TERMS OF REFERENCE FOR THE DEVELOPMENT AND IMPLEMENTATION OF THE NATIONWIDE DIGITAL CYBERSECURITY AWARENESS CAMPAIGN

1. INTRODUCTION AND BACKGROUND

NATIONAL INFORMATION TECHNOLOGY AUTHORITY, UGANDA (NITA-U), (herein after called **"the CLIENT")** is an autonomous agency of the Government of Uganda established by the National Information Technology Authority, Uganda Act, 2009 to coordinate, promote and monitor Information Technology (IT) developments in Uganda within the context of National Social and Economic development.

The Government of Uganda, through the National Information Technology Authority, Uganda (NITA-U) has received funding from the World Bank/IDA towards financing the Uganda Digital Acceleration Project – Government Network (UDAP-GovNet). As part of the UDAP-GovNet, the project shall focus on complementary infrastructure investments to expand digital connectivity in selected areas and boosting the efficiency and effectiveness of digital government services and create foundations for better resilience, climate adaptation and economic recovery among other interventions. As planned, the extension of affordable broadband to rural areas as well as the rollout of citizen centric e-services will lead to an increase in the number of users that interact, access services online as well as use the internet for socio-economic activities across all demographics. In relation to this expected impact, the cyber threats over the years have increased in persistence and sophistication with a shift of focus to the user at the edge, which raises the need to promote cybersecurity, data protection and privacy awareness for all internet users. Furthermore, the shift to offering services online increases the need to raise awareness on personal data protection and privacy. This will promote an understanding amongst internet users on their rights as well as amongst data controllers and processors on their obligations under the Data Protection and Privacy Act. In order to address this, NITA-U seeks to recruit a Firm to develop and implement a nationwide digital cybersecurity, data protection and privacy awareness campaign.

2.0 OBJECTIVES

The key objective of the assignment is to develop and implement a nationwide digital cybersecurity, data protection and privacy awareness strategy using a mix of multimedia and media communication channels. This will contribute to the gradual building of an information security, personal data protection and privacy culture within the nation among these target groups; youth, internet users, consumers of electronic services, GoU workforce, academia and the general public. The target is to raise awareness on cyber hygiene, cybersecurity, personal data protection and

privacy best practices nationwide. This will build on already existing digital assets under the 'Be Safe Online' Platform.

3.0 SCOPE OF CONSULTANCY SERVICES

The Consulting Firm shall be required to interact with the Directorates of Information Security and the Personal Data Protection Office (PDPO), the Ministry of ICT and National Guidance and other stakeholders deemed necessary to provide vital input into the work, not exceeding a total of 40 stakeholders

The assignment shall be comprised of the following:

a) Undertaking a detailed analysis of target audiences, segments and how to reach them (products, language and transmission channels). These include workforce, youth, general internet users, consumers of electronic services, women and SMEs;
b) An integrated marketing communications plan (IMC) that will detail how the objective - national cybersecurity, data protection and privacy awareness - will be achieved. The strategy should include itemized work plans with clear deliverable outcomes, outreach activities, PR community engagement plan, resources requirements, budget estimations, performance indicators and tools for the implementation of the strategy. At a minimum, the plans must include digital outreach activities spread across the country, child online safety awareness, National CERT/CC promotion, Personal Data Protection Office promotion, data protection and privacy awareness promotion, TV talk shows, influencers and creatives, radio and digital safety education for users of internet as well as e-services. The annual activities should be phased in quarterly engagements including a national cybersecurity awareness month and a data protection month;
c) Designing, producing a content plan, which must at the minimum include themes, calender, key messages, Information, Education and Communication (IEC) materials using a mix of communication channels (digital and offline) and events (central and regional) as well as support multi-language and culture capability. This should include key themes obtained from analysis of existing cybersecurity as well as data protection and privacy documentation. This must be aligned to NITA-U and PDPO branding guides;
d) Implement the approved nationwide digital cybersecurity, data protection and privacy plan as per the contract and budget provisions. The implementation must include updating and continuous improvement in accordance with best practice as well as results from the performance evaluation;
e) Establish and implement tools for tracking and evaluation of the effectiveness of the nationwide cybersecurity, data protection and privacy awareness strategy implementation to measure outcomes on a monthly basis;
f) Transfer of Knowledge - In order to promote skills development with the Project Implementation Team (Project Implementation Team includes 10 representatives drawn from NITA-U, PDPO and Ministry of ICT), lesson learning and knowledge sharing, the consultant will submit a knowledge transfer plan to be embedded in the proposal. . The Consultant will during implementation of the strategy submit as a section in implementation report, achievements made in the Transfer of Knowledge.

