

**MINISTRY OF INFORMATION AND COMMUNICATIONS**



**REPUBLIC OF SIERRA LEONE**

**SIERRA LEONE DIGITAL TRANSFORMATION PROJECT  
IDA- E1130-SL**

**Terms of Reference  
for**

**TECHNICAL ASSISTANCE TO DEVELOP CYBERSECURITY  
AWARENESS CAMPAIGN STRATEGY AND ACTION PLAN**

**APRIL 2024**

# Terms of Reference

## TECHNICAL ASSISTANCE TO DEVELOP CYBERSECURITY AWARENESS CAMPAIGN STRATEGY AND ACTION PLAN

### I. Introduction

The Government of Sierra Leone (GoSL) has committed to transforming its economy based on a more inclusive and human-centric digital growth and development approach. A high-level vision for the digital economy is articulated in the new National Digital Development Policy (NDDP), which was approved by the Cabinet in December 2021, setting the GoSL's vision to transform Sierra Leone into an inclusive digital economy and society and to leverage digital technology to support the GoSL to deliver on its national development plan effectively and efficiently. The Sierra Leone Digital Transformation Project (SLDTP) aims to expand access to broadband internet, increase digital skills and improve government capacity to deliver public services digitally. The Project will support the development of a strong enabling environment for the nation's digital transformation and digital development agenda as articulated in the National Digital Development Strategy.

### II. Project Description

The Sierra Leone Digital Transformation Project (SLDTP) is a five-year International Development Association (IDA)-funded Project supported by a US\$50 million grant. The Project's primary implementing agency is the Ministry of Information and Communications (MIC). The proposed Project Development Objective (PDO) is to expand access to broadband internet, enhance digital skills and improve government capacity to deliver public services digitally.

The SLDTP proposes four integrated and mutually reinforcing components, with a fifth component dedicated to contingent response to future emergencies (*Contingent Emergency Response Component, CERC*).

- Component 1 – Expanding Digital Access and Increasing Resilience of the Digital Environment.
- Component 2 – Digital Skills Development and Innovation
- Component 3 - Laying Key Foundations for Digital Government Services and Systems
- Component 4 – Project Management and Implementation Support; and
- Component 5 - Contingency Emergency Response Component (CERC).

The proposed activities integrated into Components 1, 2, and 3 are designed to support the Government in building resilient and inclusive policies by strengthening its legal and regulatory

frameworks, scaling up the citizen-centric digital public service delivery by reinforcing the government portal and relevant Ministries, Departments, and Agencies (MDAs) capacity. By enhancing the service delivery infrastructure and platforms, the Project will support ensuring the continuity of public services in times of crisis. The Project is being implemented by a Project Coordination Unit (PCU) in the MIC.

As Sierra Leone embarks on this digital transformation journey, the risks posed by cybersecurity and cybercrimes cannot be easily brushed aside. Thus, the Government's vision for cybersecurity is to have an enabling environment that is secure, credible, and trustworthy for using ICTs while empowering citizens with the freedom to use the Internet for the nation's socio-economic benefits safely. This responsibility lies directly within the scope of Component One in the SLDTP project, which aims to enhance digital access and bolster the resilience of the digital environment.

The Technical Leading Agency (TLA) for Cybersecurity for the Project is the National Cybersecurity Coordination Centre (NC3). NC3 is a sub-vented Agency established by the Cybersecurity and Crime Act 2021. This institution oversees all cybersecurity issues in Sierra Leone, including providing support to computer systems and networks in preventing and combating cybercrimes in Sierra Leone, formulating and implementing national cybersecurity policy and strategy, overseeing the management of computer forensic laboratories, providing support to the Judiciary and other law enforcement agencies in the discharge of their functions concerning cybercrime in Sierra Leone, promoting Sierra Leone's involvement in international cybersecurity cooperation and doing other acts or things that are necessary for the adequate performance of the functions of the relevant security and enforcement agencies under the Act.

