PURA Public Utilities Regulatory Authority

Equity in development

Position:	**CERT (COMPUTER EMERGENCY RESPONSE TEAM) - MANAGER**
Reports to:	**Director ICT**
Salary:	The position is on Category **IIB.1** of the PURA pay scale.
Number of vacancies:	(1) one

BACKGROUND

The Public Utilities Regulatory Authority (PURA) is the Gambia's independent multi-sector regulator established under the PURA Act 2001 to regulate the following sectors:

- Broadcasting
- Electricity
- Telecommunications (Mobile, Landline, ISP)
- Petroleum (Downstream)
- Water and Sewage
- Transportation
- Post

PURA in accordance with its mandate is currently striving toward performing technical, economical and safety regulatory functions with respect to regulated public services. This is done in a bid to achieve its regulatory mandate and fair competition within regulated entities to promote economic development, social inclusion, and environmental sustainability to improve service delivery and protection for consumers and service providers.

Job Summary

The CERT Manager will spearhead incident response capabilities, coordinate, and align the key resources and team members during a cyber security incident to minimize impact and keeps the team focused on minimizing damage. He/she will be responsible to manage key stakeholders, tracks deliverables, and identifies lessons learned. The successful candidate will primarily assist in investigating and analyzing response activities related to security incidents or events. He/she will lead a team of analysts responsible for driving security incidents to a state of reduced risk. This team oversees the Incident Response Plan and addresses information security matters nationally using a wide variety of security tools.

Duties and Responsibilities

- Create and maintain an Incident Response Plan (IRP)
- Investigate and analyze incidents.
- Manage internal communications and updates during or immediately after incidents occur.
- Perform hosting, network, and forensics; malware triage; and cyber incident response
- Managing Cyber Security Services engagements and engagement teams
- Recognize common attacker tools, tactics, and procedures
- Work to defend constituency privacy and other confidential proprietary information.

- Develop and maintain plans of mitigating threats of cyber risks strategies on the ICT sector by routinely auditing cybersecurity strategies.
- Provides guidance to other stakeholders during the incident response process.
- Provide feedback on process improvements and how to eliminate false positive alerts and to improve workflow processes and procedures
- Ensure that there is an adequate and efficient number of resources dedicated to critical tasks.
- Supervises resources allocated to the incident and make sure the incident is receiving the appropriate assistance to drive resolution as swiftly as possible
- Ensure to quickly escalate, prioritize, communicate, and coordinate high severity incidents ensuring observance to the gmCSIRT' s incident response process
- Involvement in the creation and execution of strategies that will enhance and increase the reliability and security of IT projects.
- Manage staffing decision regarding incident response team
- Identify and manage potential and actual operational issues within the incident
- Manage the creation of vulnerability audits, penetration tests, forensic IT investigations and related outcomes improving overall IT Security.
- Depending on the organization's structure, you may have the responsibility of managing teams with diverse skill sets from support staff, analysts through to security auditors, architects, and consultants.
- Manage and ensure ICT network operations are compliance with necessary legislation, such as the Data Protection act and other government regulations as they come in to force.
- Analyze and correlate information security events to identify appropriate event handling actions.
- Review security policies, standards, and procedures by considering the threats identified and other information collected.
- Test incident response plans periodically to ensure response times and executed procedures are acceptable.
- Communicate with employees, shareholders, and other CERT constituencies

Qualification and Experience

- A bachelor's degree in an IT related field (Computer Science, IT, or a Cyber-Security).
- Master's degree in Computer Science, Information Technology, Management Information
- Systems, Management or closely related field is required.

  At least three (3) years of experience managing a team of IT security operations engineers or 5 years working experience in IT security
- At least two years in management experience gained in a similar position
- Project management skills
- An up -to- date working knowledge of IT Security related hardware, software, and vendor solutions

Relevant industry certifications or relevant technology vendor certifications

- Strong technical background in vulnerability and risk assessment, penetration testing, Incident management, Cyber Security forensics, etc
- Strong network background and experience in cybersecurity incident handling tools
- Practical experience using computer operating systems such as MS Windows, UNIX/Linux
- Strong analytical and problem-solving skills with the ability to quickly get to the root cause of issues
- Strong Organizational skills and the ability to perform a command-and-control role, efficient and able to work unsupervised under your own initiative
- Good in teamwork
- Ability to manage and constantly triage multiple security incidents, differentiating urgent issues from the merely important.
- Ability to consume and synthesize intelligence about actors, techniques, or situations to identify emerging risk scenarios.
- Strong technical understanding of the information security threat landscape (attack vectors and tools, best practices for securing systems and networks, etc.).
- Must have strong verbal and written communication skills; ability to communicate effectively and clearly to technical and non-technical staff and senior management.
- Broad information security knowledge, including some familiarity with key regulations and standards relating to security incident response such as ISO 27001.

COMPETENCIES

- Excellent Leadership skills
- Excellent knowledge of project and programmes management
- Ability to lead strategic management and change management
- Excellent management and networking skills.
- Good experience in building consensus in multi-stakeholder group setting.
- Project management required.
- Research skills required.
- Excellent report writing skills.
- Excellent interviewing skills.

SUBMISSIONS OF APPLICATIONS

All applicants must complete and sign the PURA Job Application Form which can be downloaded from the PURA website (www.pura.gm) or picked up at the PURA office reception desk. Applications must be accompanied with a Curriculum Vitae (CV) and photocopies of relevant certificates.

All applications must be submitted to the PURA office in sealed envelopes on or before **12:00hrs, on 5th August 2022** and be addressed to:

The Director General
Public Utilities Regulatory Authority (PURA)
Kairaba Avenue
P.O. Box 4230 Bakau
KMC

*****Female Candidates are encouraged to apply**

PURA

Public Utilities
Regulatory Authority

Equity in development