4.0 KEY DELIVERABLES AND REPORTING

The expected deliverables for this assignment are detailed herein below. The deliverables/outputs Reports shall be submitted in paper (2 hard copies each – signed original and duplicate) and electronic format such as CDROM or Universal Serial Bus (USB) devices. The Consulting Firm shall be required to submit electronic reports in MS Word, pdf files (secured) and presentations in MS Power Point. Reports will be submitted in English only.

4.1Task 1: Inception Stage

Upon signing the contract, the Consulting Firm shall be availed with information and other supporting materials that provide background data (as indicated in section 8 below) to support in the development of the inception report. This report will contain full details of the consultant's understanding of the assignment, methodology, project plan, stakeholder engagement plan, project risk management plan, associated resource requirements and timelines subject to NITA-U's approval.

Task 1 Deliverable:
The Consultant shall submit an **Inception Report** from Task 1.

4.2 Task 2: Develop the draft Nationwide Digital Cybersecurity, data protection and privacy awareness Strategy and Implementation Plan

The Consulting Firm shall undertake a detailed analysis of target audiences, segments and how to reach them. NITA-U and PDPO shall avail a list of key stakeholders (maximum 40) to consult with whom the Consulting Firm shall initiate meetings. The Consultant shall then develop the draft nationwide digital cybersecurity, data protection and privacy awareness strategy and implementation plan based on analysis of findings above. The draft strategy and implementation plan must include at the minimum the following: a content plan, calender, key message themes, multi-channel, multi-lingual and culture support, itemized work plans with clear deliverable outcomes, outreach activities, PR community engagement plan, resources requirement, budget estimations, indicators and tools for the implementation of the strategy, outreach activities, child online safety awareness, school engagements, data protection and privacy, National CERT/CC promotion, PDPO promotion and digital safety education for users of internet as well as e-services. In order to reach mass awareness, the plan should heavily focus on radio, social media, large circulation print, online and billboards (at busy intersections) in the central region and also regional cities of Gulu, Jinja, Mbarara, Fortporal, Mbale, Masaka, Lira, Soroti and Jinja. The plan should also have a heavy approach to engaging and interactive content in localized languages. Furthermore, the implementation plan should include Knowledge Transfer Plan for NITA-U and PDPO nominated staff in order to promote skills development, lesson learning and knowledge sharing.

The annual activities should be phased in quarterly engagements including a national cybersecurity awareness month and a data protection month as well as reuse existing besafeonline and NITA-U platforms. In addition, as part of monitoring, the strategy should include proposes tools and metrics for tracking and evaluation of the strategy as well as all relevant information considered pertinent to the deliverables and nature of this assignment.

The Consulting Firm shall convene a meeting with NITA-U to review the results of task 2

Task 2 Deliverable

The Consulting Firm shall submit the **draft Nationwide digital Cybersecurity, Data Protection and Privacy awareness Strategy and Implementation Plan.**

4.3 Task 3: Develop the final Nationwide Cybersecurity, Data Protection and Privacy Awareness Strategy and Implementation Plan:

NITA-U will arrange a validation meeting with identified stakeholders at which the Consulting Firm shall present the draft Nationwide Cybersecurity, data protection and privacy awareness Strategy and its implementation plan. The purpose of the validation meeting is to provide a platform for stakeholders to validate and review the drafts as well as to obtain any additional inputs or concerns. The Consulting Firm will document stakeholder concerns and recommendations as well as work with NITA-U to incorporate the feedback. The Consulting Firm shall then proceed to develop the Final updated Nationwide Cybersecurity, data protection and privacy awareness Strategy and its implementation plan with all the necessary changes from the validation exercise.