### **III. Objectives**

#### **a. General Objectives**

This TOR is to recruit a consultancy firm to develop a national multi-facet cybersecurity public education and awareness campaign strategy and its action plan and provide strategic advice on effectively implementing the campaign and enhancing communication activities for the National Cybersecurity and Coordination Centre (NC3). The developed Strategy aims to create a cyber-aware and resilient society that can effectively mitigate the risks associated with cyber threats and contribute to the overall security of the country's digital ecosystem.

**b. Specific Objectives**

The specific objectives include but are not limited to the following:

- (i) Promote good cybersecurity culture and digital hygiene for different target groups.
- (ii) Increase public awareness about the risks and challenges posed by cyber threats, including educating individuals, government institutions and private organisations about the potential consequences of cyberattacks, data breaches, identity theft, and other cybersecurity incidents.
- (iii) Promote best practices by encouraging certain behaviours such as using strong passwords, regularly updating software and devices, practising safe online browsing, avoiding phishing attempts, and securely managing personal information.
- (iv) Empower children and youths to safeguard their online presence and safely navigate the Internet and parents for protecting children’s online safety.
- (v) Foster collaboration between various stakeholders, including government agencies, private sector organisations, educational institutions, and the general public, to collectively combat cybercrimes.
- (vi) Promote the protection of critical information infrastructure asset owners from cyber threats by emphasising the importance of implementing robust security measures, conducting risk assessments, and ensuring the resilience of critical systems.

**IV. Scope of Assignment**

The consulting firm will work with the National Cybersecurity Coordination Centre, NC3, to conduct a communications capacity survey and to design a Public Awareness Campaign strategy, including specific campaign content (posters/billboards, fliers, social media templates, website content, newspaper placements, audio, and video/animation-content).

This Awareness Campaign will focus on five themes outlined in Table 1 below.

<b>Theme</b>	<b>Key Objective</b>	<b>Target Audience</b>
“Know the Law that Protects You”	Shed light on the various types of cyber threats like phishing, ransomware, social engineering, cyberbullying, sextortion and identity theft and their potential consequences. Raise public	General Public

	understanding of the Cybersecurity and Crime Act of 2021 as a tool to address cybercrimes.	
“Good Cyber Hygiene for a Successful Digital Society”	Raise awareness about the impact of cybersecurity on society as a whole, addressing topics such as online privacy protection, protecting digital identities, online reputation management, and securing critical infrastructure. Educate citizens about their personal responsibility and individual actions in maintaining cybersecurity, including encouraging them to adopt best practices, such as strong passwords, secure online transactions, regular software updates and safe browsing habits.	General Public, including unlettered and physically challenged persons
“Safer Internet for Children, Families and Senior Citizens”	Promote safe online experiences for children and families addressing topics such as cyberbullying, online predators, age-appropriate content and parental controls. Also, tailor educational materials and resources to address older adults' cybersecurity challenges.	Children, Youths, Parents, Caregivers, Educators & School Administrators, and the Aged
“ Knowledge is Key: Empowering girls and women against online sexual harassment”	Increase awareness of the different types of online sexual harassment, including cyberstalking, unsolicited sexual messages, and online image-based abuse.  Educate girls and women about their legal rights and options for reporting online sexual harassment.  Provide girls and women with resources and support to help them cope with and recover from online sexual harassment.  Challenge social norms that contribute to online sexual harassment, such as slut-shaming and victim-blaming.  Promote positive online behaviors, such as bystander intervention and digital citizenship.	Women and Girls
“Building a Resilient Cyber	Create awareness of the importance of a robust cybersecurity infrastructure and proactive	Government Institutions,

Defence in the Workplace”	defence measures, including the need for organisations to invest in cybersecurity solutions, threat intelligence, and incident response capabilities. Also, educate employees on their role in maintaining a secure work environment, such as password management, email security, safe browsing and reporting potential security incidents.	Private Sector Institutions and SMEs
“Securing the Future: Cybersecurity for the Next Generation”	Educate and empower young people to be responsible digital citizens, promoting careers in cybersecurity and cybersecurity skills development.	Youths, Educators and School Administrators, Universities, Public and Private Sector stakeholders.

