RE-ADERTISEMENT - EXECUTIVE: NAMIBIA CYBER SECURITY INCIDENT RESPONSE TEAM (NAM-CSIRT) [E2]

[5 YEARS CONTRACT]
(RE-ADVERTISED)

CLOSING DATE | THURSDAY, 23 JULY 2026 | 17H00
Reports to CRAN CEO and Head of NAM-CSIRT

Primary Purpose of this position:
The Executive: Namibia Cyber Security Incident Response Team (NAM-CSIRT) is responsible for the strategic contribution to the development of the Strategic Plan and related Annual Plans with special focus on computer incident response goals and objectives, to ensure alignment to NAM-CSIRT's Mandate. The executive will be tasked with the development and progress of Cyber Security initiatives at national level.

Key Performance Areas will include:

1. **NAM-CSIRT Strategic Planning and Implementation**

- Develops a Cyber Security strategy that will support NAM-CSIRT in attaining its overall strategic objectives;
- Participates in the strategic planning and execution process of NAM-CSIRT and CRAN as a full member of the executive team;
- Cascades the relevant strategic imperatives to develop the NAM-CSIRT Operational Plan and implement according to delegations of the Authority;
- Monitors and evaluates the departmental performance against strategic and operational plans;
- Provides a holistic view of the current business and the future direction of accountable function, and the initiatives required to migrate to the desired future environment;

- Leverages enterprise architecture building blocks and components, including externally provided services and related capabilities to enable nimble, reliable and efficient response to strategic objectives;
- Oversees NAM-CSIRT's functions including but not limited to the development, review and implementation of all relevant policies, procedures and protocols; and
- Establishes and maintains a cyber-safe environment within Namibia.

2. Leadership

- Provides strategic direction to employees;
- Coaches and mentors team members as required;
- Oversees the implementation of performance management in the division;
- Ensures that the division is capacitated to execute its functions;
- Ensures that a leadership pipeline is established to ensure business continuity in the division;
- Ensures that employee engagement is optimised in the interest of healthy employee relations, productivity and retention of skills; and
- Ensures that all human capital policies and procedures are implemented and adhered to in the division.

3. Resource Management

- Participates in the annual budgeting, monitoring and control processes (CAPEX and OPEX);
- Ensures procurement and expenditure is in terms of relevant policies and procedures;
- Analyses of monthly variance reports and implement cost saving initiatives relevant to the division;
- Maintains prudent financial management controls within the division; and
- Drafts and implements the Strategic and Operational Plan of the Division.

4. National Security & Cyber Response Incident Handling

- Develops, implements and enforces a regulatory framework as related to cyber incidence response guided by cyber security sector reform initiatives;

- Develops an action plan for the implementation of a National Computer Incident Response Team, when required;
- Develops a regulatory framework for operation of the NAM-CSIRT;
- Liaises on organisational, national, regional and international level on all ICT and cyber security relevant topics to ensure information sharing, regulatory and technical compliance;
- Advises on relevant national policy and reforms thereto;
- Serves on the SADC Regional Task Team for implementation of the regional cyber security incident response team and other relevant bodies;
- Ensures protection and information security policies are implemented effectively for Namibia; and
- Liaises with law enforcement and other relevant bodies on cyber-crime investigations and incident and vulnerability handling.

5. Reporting & Contract Management

- Prepares required reports and statistical required reports for the relevant governance forums;
- Manages contracts when external service providers are involved;
- Ensures that all standards, criteria and milestones are achieved; and
- Liaises on a continuous basis with external experts regarding issues pertaining to cyber security, technology and standards to provide and obtain relevant information.

6. Liaison with Stakeholders

- Liaises with stakeholders on national and international regulatory issues;
- Maintains cordial relationships with identified stakeholders; and
- Keeps informed on relevant legislations and ensures legislative compliance adhered to and deployed within division and the organisation.

Education, Experience and Skill Requirements:

- Bachelor's degree in one or more of the following disciplines: Computer Science, Electronic Engineering or Cyber Security;
- Senior Management Programme;
- Relevant Master's degree will be an added advantage;
- Certification in Cyber Security or Data Security;
- Three (3) years experience in Senior Management role with eight (8) years experience within the Cyber Security Industry; and
- Valid driver's licence.

To receive consideration:

Applicants meeting the criteria should register their applications including motivation letter, CV, and relevant qualifications at Direct Hire by clicking on the following link:

https://cran.mcidirecthire.com/External/CurrentOpportunities

Remuneration Package:

CRAN offers a competitive market-related cost to company remuneration package commensurate with relevant experience and qualifications.

Only short-listed candidates will be contacted. CRAN reserves the right to withdraw this advert should circumstances change.

ALL FOREIGN QUALIFICATIONS MUST BE RECOGNISED AND ACCREDITED BY NQA.
CRAN IS AN EQUAL OPPORTUNITY EMPLOYER. WOMEN & PERSONS WITH DISABILITIES ARE ENCOURAGED TO APPLY.