بسم الله الرحمن الرحيم

National Centre for Information Technology
64, Kalaafaanu Hin'gun, Male', Republic of Maldives

Date: 26 September 2024

Announcement Reference no: (IUL)164-HR/1/2024/74

Project	Digital Development Project
Initiative	Government Cyber Security Initiative
Position	Security Operations Center Engineer
Vacancy	1
Type of Contract	Individual
Duration	24 Months

Terms of Reference

A. BACKGROUND

The Ministry of Homeland Security and Technology (Mohst) through the National Centre for Information Technology (NCIT) is implementing the Strategic Action Plan of NCIT and Digital Development Action Plan from the National Resilience and Recovery (NRR) Plan of the Government. The Project will be managed by the Project Management Unit (PMU) setup within NCIT and reporting to and working under the guidance of the NCIT Senior Management.

The aim of the Project is to deliver on the digital development pledges of the Government, establishing the foundational components to drive the development of digital government, digital economy and digital society. The Project will prioritize the establishment of a government technology stack and open data platform, enhancing government productivity, enabling work from home and hybrid workplaces, enhancing the regulatory framework for digital development, and digital transformation of health and national care systems.

B. OBJECTIVES OF ASSIGNMENT

The Government Cyber Security Initiative aims to develop a Cyber Security framework policy and capabilities to enable the government to safeguard digital services and protect critical government infrastructure by adopting security standards and preparation of required cyber security regulations.

The NCIT intends to hire a Security Operations Center (SOC) Engineers with experience in Network Security for the Cyber Security Operations Center at NCIT. SOC Engineers will work within the PMU, which has been established for the implementation of the Government Cyber Security initiatives. SOC Engineers will work as part of a team to assist in the Cyber Security objectives to support the delivery of the Government Cyber Security Framework and Policy.

C. OVERALL RESPONSIBILITY

The overall responsibilities of the SOC Engineer include, but is not limited to the following:

1. Operations of the Cyber Security Operations Center
2. Support the development and implementation of SOPs for the Computer Incident Handling and Response Team.
3. Develop, test, deploy, bugfix and support Government Software Quality Assurance Stack
4. Vulnerability assessment and compliance auditing including running scans and performing manual audits of critical government systems.
5. Support the development of the SOPs required for the Cyber Security Operations Center.
6. Ensure Compliance of the systems monitored in the Cyber Security Operations Center.
7. Triage, Alert and Assign incidents and work with relevant teams for remediation.
8. Microsoft Office365 Government Tenant Security and Compliance.
9. Implementing Cyber Security Standards and checking compliance.
10. Supporting the preparation of Government Cyber Security Standards and Policies.
11. Develop and implement the National Cyber Security Strategy key initiatives.
12. Writing detection rules and enhancing the telemetry of Government Cyber Security Stack.
13. Enhance the detection rules of the Government Security Operations Stack.

D. SCOPE OF SERVICES

The position is within the PMU of NCIT and will be under the Lead SOC Engineer leading the development of the Government Cyber Security Initiative. In addition, his/her duties will include, but will not be limited to:

1. Carryout tasks for achieving the National Cyber Security Framework key initiatives and Security initiatives implementation plan.
2. Maintain the cyber security of the Government Software Quality Assurance Stack and the Government Cyber Security Stack.

3. Support the Lead SOC Engineer in building security architectures and systems.
4. Assist in the designing, implementation and monitoring of the Security Operations Center.
5. Write, revise and maintain Standard Operating Procedures, Cyber Security Framework Documentation, operations documentation, and user guides following standards practiced by NCIT.
6. Ensure that all development activities are carried out in accordance with the set standards in the organization and fully adhere to change and configuration management best practices set forth by the PMU and ensure that systems are up to date.
7. Propose, prepare and install solutions by determining and designing system specifications, standards and programming.
8. Work collaboratively with other departments and divisions to achieve organizational goals and accomplish the organization's mission by completing related results as needed.
9. Collaborate and work with the Government Technology Stack and other product teams of the PMU to ensure security by design principles are applied throughout the development process at the NCIT and brainstorm and create new products.
10. Any other duties that may be assigned from time to time.

