Draft Terms of Reference (ToR) for a consultancy to develop the SIOFA Information System Security Policy (ISSP)

Consultancy for the Development of the SIOFA Information System Security Policy (ISSP)

1. Background

The Southern Indian Ocean Fisheries Agreement (SIOFA) is an international organization established to ensure the long-term conservation and sustainable use of fishery resources in the Southern Indian Ocean.

The SIOFA Secretariat is a small structure based in Reunion Island, and its staff consists of 5 people, one Executive Secretary 3 Officers and 1 Expert in Technologie Information and Communication.

The Secretariat is in contact with many people from the SIOFA contracting parties, cooperating non-contracting parties and participating fishing entities (CCPs) and rely a lot on email for information exchanges. SIOFA usually hold 3 meetings each year which take place outside of the Secretariat, usually hosted in one CCP country. The SIOFA website is the main tool for providing information and managing meeting documents.

For achieving its objective SIOFA and the Secretariat relies on information systems to store, manage, and exchange sensitive operational, scientific, and administrative data. With growing reliance on digital platforms, cyber threats and lacks policies may increase risks to the confidentiality, integrity, and availability of sensitive data.

To address this, SIOFA requires a comprehensive Information System Security Policy (ISSP) to provide a structured framework for information security management across all its information systems and devices.

2. Objectives

The objective of this consultancy is to:

- Develop a comprehensive and context-specific Information System Security Policy (ISSP) for SIOFA.
- Ensure that the policy aligns with international best practices and is tailored to the operational environment and mandate of SIOFA. Attention must be paid to the small size of SIOFA and its Secretariat, where there is very limited possibility to increase its budget or staffing.

- Provide recommendations for implementation, including controls, roles and responsibilities, and monitoring mechanisms.

3. Scope of Work

The consultant will undertake the following tasks:

a. Situational Analysis

Review SIOFA's current information systems, infrastructure, workflows, and existing policies.

Assess security risks and vulnerabilities in existing systems and processes, with an emphasis on sensitive information and confidential data.

Identify key stakeholders and data custodians.

b. Policy Development

Develop a ISSP including (but not limited to) the following components:

Policy objectives and scope

Governance and roles/responsibilities

Information classification and handling

Access control policies

Network and system security

Data backup and recovery

Incident response and reporting, including cyber incident and hacking

Physical and environmental security

Training and awareness

Compliance and audit

c. Consultant Engagement

Conduct consultations with SIOFA Secretariat staff and CCP representatives to validate findings and gather input.

Present the draft policy for feedback.

d. Finalization and Handover

Incorporate feedback from the Meeting of the Parties and submit the final version of the ISSP.

Provide an executive summary and implementation roadmap.

Deliver a short training/implementation session and a presentation for key SIOFA staff.

4. Provision by the Secretariat

The Secretariat will provide the Consultant with the following materials:

- Reports of the Data and Security audits performed in 2021-2022 (ref project SEC 2021-06).
- Current policies and procedures in place
- Current Software and IT service subscriptions

5. Deliverables and timeline

- Inception Report – outlining methodology, timeline, and consultation plan (within 2 weeks of contract signing).
- Draft Information System Security Policy.
- Secretariat and CCPs consultation report.
- Final ISSP incorporating feedback.
- Implementation roadmap and training materials.

Tentative dates	Deliverable	Payment
15 April 2026	Contract signature	20 %
10 May 2026	Inception report	30 %
15 May 2026	Secretariat and CCPs consultation report	
15 May 2026	Draft ISSP (presented at MoP13)	20 %
30 July 2026	Final ISSP + implementation roadmap and training materials	50 %

6. Duration and Location

Duration: Up to 2.5 months from the signing of the contract.

Location: Remote, with potential virtual meetings with SIOFA Secretariat and other parties.

Starting Date: 20 April 2026

7. Qualifications and Experience

The consultant (individual or company) should possess the following qualifications:

- Advanced degree in Information Security, Computer Science, or related field.
- Minimum of 5 years' experience in developing IT security policies or cybersecurity frameworks
- Demonstrated knowledge of international standards (e.g., ISO/IEC 27001, NIST). Experience working with international or intergovernmental organizations is an advantage.
- Strong analytical, communication, and writing skills.

8. Reporting and Management

The consultant will report to the Executive Secretary of SIOFA.

The consultant will also liaise with the TIC expert, the Data Officer, the Science Officer and the Compliance Officer for technical aspects.

9. Confidentiality

The consultant shall not release non-public data, restricted or confidential information for conducting this study to any person or any organisation, other than SIOFA Secretariat. Such information will remain the property of the SIOFA Secretariat.

The consultant shall delete all the confidential or restricted information obtained as a part of the contract immediately after the conclusion of the contract.

10. Application Requirements

The applicant(s) should submit a proposal that contains the following items:

- A current CV that summarises the applicant(s) relevant educational background and professional experience.
- A brief proposal outlining the proposed methods and analyses, including a description of how the objectives of the ToR will be achieved.
- A competitive financial proposal.
- Any proposed exclusions to the intellectual property clause.
- Identification of any project risks and associated mitigation and management required to successfully complete the project.
- A statement that identifies any perceived, potential, or actual conflicts of interest of the applicant(s), including those described in paragraph 4 of the SIOFA recruitment procedure (see https://siofa.org/science/sc-guidelines);

The applications must be submitted to Thierry Clot, Executive Secretary, thierry.clot@siofa.org by 10 April 2026.