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

JOB DESCRIPTION

MTCSMEC 65/2024: INCIDENT RESPONSE SPECIALIST (COMPUTER EMERGENCY RESPONSE TEAM), DEPARTMENT OF COMMUNICATIONS

Corporate Information

1. Position Level:	Band I (Step1 – 4)
2. Salary Range	$43,296.63 - 55,508.50
3. Duty Station:	Suva
4. Reporting Responsibilities	a) Reports to the Director CERT b) Liaises with the Director General, Permanent Secretary, other development partners, and private sector stakeholders c) Subordinates: none

POSITION PURPOSE

The candidate will be responsible for taking the lead on triaging, managing and investigating cyber incidents which will include ensuring that appropriate advice is sent out to affected parties, to warn them and inform them on how to mitigate the threat. The candidate must possess the ability to investigate and determine the best course of action to take. The complexities include making holistic decisions when involving stakeholders and being well-informed to make recommendations for important decisions made on experience. Given the rapid cyber evolution there is a requirement for the candidate to stay updated on incidents locally, regionally and globally, and efforts on combatting cybercrime. The candidate will be expected to make sound recommendations for cyber security strategy, be available on a roster, and maintain confidentiality and neutrality in a sensitive environment.

KEY RESPONSIBILITIES

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

1. To plan, execute, assess and monitor all tasks assigned under the National Computer Emergency Response Team (CERT)
2. Incident response and security monitoring as assigned to the National Computer Emergency Response Team (CERT)
3. Regular reporting retrieved from the monitoring tools of the CERT and to communicate these effectively to the CERT constituents
4. Assist in the strategic Policy and Security Program Development that aligns with the recommendations from the National Cyber Security Strategy and results in a more cyber-resilient nation
5. Awareness Training and Development to build cyber capacity for the CERT and CERT Constituents
6. Communication in the form of awareness campaigns, collaborating with partner CERTs to best convey information to the public
7. Continuous Improvement of the National CERT and its team members

KEY PERFORMANCE INDICATORS

Performance will be measured through the following indicators:

1. Conduct research and continuously improve investigative methodologies and techniques for managing security incidents on the CERT;
2. Directing the development and maintenance of the incident management systems of the CERT
3. Responsible for planning and coordinating all the activities required to manage and analyse incidents, including serious national Incidents within defined timeframes, including:
    - Triage and response to incidents
    - Interpreting threat intelligence
    - Incident referral (Domestic & International)
    - Prepare, document and maintain incident reports and investigative plans
4. Serious cyber incident response and coordination, including:
    - Leading the unit's technical response, and thereby being instrumental in the coordination of Fiji's overall response to serious cyber incidents as assigned to the CERT
    - Conducting and Supporting briefings to senior executives
    - Communicating with technical and non-technical audience

5. Issue advisories regarding new threats and vulnerabilities to CERT constituents;
6. Collaborate with internal and external entities for incident response for minimal downtime and to restore services efficiently;
7. Be available as per call roster in cases of cyber incidents; and
8. Transfers knowledge and learning to the team and CERT constituents.
9. Engage and develop direct relationship with other international CERT.

PERSONS SPECIFICATION

In addition to Bachelor's Degree in Computer Science/ Information Systems/ Network Security together with the following Knowledge, Experience, Skills and Abilities required to successfully undertake this role are:

Knowledge and Experience

1. At least 3 years' experience in working with information security systems and policies or equivalent combination of education and work experience.
2. Sound knowledge of Cybersecurity Standards and Framework.
3. Working knowledge of incident management and response processes.
4. Proven capability to develop and maintain SOP's and documentation.
5. Detailed understanding of information security management practices.
6. Understanding of security architecture and models.

Skills and Abilities

1. Ability to plan, organise, evaluate and analyse reports and other relevant information to propose strategic recommendations.
2. Ability to co-ordinate programs and activities to achieve the desired goals and objectives of Government programs.
3. Ability to identify and prioritise cyber security issues and work effectively with others to achieve positive outcomes.
4. Ability formulate and administer policies and initiatives.
5. Ability to work in a challenging environment and willingness to work beyond the call of duty.

6. Ability to find ways of solving or anticipating problems.
7. Deep technical skills in at least one of these areas: system administration, network administration, programming, incident response, or intrusion detection.
8. A solid understanding of security controls and how to mitigate threats.

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.