E. QUALIFICATIONS AND SKILLS REQUIRED

1. Bachelor's degree or above certificate in computer science or a related field.

   OR

2. Bachelor's degree or above certificate in computer science or a related field with less than 4 years of relevant work experience.

   OR

3. Bachelor's degree or above certificate in computer science or a related field with 5 or more years of relevant work experience.

F. ADDED ADVANTAGE - ADDITIONAL SKILLS/EXPERTISE

1. Establish and maintain different Network Security platforms
2. Experience in Cyber Security Incident Handling and Response
3. Knowledge in Operating Systems, Virtualization, Computing, Enterprise storage systems, open source, Networking technologies and cloud technologies.
4. Understanding of Active Directory and Group Policies, Knowledge of Windows, and UNIX platforms, understanding of network security concepts
5. Knowledge of different databases (MySQL, Postgres, MSSQL, MongoDB, MariaDB, Oracle) and database types (centralized, distributed, real-time, relational etc.).

6. Experience with cloud services such as AWS, Digital Ocean, Google Compute Engine, Oracle, Microsoft Azure or similar products.
7. Experience in administering monitoring stacks (SIEM) or network monitoring tools.

G. SCHEDULE FOR THE ASSIGNMENT

Duration of the assignment is 24 months with the potential extension based on need and performance.

This position is based at the PMU at the National Centre for Information Technology.

H. REMUNERATION AND OTHER BENEFITS

1. The Security Operations Center Engineer will receive a monthly salary ranging from MVR 22,000 to MVR 36,000, depending on their education and experience.
2. Training and travel expenses under the PMU as budgeted under the Project and approved by the NCIT, Ministry of Homeland, Security and Technology and Ministry of Finance.
3. Participate in the "Maldives Retirement Pension Scheme"
4. Ramadan Allowance
5. Leave in accordance with the Maldives Employment act.

I. REPORTING OBLIGATIONS

The SOC Engineer:

1. The role is based within the Project Management Unit under the Government Cyber Security Initiative and will be required to provide support to internal and external customers.
1. Shall report directly to the Lead SOC Engineer on all aspects of the assigned digital service products throughout the duration of the contract.
2. Is expected to report to work on weekdays from 0800 – 1400 hours other than public holidays and provide services for an average of 44 hours a week.
3. Shall provide all the necessary reports and updates to the Project Management Unit as needed.
4. Is required to report to work in official attire.

J. SERVICES AND FACILITIES

1. Office space and other facilities such as computers will be provided as required.

K. SELECTION CRITERIA

The SOC Engineer will be selected based on the following criteria's

Criteria	**Points**
Educational Qualification (Section E)	10
Work Experience (Section E)	30
Additional Skills/ Expertise (Section F)	10
Interview	30
Practical	20

L. APPLICATION

1. Curriculum Vitae (clearly stating the starting and ending month and year for previous experiences)
2. Copy of National ID Card
3. Accredited copies of Academic Certificates (Only documents accredited by Maldives Qualification Authority will be accepted)
4. Certificates/ Letter of completion from the university together with a written document from Maldives Qualification Authority stating that the course completed is accredited to a certain level.
5. Employment Verification Letters from previous employer(s), detailing the work carried out, details of technologies and equipment involved in the work and duration of the responsibilities, start and end date of the employment period.
6. Candidates must submit additional documents to prove expertise/experience in areas highlighted under section E and section F.

M. SUBMISSION

Interested candidates may email their proposals on or before 1330 hours of 10 October 2024 to the following address. Note that the time that the email is received will be considered as an on-time submission.

Human Resource Section

jobs@ncit.gov.mv

National Centre for Information Technology

No 64, Kalaafaanu Hingun

Male', 20064, Republic of Maldives