The Consulting Firm shall convene a meeting with NITA-U to review the results of task 3 and approve the updated Nationwide Cybersecurity, data protection and privacy awareness Strategy and its implementation plan.

Task 3 Deliverable

The Consulting Firm shall submit the **final Nationwide Cybersecurity, Data Protection and Privacy awareness Strategy and Implementation Plan**. This should include an appendix for depository of all records related to task 3.

4.4 Task 4: Implement the Nationwide Digital Cybersecurity, Data Protection and Privacy Awareness Strategy

The Consulting Firm shall implement the Nationwide Cybersecurity, data protection and privacy awareness Strategy as per the approved implementation plan and goals/targets working with NITA-U and PDPO. The Consulting Firm shall carry out these activities on a quarterly basis spread over two years. This will entail use of a mix of multimedia channels and outreach events aimed at raising cybersecurity, data protection and privacy best practices. The consultant shall handle: content production – including copywriting, creatives' development, editing, production of content assets (video, images, infographics, blog articles, etc) with multi-language and culture capability, collateral design and printing, media buy in, translation of content for radio in local languages, tv shows, radio ads, jingles, radio mentions, digital media influencers, celebrity ambassadors, event setup and production. The provisions under the contract will guide this implementation. As part of the agreed upon implementation schedule, the Consulting Firm shall track and monitor performance with metrics and analytics to measure effectiveness. At the minimum, the metrics shall on a monthly basis include listenership for radio and tv as well as hashtag tracking, brand monitoring, influencer performance and social media campaign monitoring and bounce rate,

unique visitors, top pages and average session duration for the besafeonline website. The Consulting Firm should have licensed tools to undertake this tracking and metrics reporting.

The Consulting Firm shall work with NITA-U and PDPO to review and update the Nationwide Cybersecurity, data protection and privacy awareness Plan. This is part of continual improvement to increase the suitability, adequacy and effectiveness of the strategy. Continual improvement should entail consideration of changes in the cyber threat landscape and results of performance reports. The Consulting Firm shall then proceed to revise plan where necessary with all the necessary changes from the review exercise

Task 4 Deliverable

The Consultant shall submit the following:

a) **Monthly performance reports;**
b) **Quarterly detailed reports.**

Table 1: Deliverables and submission Timelines

No.	Name of Deliverable	Contents of Deliverable	Timeline for Submission from date of contract effectiveness
1.	Inception Report	contain full details of the consultant's understanding of the assignment, methodology, project plan, stakeholder engagement plan, project risk management plan, associated resource requirements and timelines	2 weeks
2.	Draft Nationwide Digital Cybersecurity, data protection and privacy awareness Strategy and Implementation Plan	The draft strategy and implementation plan must include at the minimum the following: a content plan, calender, key message themes, multi-channel and culture support, itemized work plans with clear deliverable outcomes, outreach activities, PR community engagement plan, resources requirement, budget estimations, indicators and tools for the implementation of the strategy, outreach activities, child online safety awareness,	6 weeks

		school engagements, National CERT/CC promotion, PDPO Promotion, data protection and privacy and digital safety education for users of internet as well as e-services. Furthermore, the implementation plan should include Knowledge Transfer Plan for NITA-U nominated staff	
3.	Final Nationwide Digital Cybersecurity, data protection and privacy awareness Strategy and costed implementation Plan	Final updated Nationwide Cybersecurity, data protection and privacy awareness Strategy and its implementation plan with all the necessary changes from the validation exercise.	2 weeks
4.	Nationwide Digital Cybersecurity, data protection and privacy awareness Strategy Implementation	a) Monthly performance reports; and b) Quarterly performance reports	Quarterly basis as per the contract for a period of 24 months after approval of the final plan