More specifically, the Consultant is expected to carry out the following tasks:

***a) Communications Capacity Survey Report and Associated Toolkit***

The Firm will produce a rapid communication capacity survey around the country and provide recommendations on how NC3 can engage the public coherently and effectively, including in times of crisis and the implementation of the Awareness Campaign Strategy. The Communications Capacity Survey Report will cover the following key topics:

- Summary SWOT (Strengths, Weaknesses, Opportunities, Threats) analysis with a particular focus on identifying appropriate communications measures and medium for NC3 to increase the cybersecurity awareness for the above targeted audience.
- Identify various communication channels, platforms, and tools for nationwide awareness campaigns based on locations and target groups and evaluate their pros and cons for the expected effectiveness.
- Recommend messaging, branding and visual elements that can be employed in reaching and engaging the various audiences, for example, community stakeholders, students, technocrats, youths, etc.
- Skillset, media, equipment and other resources to be used by NC3’s communications staff for effective communication

The survey will result in developing a Toolkit for improving NC3’s communications, particularly how to strengthen its ability to successfully implement the National Cybersecurity Awareness Campaign Strategy and similar communications efforts. These recommendations will include, but

not be limited to: NC3's communications staff and budget; guidelines and protocols for effective media engagement; website management (incl. search engine optimisation); social media management incl. (paid and unpaid) content promotion approach; and branding recommendations.

**e. Public Awareness Campaign Strategy and Action Plan**

The Firm will work with NC3 to develop a multi-faceted public awareness campaign strategy reflecting the five themes outlined in this TOR. The Strategy will cover:

- **Key Messages:** Define key messages for each of the five themes, ensuring that these are concise, coherent, reflective of the current cybersecurity landscape and effective in the local cultural and socio-economic context; key messages should be in both English and six common local languages; the messages should be embedded in a strategy with concrete objectives; Customised materials developed by ITU on child online protection can also be utilised;
- **Target Audience:** Confirm key target audiences for each of the five themes and associated key messages (these may overlap); the Firm is expected to organise at least one focus group for each theme in English and Krio, respectively, to test the relevance and effectiveness of proposed messages with a representative set of the population;
- **Outreach Strategy / Channels:** Analyse available (media) channels (local popularity, audience type, cost etc.) and recommend a strategy for dissemination of key messages to target audiences, taking into account cost-effectiveness.

Possible channels for the campaign may include social media (paid and unpaid), specific newspapers or radio/TV channels/shows, and public billboards; use of other (non-media) channels to raise awareness is also encouraged (e.g. discussions in schools; stalls at popular markets or events; NC3 staff/management joining public talks etc.). Communication channels may differ across themes/audiences, and a strategy coordinating the various media and themes is expected.

- **Partners & Champions:** Analysis of potential partners and champions to amplify NC3's outreach and support the planned campaign – this may include local community leaders; local celebrities; officials; or NGOs and private actors active in the sector, as well as an assessment of their proposed roles in the campaign;
- **Audio-Visual and other Content:** In line with the Strategy, confirm content to be produced by the Firm for the public awareness campaign for each theme (see below);
- **Timeline and Roll-out Plan:** Based on the identified objectives, key messages, target audiences, outreach strategy, partners/champions, identified distribution channels and proposed media content, develop a specific roll-out plan and timeline for the campaign;

- **Budget:** The consultancy will identify a detailed budget for the proposed campaign/media plan, including proposed sponsorships and media/advertisement purchases as necessary, confirming current local prices; any additional staff / temporary staff needs (e.g. to staff stalls or hand-out fliers) should be identified, relying as much as possible on existing NC3's staff; any events (e.g. launch event/workshop) should be part of this budget;
- **Framework for evaluation:** Based on the campaign objectives, the Strategy should define a plan to evaluate the impact and success of the campaign;

***f. Media Content***

The Public Awareness Campaign Strategy will confirm the specific media content to be produced by the Firm (see above). However, for purposes of this TOR and associated proposals by shortlisted firms, the following content is assumed to be produced in English and Krio except otherwise specified. All content created will be the property of the National Cybersecurity Coordination Centre.

