TERMS OF REFERENCE

Consultancy for Cyber Security Awareness Workshop

1.0 BACKGROUND

German Sparkassenstiftung Eastern Africa (DSIK) is an international NGO headquartered in Bonn, Germany, dedicated to combating poverty through sustainable financial inclusion. At the heart of its mission lies a commitment to partnering with local organizations to execute project activities collaboratively.

In Tanzania, DSIK is providing advisory services to the Savings and Credit Cooperative Union League of Tanzania (SCCULT). Project activities in Eastern Africa are not limited to Tanzania, but also include Burundi, Kenya, Rwanda, and Uganda. In Tanzania, DSIK is a registered International Non-Governmental Organization under The Non-Governmental Organization Act, 2002 made under Section 11 (1) and 17 (2) of Act No. 24 in 2002 with Registration No. I-NGO/R1/005.

Within this initiative, DSIK is set to collaborate closely with SCCULT, the umbrella organization for SACCOS in Tanzania mainland. Established in 1992 under the Cooperative Act 15, SCCULT is dedicated to empowering and advancing Savings and Credit Cooperative Organizations (SACCOS) through advocacy, financial assistance, and technical support. SCCULT (1992) Ltd is licensed under the Microfinance Act of 2018, holding license number MSP3-TCDC/2021/00374 issued in 2021.

2.0 OBJECTIVES

Cybersecurity threats are a global concern, with cyberattacks becoming increasingly sophisticated and widespread. While digitalization offers numerous opportunities in service provision, innovation, and efficiency, it also introduces heightened risks and new avenues for threat actors. In recent years, high-profile cyberattacks have targeted diverse sectors, severely impacting both public and private institutions. Financial institutions, including Savings and Credit Cooperative Organizations (SACCOS), are not immune to these threats. A World Bank report titled "*Cyber Threats to the Financial Sector in Africa*"[1] indicates that African financial institutions face significant threats from organized criminal groups and financially motivated nation-states conducting high-value thefts in heist-style operations.

Within this context, the importance of cybersecurity awareness cannot be overstated. This initiative therefore aims to enhance knowledge on cybersecurity risks and best practices specific to the SACCOS sector. Additionally, it seeks to raise awareness on the regulatory requirements related to cybersecurity, ensuring that SACCOS can effectively safeguard their operations and protect their members' assets.

[1] World Bank. (2022, March). *Cyber threats to the financial sector in Africa: An assessment of the current threat and an analysis of emerging trends on the future threat landscape*. Retrieved from https://documents1.worldbank.org/curated/en/099830405172214598/pdf/P164770006015307 60af01093740e385fe8.pdf

By fostering a culture of cybersecurity awareness and compliance, SACCOS can mitigate risks, enhance their resilience against cyber threats, and maintain the trust and confidence of their members.

3.0 SCOPE OF WORK

This assignment, which should be completed within five (5) working days, entails conducting an expert awareness workshop on Cybersecurity for selected SACCOS staff from Tanzania Mainland. The workshop is scheduled for the **20th and 21st of June 2024** in **Dodoma**. Preceding the workshop, the consultant shall prepare comprehensive materials, including presentation slides, handouts, and supplementary resources, to facilitate in-depth discussions and analysis during sessions. Additionally, the workshop will serve as a platform to assess and gauge the current status of cybersecurity within SACCOS in Tanzania.

Therefore, the workshop aims to address the following areas:

(i) Presentation of the current industry status and relevant case studies. Provide an overview of the cybersecurity landscape within the financial services sector. Drawing upon this, present relevant cybersecurity case studies that align with the specific challenges, industry context, and risk profile of SACCOS operations.

(ii) Gather input from participants on their cybersecurity experience. Identifying best practices, shortcomings, and strategies for implementing quick and effective countermeasures.

(iii) Raising awareness of cybersecurity regulatory requirements. Provide participants with an understanding of regulatory requirements applicable to financial institutions, with a specific focus on those relevant to SACCOS operations.

4.0 KEY DELIVERABLES

The expected deliverables in this assignment are:

(i) **A Workshop Report** – This will include a presentation of the workshop summary, findings, and recommendations. The report should be produced within three (3) days after completing the workshop.

(ii) **Cybersecurity Best Practices for SACCOS: Dos and Don'ts** – Based on cybersecurity best practices, regulatory requirements and guidelines, this document will outline the dos and don'ts specific to SACCOS. It shall be produced within three (3) days after completing the workshop, alongside the workshop report.

(iii) **Workshop materials and resources** – This will include resources and materials used and shared during the workshop, such as PowerPoint presentations and reports, among others. These shall be shared along with the workshop report.

5. QUALIFICATION AND EXPERIENCE OF THE CONSULTANT

The Consultant should have at least a master's degree in a discipline relevant to Cybersecurity, Information and communication technologies (ICT), Information Technology (IT), Digital Finance or other relevant discipline. Candidates with bachelor's degrees, possessing adequate experience in cybersecurity will also be considered.

The consultant should have relevant qualifications and working experience, particularly:

(i) At least a master's degree in Cybersecurity, Information and communication technologies (ICT), Information Technology (IT), Digital Finance or related field.
(ii) Specialized cybersecurity certifications such as Certified Information Security Manager (CISM), Certified Information Systems Auditor (CISA), Ethical Hacking, PenTest or related field.
(iii) At least 3 years of working experience in Cybersecurity and at least 10 years of experience in Information Technology and/or Digital Finance.
(iv) A comprehensive knowledge on cybersecurity regulations, policy updates, and circulars applicable to the financial sector in Tanzania.
(v) Experience in communicating effectively with a diverse team of partners.
(vi) Experience in developing and delivering cybersecurity awareness training programs for diverse audiences, including executives, employees, and stakeholders.
(vii) Proficient in producing concise reports.

An eligible consultant may either be an individual or a firm.

6. MODE OF APPLICATION/BIDDING REQUIREMENTS:

Interested consultants should submit their letter of interest along with a quotation of their consultancy fees. Bidders must be VAT registered (if they are a firm) and capable of providing Electronic Fiscal Device Receipts (EFDs). Additionally, applicants should include the following in their application: the Company Profile (for firms), CVs of the responsible team, postal address (PO Box), phone number, email address, physical address, and a list of both previous and current corporate customers.

The applications should be submitted to the following e-mail by **13th June 2024** at 17:00 (EAT): Office.Tanzania@dsik.org

Please be informed that candidates who will not hear responses by **18th June 2024** should consider themselves unsuccessful.

For any enquiry you may contact: Ms. Kalunde Kapaliswa via Tel: +255 766 0202 84 or E-Mail: Kalunde.Kapaliswa@dsik.org