5.0 MINUMUM REQUIREMENTS OF THE CONSULTING FIRM AND KEY STAFF

5.1 Requirements for the Consulting Firm

a) Shall be a legally registered organization either in Uganda or overseas
b) Demonstration of a strong track record over the last three (3) years in the development and delivery of creative communications campaigns, public relations, strategic communications planning as well as execution and at least 4 (four) assignments of similar type, scope and nature. The firm must clearly show these four similar assignments including details of what was done, results achieved signed reference letters (including start and finish dates)
c) The consulting firm must demonstrate ability to work on cybersecurity, data protection and privacy awareness content
d) The consulting firm must demonstrate ability to field within the country a team of experts with required qualifications and experience for the assignment.
e) Consulting Firms may associate with other firms of a Joint Venture (JV) or a sub consultancy to enhance their qualifications.

5.2 Expertise and Qualifications of Team Members

The consulting firm should field a team of key experts and non-key experts including among others the following key experts.

5.2.1Team Leader (1)

Roles and Responsibilities

a) Responsible for the overall management of the Project and successful timely completion of all deliverables
b) Ensures the quality of all deliverables by providing guidance and coordinating with team members with their inputs and contribution.

Experience

a) The consultant should have at least ten (10) years of experience in assignments that include development and implementation for communication and/or awareness strategies. CV should show this experience
b) Have led at least three projects having similar objectives. CV should show this experience
c) The consultant should have good skills in managing teams and communications
d) Excellent written and verbal communications skills
e) Excellent planning skills
f) Fluent oral and written English language skills

Qualification

a) Should have Bachelor's Degree related to Marketing, Business Communication Management, Public Relations, Mass Communication, Business Computing or related area from an internationally recognized institution
b) Certification in Marketing is an added advantage
c) Additional training in organization change management is highly desirable

5.2.2 Cyber security Lead (1)

Roles and Responsibilities

a) Responsible for quality assurance for all cybersecurity awareness content
b) Research, write and on cybersecurity awareness best practices

Experience

a) Should have at least three (3) years of working IT experience that involve aspects related to cybersecurity
b) Excellent written and verbal communications skills
c) Excellent planning skills
d) Fluent oral and written English Language skills

Qualification

a) Should have a degree in Information Technology, Business Computing, Telecommunications or related area from an internationally recognized institution
b) Certification in Information Security (such as Certified Information Security Manager, Certified Information Systems Security Professional, etc) is required

5.2.3 Content Writer (1)

Roles and Responsibilities
Develop and guide the tone and voice for all communications content

a) Strengthen efficiency of communication messages with a strong writing style
b) Provide original copywriting for all communication messages
c) Edit and proofread texts

Experience

a) Should have at least three (3) years of working experience in a communications and PR related firm
b) Experience in developing communications material
c) Excellent writing and communications skills
d) Fluent oral and written English skills

Qualification

a) University degree in from a reputable university

5.2.4 Visual and Graphics Design Lead (1)

Roles and Responsibilities

a) Deliver creative and innovative ideas for multi-communication channels
b) Design and layout of communication multi-media materials
c) Deliver creative visual and graphic material

Experience

a) Should have at least three (3) years in visual and graphics design
b) Experience in visual and graphic production from ideation to publishing
c) Good understanding of new and evolving technologies and digital platforms
d) Fluent oral and written English language skills

Qualification

a) University degree in Industrial & Fine Art or related area from a reputable institutional

b) Training in graphic design, including the use of design software is an added advantage

5.2.5 Public Relations and Media buying lead (2)

Roles and Responsibilities

a) Responsible for the PR management of the Project and successful timely completion of all deliverables. PR management will include both traditional PR and new age PR, along product and brand PR verticals.
b) Ensures the quality of all PR deliverables by providing guidance and coordinating with team members with their inputs and contribution.
c) Value for money multi-media buying strategy
d) Implementation of agreed upon IMC strategy.