- A common visual identity (this may be based on existing NC3's official logo) to be used in all content of the public awareness campaign and other communications tasks (e.g. standardised taglines, colour scheme and logo for all posters, video-content, social-media posts etc.);
- Video content for social media, public events and TV advertisements: 15 animated video clips of no longer than 60 seconds (also done in Limba, Temne, Mende, Fullah, Kono and Loko) ;
- Audio content:
  - 15 short local-language (translated into six local languages) audio clips with an average length of 30-60 seconds suitable for distribution through radio advertisements or social media;
  - Talking points on each of the five themes for use by NC3's management during public/media discussions;
- Ten print advertisements for national/local newspapers;
- Social media content: At least 40 prepared social media posts for distribution on Twitter/Facebook/WhatsApp/Instagram. These should be concise, privileging striking messages and visual content;
- Ten billboard designs reflective of the key themes and messages;
- Live Event: Content and discussion guidelines for a public event of no more than one hour to engage live audiences (e.g. for schools or general community discussions);



Technical proposals of shortlisted firms may propose other optional content, but for comparability, financial proposals should be based on the above.

## V. Reporting, Time Schedules, and Payment Schedules

The Firm is expected to complete the assignment in full within 9 months, The Firm will regularly report to the National Cybersecurity Coordinator, on all aspects of the agreed activities and also report to the SLDTP Project Coordinator.

The deliverables comprise the following:

No	Deliverable	Timeline	Indicative payment schedule
1	Contract Award	Commencement	10%
2	Inception Report / Work Plan,	Commencement + 2 Weeks	15%
3	Draft Capacity Survey Report & Draft Public Awareness Campaign Strategy	Commencement + 3 Months 2 Weeks	25%
4	Draft Public Awareness Campaign Strategy		
	Draft Content, Complete package of draft content (graphical, video, audio, texts etc) for review by SLDTP and NC3.	Commencement + 4 Months 2 Weeks	20%
	Final Reports & Content (Final Communications Capacity Review, Final Public Awareness Campaign Strategy, Final content for the public awareness campaign)	Commencement + 5 months	30%

## VI. Qualification and Experience of Team Members

The assignment calls for a team of at least 5 persons who will possess the following qualifications, skills and experience:

Key Position	Experience
--------------	------------

(1) Team Leader	Minimum of 15 years of work experience, preferably including in Sierra Leone/West Africa and with public service providers; the team leader will be responsible for coordinating the team, communications with the SLDTP and the client (NC3), and the overall direction, quality and timeliness of all outputs;
(1) Cybersecurity Specialist	Minimum of 10 years of work experience in cybersecurity and implementing best practices. This specialist will provide domain knowledge and expertise in cybersecurity. The specialist must understand the current threat landscape S/he will help refine messaging and ensure the final content is accurate and relevant to the campaign content.
(1) Communication and Marketing Specialist	This specialist is responsible for developing the campaign's messaging and communication strategy. They ensure the campaign materials are engaging, clear, and tailored to the target audience. They may also oversee the selection of appropriate communication channels and mediums. They will ensure that messages and graphic elements of the public awareness campaign are framed in a manner that is effective and appropriate in the local cultural context.
(1) Graphic Designer	Experienced graphic designer with a background in advertisement and a keen sense of how to communicate core messages effectively through images and graphic design;
(1) Video/Audio Editor and Animator:	Experienced video/audio editor, preferably with the ability to implement animations (e.g. in Adobe After Effects / Animator);