GOVERNMENT OF KIRIBATI

POSITION DESCRIPTION

1. **Ministry:** Ministry of Information, Communication, Transport and Tourism Development
2. **Position Title:** Information Security Analyst
3. **Salary Level:** L9-7
4. **Division:** ICT Unit
5. **Reports To:** Senior Information Security Analyst
6. **Direct Reports:** Senior Information Security Analyst
7. **Primary Objective of the Position:** Coordinate CERT awareness programs, engagement with stakeholders and support Senior Information Security Analyst in Cybersecurity Incident Handling.

8. **Position Overview**

9. Financial: N/A

10 Legal: N/A

11. Internal Stakeholders:
    - Permanent Secretary
    - Director of ICT
    - MICTTD Staff

To be referred to Manager:
- Progress report.
- Implementation of work plan

12. External Stakeholders:
    - Telecom companies i.e. ATHKL, Oceanlink
    - Banking institutions i.e. ANZ
    - Public

To be referred to Manager
- Membership and involvement to those entities.
- Assistance to be provided to the stakeholders.
- Any other activities required of him by these bodies.

This is position description provides a comprehensive, but not exhaustive, outline of the key activities of the role. It is an expectation that you may be required to perform additional duties as required.

Approved by:	Date of Issue:

13. KEY ACCOUNTABILITIES *(Include linkage to KDP, MOP and Divisional Plan)*

- *KDP/KPA:*
- *MOP Outcome:*
- *Divisional/Departmental/Unit Plan:*

Key Result Area/Major Responsibilities	Major Activities/Duties	Performance Measures/Outcomes
Incident Validation and Classification	• To provide technical proof that an event is a security incident, network or hardware error and identify the potential security impact and damage on the Confidentiality, Availability, and/or Integrity of information assets in an area the CSIRT	Determine whether a reported event is indeed an incident that needs to be handled or whether the report can be registered in the relevant systems and closed without further action for the CSIRT or passed on to a relevant entity. Derive particulars of the events that have lead the constituent to believe that a security incident has indeed occurred and determine whether there is malicious intent or if there is a different reason – such as misconfiguration or hardware failure.
Information Collection	• Collection of reports regarding malicious or suspicious events and incident reports from constituents and 3rd parties (such as other security teams or commercial intelligence feeds), whether manual, automated or machine-readable forms. • Gathering and cataloguing of digital data that may be, but are not guaranteed to be, useful in understanding incident activity (e.g., disk images, files, network logs/flows).	Incident report, digital data and other data types (non-digital) related to the incidents are collected and stored.
Coordination and reporting	• Communicating with media to explain what happened in a given incident in a manner suitable	Information are distributed to internally and externally of the CERT in order to

	for release to the public. This typically means simplifying the issues and leave out confidential information, but still give a clear picture of the situation. This can be on behalf of the constituent or on behalf of the CERT itself. It is important that the CERT has predefined processes with its stakeholder communication department.	assist others in the detection, protection or remediation of on-going activities from adversaries.

10. Key Challenges

- Willing to work 24x7 or on-call duty (depending on the service model)
- Maximum of travelling distance (in case of emergency availability in the office; maximum travelling time)
- Level of education
- Experience in working in the field of IT security

11. Selection Criteria

11.1 PQR (Position Qualification Requirement):
Education:

1. Bachelor Degree in Computing Science AND Information System.

Experience: 3 years working experience OR proven knowledge and experience in Networking Security and Administration.

Job Training:

Prerequisite:

11.2 Key Attributes (Personal Qualities):

1. **Knowledge and Skills**
   - Broad knowledge of Internet technology and protocols
   - Linux and Unix System (depending on the equipment of the constituency)
   - Windows System (depending on the equipment of the constituency)
   - Network infrastructure equipment (Router, switeches, DNS, Proxy, Mail, etc)
   - Internet applications (SMTP, HTTP(s), FTP, telnet, SSH, etc)

This is position description provides a comprehensive, but not exhaustive, outline of the key activities of the role. It is an expectation that you may be required to perform additional duties as required.

Approved by:	Date of Issue:

- Security threats (DDos, Phishing, Defacing, sniffing, etc.)
- Risk assessment and practical implentations

2. **Attributes**
   - Flexible, creative and a good team spirit
   - Strong analytical skills
   - Ability to explain difficult technical matters in easy wording
   - A good feeling for confidentiality and working in a procedural matter
   - Good organizational skills
   - Stress durable
   - Strong communicative and writing skills
   - Open minded and willing to learn

This is position description provides a comprehensive, but not exhaustive, outline of the key activities of the role. It is an expectation that you may be required to perform additional duties as required.

Approved by:	Date of Issue: