بسم الله الرحمن الرحيم

National Centre for Information Technology

64, Kalaafaanu Hin'gun, Male', Republic of Maldives

Date: 09 September 2024
Announcement Reference no: (IUL)164-HR/1/2024/70

Project	Digital Development Project
Initiative	Government Cyber Security Initiative
Position	Lead Security Operations Center Engineer
Vacancy	1
Type of Contract	Individual
Duration	24 Months (with the potential extension based on need and performance)

Terms of Reference

A. BACKGROUND

The Ministry of Homeland Security and Technology (Ministry) through the National Centre for Information Technology (NCIT) is implementing the Digital Development Action Plan and Cyber Security Initiative 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, enable 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 main objective of the Lead SOC Engineer (Head of Cyber Security) is to protect the organization's IT infrastructure, National Computer Network, sensitive data, and intellectual property including government hosted systems, applications and services from cyber threats, security vulnerabilities and attacks. This includes acquiring, implementing, and maintaining robust cybersecurity strategies, tools and systems. The Government Cyber Security Initiative aims to develop a cyber-security framework policy

that enables 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 Security Engineer with experience in Cyber Security, Security Operations and manage the operations of the Cyber Security Operations Center. The Security Engineer will work for the PMU, which has been established for the implementation of the Government Cyber Security initiatives. The Security 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 Senior Security 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, bug fix 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 Lead SOC Engineer will:

1. Prepare tasks for achieving the National Cyber Security Framework key initiatives and Security initiatives implementation plan. Design, implement, and monitor security measures for the protection of computer systems, networks, and information.
2. Determine operational feasibility by evaluating analysis, problem definition, requirements, solution development and proposed solutions.
3. Develop technical solutions and new security tools to help mitigate security vulnerabilities and automate repeatable tasks.
4. Regular security assessments reports.
5. Designing, implementation and monitoring of the Government Security Operations Center and configure and troubleshoot security infrastructure devices.
6. Write, revise and maintain comprehensive standard operating procedures, Cyber Security Framework Documentation, operations documentation, and user guides following standards practiced by NCIT.
7. Perform vulnerability assessments and penetration testing of software built in-house or by other government agencies and conduct threat and risk analysis and provide essential suggestions.
8. Respond to security breaches and lead incident response activities.
9. Incident response reports and post-incident analysis.
10. Ensure that the organization is compliant with all relevant regulations and standards.
11. Stay updated on the latest cybersecurity technologies and methodologies and conduct Security awareness training programs internally and externally.
12. Collaborate closely with the Software Development, Network and IT Infrastructure teams to ensure integrated security measures across all systems and applications.
13. Liaise with external security vendors and service providers.
14. Train and provide security awareness across the departments.
15. Any other duties that may be assigned from time to time.

E. QUALIFICATIONS AND EXPERIENCE

The following list identifies ideal qualifications, but not limited to:

1. Master's or equivalent Degree/ Professional Certificate in Network Security, Computer Science or related field, with professional work experience of 7 years or more;
2. A minimum of 5 years of experience in a cybersecurity role, with preferably 2 years in a senior position.

3. Extensive knowledge of security protocols, cryptography, authentication, authorization, and security.
4. Relevant certifications such as CISSP, CISM, CEH, CCNP Security, or vendor-specific certifications like Palo Alto Networks, Check Point, or Fortinet.
5. Hands-on experience with firewalls, VPNs, IDS/IPS, SIEM, router access control lists, intrusion detection and prevention systems and managing advanced application layer firewalls and mitigations and related security tools.
6. Knowledge of industry standards and regulatory requirements such as GDPR, HIPAA, PCI-DSS, and ISO/IEC 27001.
7. Relevant certifications such as CISSP, CISM, CEH, CCNP Security, or vendor-specific certifications.
8. Proficiency in security incident response and forensic investigation.
9. Excellent writing, editing and analytical skills and fluent in written and spoken English and Dhivehi.
7. Capability to work independently.
8. Must give attention to details even under pressure
9. Time management skills with the ability to meet deadlines

F. ADDITIONAL SKILLS/EXPERTISE

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

16. Ability to work independently and as part of a team.
17. Attention to detail and a high level of accuracy.
18. Strong project management skills.
19. Ability to handle high-stress situations and make decisions under pressure.
20. Continuous learning attitude to keep up with the evolving cybersecurity landscape.

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. MVR 43,700.00 per calendar month, based on education and experience, as remuneration for the services provided by the
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 Employment Act.

I. REPORTING OBLIGATIONS

The Lead SOC Engineer:

1. The role is based within the Project Management Unit under the Government Digital Services Initiative and will be required to provides support to internal and external customers
2. Shall report directly to the Project Director or designate on all aspects of Project Management 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 report and updates to the Project Director whenever 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

1. 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)	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 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 under section E and section F.

M. SUBMISSION

Interested candidates may email their proposals on or before 1330 hours of 19 September 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