promote the CERT
- Engage with other national CERTs and international stakeholders in alignment with CERT's interests
- Represent CERT Fiji at domestic and international events, forums and activities
- Build trust and understanding of CERT's functions and objectives with key stakeholders and develop strong relationships with senior managers across the public and private sectors
- Represents CERT views and protects its reputation in external interactions

PERSONS SPECIFICATION

In addition to a Master's or a Post Graduate Degree in Cybersecurity/ Computer Science / Information Technology/ Information Systems or a related field together with the following Knowledge, Experience, Skills and Abilities required to successfully undertake this role are:

Knowledge and Experience

1. With a Master's degree at least 7 years' demonstrated and relevant cyber experience in ICT and cybersecurity at a managerial role; or, with a Bachelor's degree, at least 5 years demonstrated and relevant experience in cybersecurity in a managerial role, especially in operational response environment and experience in disaster recovery
2. Experience of working and influencing at a senior levels on information/cyber security issues
3. Politically Astute can effectively manoeuvre through complex situations
4. A proven track record of experience and achievement as a strategic and operational leader:
   - strong interpersonal skills that will enable you to build credible, respected relationships with key stakeholders including Ministers, senior managers, team members, staff in partner

agencies and key external stakeholders and opinion leaders, and act as the public face of the CERT
   - influencing at senior levels and working with stakeholders to deliver outcomes
   - understanding and navigating systems to overcome roadblocks and accomplish objectives
   - leading and managing change in response to developments in the cyber security environment
5. Ability to engage with both security practitioners and business leaders with credibility
6. Technical understanding of cyber security issues and knowledge of risk assessment
7. A relevant tertiary qualification or extensive and comparable relevant experience

Skills and Abilities

1. Ability to multi-task and proficiently in a fast-paced, complex, dynamic and multicultural environment.
2. Excellent leadership skills and ability to lead strategic management and change management together with strong organisational skills and the ability to adapt rapidly and be self-directed.
3. Excellent relationship and communication management skills, with the ability to communicate appropriately and comfortably with stakeholders at all levels and of various technical knowledge.
4. Demonstrated ability to foster the development of communities of practice and play a leadership and organising role in international and multistakeholder contexts.
5. Build and maintain relationships with stakeholders in Pacific, including through the Pacific Cybersecurity Operational Network (PaCSON) and other relevant fora.
6. Good team player, confident and self-motivated with attention to detail and excellent problem-solving skills.
7. Excellent verbal, written communication and presentation skills and demonstrated ability to maintain confidentiality and neutrality in a sensitive environment.
8. Ability to present highly technical information to non-technical audiences and to interact professionally with a diverse group, executives, managers, and subject matter experts.

PERSONAL CHARACTER

Applicants for employment must be of good character, with a background that demonstrates their commitment to the Civil Service Values contained in the Fijian Constitution. Applicants must also be Fijian Citizens, under age 60 years, in sound health and with a clear police record. The selected applicant will be required to provide a medical certificate and police clearance prior to taking up duty.