CRAN
Communications Regulatory Authority of Namibia

VACANCY

TEMPORARY SUPERVISOR: CYBER SECURITY [D2]

CLOSING DATE | TUESDAY, 06 MAY 2025 BEFORE 17H00

Primary purpose of the position:

Reporting to the Executive: CIRT, the Supervisor: Cyber Security Incident Handling is responsible to supervise the coordination and administration of the cyber incidence through analysis, tracking, recording and reporting of incidence and to implement actions that are agreed to promote a safer national cyberspace.

Key Performance Areas will include:

National Security and Cyber Incidence Response Coordination

- Oversees the day-to-day operations of the division;
- Collects all information relating to the security and stability of critical infrastructure, critical information infrastructure and computer information systems and disseminate such information for the promotion of computer security;
- Coordinates with international bodies to promote the security and stability of critical infrastructure, critical information infrastructure and computer information systems;
- Undertakes all necessary steps to diminish the risk of incidence involving the use of critical infrastructure, critical information infrastructure and computer information systems;
- Ensures the detection and prevention of the use of critical infrastructure, critical information infrastructure and computer information systems in hiding the proceeds of crime; and
- Implements response strategies and initiatives to diminish the risk of incidence involving the use of critical infrastructure, critical information infrastructure and computer information systems.

Computer Emergency Response Coordination

- Administers the establishment of adequate systems and frameworks to ensure an expert handling of computer security incidents;
- Develops and establishes capacity to quickly and effectively coordinate communication among experts during security emergencies in order to prevent future incidents;
- Ensures the implementation of the national cyber incident response plan;
- Ensures the accurate identification and classification of cyber-attack scenarios;
- Ensures the determination and availability of the tools and technology used to detect and prevent cyber attacks; and
- Determines the scope for investigations and once an attack occurs, ensure that investigations are conducted within the scope.

Cyber Security System Implementation

- Implements the cyber security management framework to mitigate cyber threats and foster a safer national cyberspace;
- Assists with conducting research to support the establishment of a secure and resilient cyber and communications infrastructure;
- Develops and fosters professional engagement with partners and experts through information sharing to manage threats, vulnerabilities, and incidents;
- Conducts threat and risk analysis and analyse the national impact of new and existing systems and technologies to eliminate risk, performance, and capacity issues;

- Implements vulnerability assessments and audits of operating systems and databases and detect patterns and malicious activities in the infrastructure;
- Conducts diagnostics on any changes to data to verify any undetected breaches; and
- Recommends systems and procedures for specialised security features and for software systems, networks, and hardware.

Cyber Crime Investigation

- Provides assistance to law enforcement officers authorised by law to perform any search or seizure of a computer system;
- Provides assistance to law enforcement officers who during a search that require a key or password to access a storage medium to determine any matter that is relevant for the investigation of an offence;
- Cooperates with lawful investigations and provide the requisite information, computer data, printout or other intelligible output of that data as ordered by a judge or magistrate; and
- Cooperates with lawful and authorised law enforcement orders to preserve information and to avoid loss, modification or destroying of such information to aid the criminal investigation.

Incident Handling

- Undertakes incident analysis, tracking, recording and response;
- Coordinates the reactive and proactive guidance that will be provided to the constituency;
- Interacts with the CSIRT team, external experts and other members as appropriate;
- Implements the national cybersecurity policies, laws and regulations;
- Identifies and reports early warning signs and potential cybersecurity threats; and
- Conducts research projects to better understand the nature and impact of cybersecurity threats as directed.

Education, Experience and Skill Requirements

- An Honours Degree in Cyber Security or related equivalent qualification;
- Three (3) to Five (5) years' experience within the ICT industry;
- Supervisory skills training and experience;
- A Project Management certificate would be an added advantage;
- Relevant professional cyber security or information security certifications;
- Good practical skills in the application of relevant Cybersecurity and Data Protection laws;
- Knowledge of application of ISO 27001 and related series;
- Ability to operate under high levels of pressure;
- Strong written and verbal communication skills; and
- Excellent analytical and strategic thinking skills;

Additional Information

- Valid code B Driver's Licence;
- Shortlisted candidates will be required to submit proof of Namibian Police clearance.

Applicants meeting the above 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 to relevant experience and qualifications.

CRAN IS AN EQUAL OPPORTUNITY EMPLOYER. WOMEN & PERSONS WITH DISABILITIES ARE ENCOURAGED TO APPLY.