بسم الله الرحمن الرحيم

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

Date: 23rd May 2022

Announcement Reference no: (IUL)164-HR/1/2022/54

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

Terms of Reference

A. BACKGROUND

The Ministry of Environment, Climate Change and Technology (Ministry) through the National Centre for Information Technology (NCIT) is implementing the 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 Ministry.

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 Ministry intends to hire a Lead Security Operations Center (SOC) Engineer with experience in Network Security and manage the operations of the Cyber Security Operations Center. The Lead SOC Engineer will work for the PMU, which has been established for the implementation of the Government Cyber Security initiatives. The Lead SOC Engineer 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. The Lead SOC Engineer will support the Cyber Security Consultant in the design, implementation, and overall management of the Government Cyber Security initiatives.

C. OVERALL RESPONSIBILITY

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

1. Oversee and Manage the Cyber Security Operations Center
2. Develop 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. Develop 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. Preparation of Government Cyber Security Standards and Policies
11. Follow guidance of Cyber Security Consultant for the implementation plan of National Cyber Security Strategy key initiatives and assist in the implementation plan
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 supervision of the Cyber Security Consultant leading the development of the Government Cyber Security Initiative. In addition, his/her duties will include, but will not be limited to:

1. With the guidance from Cyber Security Consultant, prepare tasks for achieving the National Cyber Security Framework key initiatives and Security initiatives implementation plan.
2. Determine operational feasibility by evaluating analysis, problem definition, requirements, solution development and proposed solutions.
3. With the guidance from Cyber Security Consultant, assist in the designing, implementation and monitoring of the Security Operations Center.
4. Write, revise and maintain Standard Operating Procedures, Cyber Security Framework Documentation, operations documentation, and user guides following standards practiced by NCIT.
5. Ensure and enforce 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.
6. Prepare and install solutions by determining and designing system specifications, standards and programming.
7. Work collaboratively with other departments and divisions to achieve organizational goals and accomplish the organization's mission by completing related results as needed.
8. 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.
9. Any other duties that may be assigned from time to time.

E. QUALIFICATIONS AND SKILLS REQUIRED

1. Master's or equivalent Degree in Network Security, Computer Science or related field, with professional work experience of 7 years or more;
2. Demonstrates good oral and written communication skills in substantive and technical areas. A thorough knowledge or demonstrated ability to rapidly acquire knowledge about technical assessments, research processes, procedures for performance monitoring and evaluation;

3. Should have strong leadership, management, and proactive interpersonal communication skills in presenting, discussing, and resolving difficult issues, and have the ability to work efficiently with a technical team.
4. Understanding of Active Directory and Group Policies, Knowledge of Windows, and UNIX platforms, Operating System Hardening and Solid understanding of network security concepts
5. Must also have knowledge of firewalls and router access control lists, intrusion detection and prevention systems and managing advanced application layer firewalls and mitigations

F. ADDED ADVANTAGE - ADDITIONAL SKILLS/EXPERTISE

1. Knowledge in BGP routing and configurations
2. Establish and maintain different Network Security platforms
3. Cyber Security Incident Handling and Response
4. Extensive knowledge in Operating Systems, Virtualization, Computing, Enterprise storage
5. systems, open source, Networking technologies and cloud technologies
6. Knowledge of different databases (MySQL, Postgres, MSSQL, MongoDB, MariaDB, Oracle) and database types (centralized, distributed, real-time, relational etc.).
7. Experience in administering production level databases with proficient understanding of SQL.
8. Project Management Skills – Good planning, scheduling, and analytic skills.
9. Experience with cloud services such as AWS, Digital Ocean, Google Compute Engine, Oracle, Microsoft Azure or similar products.
10. Experience in administering monitoring stacks (SIEM) or network monitoring tools.
11. 5+ years of leadership experience in managing information /cyber security and managing a security team.

G. SCHEDULE FOR THE ASSIGNMENT

Duration of the assignment is 24 months with the potential extension based on need and performance. The successful candidate is expected to commence the services in June 2022.

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

H. REMUNERATION AND OTHER BENEFITS

1. MVR 43,700 per calendar month, based on education and experience, as remuneration for the services provided.
2. Training and travel expenses under the PMU as budgeted under the Project and approved by the Ministry.
3. Participate in the "Maldives Retirement Pension Scheme"
4. Ramadan Allowance
5. Leave in accordance with the rules and regulations of Maldives.

I. REPORTING OBLIGATIONS

The Lead 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.
2. Shall report within the Project Management Unit Structure on all aspects of the Government Cyber Security initiatives, working under guidance and instruction of the Cybersecurity Consultant, throughout the duration of the contract.
3. 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.
4. Shall provide all the necessary reports and updates to the Project Management Unit as needed.
5. 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 Lead 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)	20
Interview	40

L. APPLICATION

1. Curriculum Vitae (clearly stating the starting and ending month and year for previous experiences)
2. Copy of National ID Card
3. Copies of Academic Certificates
4. Certificates/ Letter of completion from the university
5. Employment Verification Letter from previous employer(s), detailing the works carried out, details of technologies and equipment involved in the work and duration of the responsibilities.
6. Candidates must submit additional documents to prove expertise/experience in areas highlighted in section

M. SUBMISSION

Interested candidates may email their proposals on or before 1330hrs of 30 May 2022 (Monday) 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