بسم الله الرحمن الرحيم

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

# Terms of Reference

## Retainer based Cybersecurity Consultancy to NCIT

### 1. Introduction

National Centre for Information Technology (NCIT) was established on the 25th of March 2003 by the Government of Maldives as the main government agency for the development, promotion and propagation of Information Technology (IT) in the Maldives. Hence, to ensure the security of its systems and infrastructure, NCIT requires the services of a **Cybersecurity expert** to act as an independent Retainer based Cybersecurity Expert (Maldivian/Individual).

### 2. The Scope of work

2.1. Assisting in developing national strategies and legislations of cybersecurity; Ensuring the dissemination of best practices in the fight against existing and emerging cybercrimes.

2.2. Promoting accuracy and integrity of ICT data at the national, regional and continental levels and identifying gaps in evidence and suggesting priority research areas in the field of cybersecurity

2.3. Design a model for cybersecurity capacity building that takes into consideration all aspects (policy, technology, skills development)

2.4. Identifying areas of research needed for the formulation of policies, guidelines, etc., which can be general or sector-specific, for instance, cybersecurity for financial systems and for equipment monitoring tools.

2.5. Proactive Cyber Threat Hunting on e-Government Infrastructure. The client must conduct regular tests for compliance with security policies and procedures to ensure security measures are protecting the organisation.

2.6. Analyse and assess vulnerabilities in the infrastructure (software, hardware, networks), investigate available tools and countermeasures to remedy the detected vulnerabilities,

and recommend solutions and best practices to protect against internal and external attacks.

2.7. May assist in the creation, implementation, and management of Security Solutions.

2.8. The retainer must prepare reports for the client, detailing the weak security areas and make recommendations to correct the problems.

2.9. Assist with the validation of the security posture of new changes to the Infrastructure of National Computer Network and e-Government Hosting Infrastructure and advice required changes.

2.10. Attend to incidents handling and response requested by Government and state organisations. Analyse and assess damage to the data/ Infrastructure as a result of security incidents, examine available recovery tools and processes, and recommends a solution.

2.11. During the incident handling and response, the advisor should submit forensic evidence to identify patient zero. Initiate the remediation process and propose recommendations to mitigate future threats. Discover indicators of compromise (IOCs) or create new IOCs from incident handling and response processes for cyber threat intelligence, which can be used for mitigations across the government in future as a reference on attacker patterns.

2.12. Alert the organisation on new cyber threats to be published to the media.

2.13. Assist during the implementation process of the National Security Operations Center and the National Computer Emergency Response Team (CERT).

**3. Deliverables**

3.1. Just-in-time technical assistance, delivered, as required

3.2. Overall Cyber Security Strategy and Work Plan

3.3. Support drafting of guidelines, regulations, and bylaws to assist the government in cyber security programs

3.4. Human capacity development

3.5. Proactive Cyber Threat Hunting on e-Government Infrastructure and provide all IOCs.

**4. Experience/ Skills**

4.1. Proven experience in cyber security tasks at high-level Government institutions and various other stakeholders with minimum of experience of 7 to 10 years in ICT security,

Cyber Security Incident Handling and Response and digital forensics, in the public and private sector.

4.2. Demonstrated capabilities in consulting specialists, in fields such as technology, privacy, security, interconnection etc;

4.3. Hands on experience in virtualisation, DBMS, SAN, firewall and handling complex enterprise environments.

4.4. Have in-depth knowledge of attack and defence mechanisms.

4.5. Should have a thorough knowledge in Windows and *nix Operating Systems

4.6. Experienced in OS hardening.

4.7. Networking and Virtualisation environments security.

4.8. SIEM designs for proactive threat hunting.

4.9. Forensics and Anti-Forensics (Rootkits).

4.10. Application Layer Vulnerability Assessment and Penetration Testing.

4.11. WLAN Penetration Testing for 802.11 & 802.1x.

4.12. Memory Forensics.

4.13. Understanding of Database Administration or MS DBMS FCI and Availability Groups

4.14. Knowledge in Enterprise SANs.

4.15. Custom Scripting for Digital Forensics and Incident Response.

4.16. Active Directory Security Implementations.

**5. Contract Duration**

5.1. The contract duration will be 24 Calendar Months with possibility of renewal based on performance.

**6. Monthly Remuneration Package**

6.1. Maldivian Rufiyaa (MVR) 45,000/- paid as a flat monthly fee upon submitting an invoice.

**7. Application Documents**

Interested candidates should submit:

a) Application Form
b) Copy of National Identity Card
c) The CV (Should contain a list of references with contact numbers)
d) Copies of relevant certificates

e) Reference letters proving the candidates are well versed in the cybersecurity field.

**8. Bid Validity and Bid Opening**

8.1. Bids shall be valid for a period of 90 calendar days from the date of bid.

**9. Bid Submission**

9.1. Bids shall be submitted to the office reception at the address given below, before 10:01 AM Maldivian Time on 31st August 2021. Late bids will be rejected.

9.2. The bids will be opened at 10:05AM on 31st August 2020 in the presence of the bidders or their representatives, who wish to attend the bid opening.

**10. Marking Criteria**

| | |
|---|---|
| Experience and adequacy for the assignment | |
| Over 7 Years experience in leading a cyber security team in a government organisation | 50 Marks |
| 2 years or more experience in advanced digital forensics in incident handling and response | 20 Marks |
| 2 or more years of experience in managing Datacentre infrastructure | 10 Marks |
| Academic Background | |
| Specialised Certifications in cybersecurity and IT related fields | 10 Marks |
| Participation in internationally recognised specialised training for cybersecurity | 5 MArks |
| Academic Diploma / Degree in Business, IT, computer science or related field | 5 Marks |