Experience

a) The consultant should have at least three (3) years of experience in assignments that include development and implementation for communication and/or awareness strategies
b) Demonstrable understanding of PR landscape in Uganda
c) The consultant should have good skills in managing teams and communications
d) Excellent written and verbal communications skills

Qualification

a) Should have university Degree in Public relations or related area from an internationally recognized institution
b) Membership to PR affiliated body is a requirement
c) Certification in Marketing is an added advantage

5.2.6 Data Protection & Privacy Lead (1)

Roles and Responsibilities

a) Responsible for quality assurance for all personal data protection and privacy awareness content
b) Research, write and on personal data protection and privacy best practices

Experience

a) Should have at least one (1) year experience on any role that involves aspects related personal data protection and privacy
b) Excellent written and verbal communications skills
c) Excellent planning skills
d) Fluent oral and written English Language skills

Qualification

a) Should have a degree in Information Technology, Business Computing, Telecommunications, Law or related area from an internationally recognized institution
b) Certification that includes domains related to Data Protection and Privacy (such as Certified Information Security Manager, Certified Information Systems Security Professional, Certified Data Privacy Solutions Engineer, Certified Information Privacy Professional, PECB Certified Data Protection Officer, Certified Information Privacy Manager, Certified Information Privacy Technologist, etc) is required

5.2.7 Digital Campaign Lead (1)

Roles and Responsibilities

a) Provide digital strategy and leadership for digital campaigns
b) Provide recommendations on digital opportunities, technologies or tools
c) Identify, recommend and coordinate digital media channels and partners
d) Negotiate and purchase digital media according to the plan approved

Experience

a) Must have at least 5 years demonstrable experience in digital marketing with understanding of SEO and web traffic metrics
b) Experience in influencer marketing, social media engagement, blogger engagement and endorsements
c) Should have experience with audience and buyer persona research
d) Excellent written and verbal communications skills
e) Excellent planning skills
f) Fluent oral and written English Language skills

Qualification

a) Should have a Bachelor's degree from a reputable University
b) Post graduate training in Digital Marketing
c) Membership of an IT affiliated body is a requirement
d) Digital Marketing Certifications are an added advantage

6.0 DURATION OF ASSIGNMENT

The duration of the assignment is expected to be undertaken in an estimated period of twenty-four months from contract commencement.

7.0 REPORTING

The selected consultant shall report to the Director Information Security or any persons that may be selected by the Director Information Security. In addition, the consultant shall be required to provide a weekly and monthly report detailing progress achieved and/or any difficulties encountered prior to providing the final project report. Further information can be obtained at the address below during office hours from 08:00 to 17:00 hours East African Time (EAT) on working days and from the NITA-U website (http://www.nita.go.ug)

8.0 DATA, SERVICES AND FACILITIES TO BE PROVIDED BY THE CLIENT

The Client will provide the following information, data or reports:

a) National Cyber Security Index - Uganda
b) National Cyber Security Strategy
c) Uganda Cyber Capability Maturity Model
d) Data Protection and Privacy Act

e) Data Protection and Privacy Regulations

9.0 REQUIREMENT FOR QUALITY PLANS

The Consultant will be required to demonstrate in their proposal, evidence of adoption of use of a Quality Assurance System as well as to describe how quality control will be implemented in the course of the project.

10.0 PAYMENT SCHEDULE

No.	Description	Percentage
1.	After acceptance of the Inception Report	15%
2.	Draft Nationwide Digital Cybersecurity, data protection and privacy awareness Strategy and Implementation Plan	20%
3.	Final Nationwide Digital Cybersecurity, data protection and privacy awareness Strategy and costed implementation Plan	30%
4.	Implementation of the Nationwide Digital Cybersecurity, Data Protection and Privacy Awareness Strategy and acceptance of a) Monthly performance reports; and b) Quarterly performance reports	30%
5.	After acceptance of the Final Report	05%
Total		100%