GOVERNMENT OF KIRIBATI

POSITION DESCRIPTION

1. Ministry: Ministry of Information, Communication, Transport and Tourism Development		
2. Position Title: Senior Information Security Analyst	**3. Salary Level:** L6-5	**4. Division:** ICT Unit
5. **Reports To:** Chief Information Security Officer	**6. Direct Reports:** Information Security Analyst	
7. **Primary Objective of the Position:** Manage CERT Operations such as handling of every type of information security incident, provide technical and operational recommendations and advisories, awareness raising, training and consultancy.		

8. Position Overview	
9. Financial: N/A	10 Legal: N/A
11. Internal Stakeholders: • Permanent Secretary • Director of ICT • MICT Staff To be referred to Manager: • Progress report. • Activity plans • Divisional Budget	12. External Stakeholders: • Telecom companies i.e. Vodafone, Oceanlink • Internet Service providers • 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 handling	• Conclusively verifying that a reported incident in fact occurred and has had some impact on the involved systems and is relevant to the CERT's mandate • Documenting information about actions taken to resolve an incident, including critical information collected, analysis performed, remediation and mitigation steps taken, closure and resolution	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.
Incident Analysis	• To identify the size and scope of the incident to include affected parts of the infrastructure, services, data, and department or organization. A general approach to remediation can be made based on this analysis • Find measures to stop an ongoing issue, e.g. close a security hole or stop a malicious process. • Define a plan to restore impacted services to full functionality without reopening the original security issue	The (potential) damage that an incident has incurred or might incur is identified. Identified not only technical aspects, but also any media coverage, loss of trust or credibility and any reputational damage.

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:**

Restore confidentiality, integrity and availability	• Restore the all systems to full functionality • Stopping immediate damage and limiting the extent of malicious activity through short-term tactical actions (for example, blocking or filtering traffic); can also involve regaining control of systems. • Preventing further damage through eradication, implementing a workaround, or implementing more in-depth and comprehensive containment strategies. • Implementing changes in the affected domain, infrastructure or network necessary to fix and prevent this type of activity from reoccurring. This includes strengthening the organizational defensive posture and operational readiness by policy changes and additional training and education. • Restoring the integrity of affected systems and returning the affected data, systems and networks to a non-degraded operational state.	Services are restored to full capacity. Any detected vulnerabilities that lead to the original incident are closed.
Cybersecurity Awareness	• Lead the development of cybersecurity awareness materials for government, private sector and the general public • Organise and coordinate national cybersecurity awareness campaigns – communities & schools. • Lead the develop multimedia awareness contents including radio, social media, and printed materials.	Government, private sector, and public have sufficient cybersecurity knowledge.
Cybersecurity Capacity Building	• Analyse and identify skill gap in Cybersecurity across government. • Lead the development of plans and strategy for Cybersecurity capacity building for all of government. • Lead the development and plan for Cybersecurity inclusion in Education curricula	Officials and students have sound knowledge on Cybersecurity and internet safety

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:**

Cybercrime advisory	• Provide general and technical advisory on cybercrime to the government, including law enforcement officers, the judiciary, and prosecutors. • Review and improve the Cybercrime Act	Advisory rendered on cybercrime matters, including review and improvement to the Cybercrime Act.
Cybercrime technical analysis	• Provide and render technical analysis for cybercrime matters	Evidential and technical analysis to cybercrime cases or matters.
National Contingency Plan and Strategy for Critical Infrastructure	• Develop, design, and review national contingency plan for national critical infrastructure • Coordinate implementation of the national contingency plan	National Critical Infrastructure Contingency Plan developed and implemented
Child Online Protection	• Lead discussions on Child Online Protection Working Group (COPWG) and identify resolutions for national child online protection efforts • Implement outcomes from the COPWG	Child Online Protection plan implemented and COPWG convene at least twice annually
National Cybersecurity Initiatives	• Lead discussions on the Kiribati Cybersecurity Working Group (KCWG) on national cybersecurity plans, initiatives, and priorities. • Implement outcomes from the KCWG	National Cybersecurity ambitions identified and implemented. KCWG convene at least twice annually
Critical National Infrastructure Protection	• Develop, review and improve Critical National Infrastructure (CNI) Protection plan. • Convene a stakeholder meeting with critical infrastructure providers to identify priorities on protection plans. • Implement and review technical readiness of CNI providers.	Critical national infrastructure plan developed and implemented.

10. Key Challenges	**11. Selection Criteria**
	11.1 PQR (Position Qualification Requirement):

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:**

• 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	**Education:** 1. Bachelor Degree in Computing Science AND Information System or Master Degree in Cybersecurity related field. **Experience**: 5 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) • 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

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:**

	• 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:**