Statement of Work

This Statement of Work is valid when signed

This Statement of Work ("SOW") is made and entered into as of the later of the signature dates below ("SOW Effective Date"), by and between "AIF" and "Customer". This
SOW is governed by the overarching Terms of Services Agreement (the "Agreement"), between "Customer" and "AIF".

1. Background

The consumer goods industry is a massive and fundamental part of the Global economy. It encompasses the vast array of products that are intended for celebratory and everyday use by individual consumers and households. Of the two major groups the goods can be classified which are the Fast-Moving Consumer Goods (FMCG) and Durable Goods, "customer" is a reputable brand in the FMCG category.

A few key characteristics of "Customer" Goods Industry involve:

-Brand Driven: Since companies place a significant emphasis on building strong brands that resonate with consumers. Marketing and advertising play a crucial role in differentiating products and influencing purchasing decisions.

-Customer Trends: The industry is constantly evolving to keep pace with changing consumer preferences. Trends in entertainment, refreshment, health, wellness, sustainability, and technology all have a major impact on the types of products that are developed and marketed.

-E-commerce: With the perforation of the internet in the global space and last mile service operators "Customer" can benefit from secure technology and last mile transportation to facilitate the efficient routing of goods to customers who need it directly above a certain amount within the country.

-Industry Challenges and workaround: CSG industry is faced with intense competition, rising production of costs of goods, workers' salaries etc., so adopting sustainability, secure technologies and automation for streamline production will help alleviate cost in the long run.

2. Description of Services

The objective of this professional services engagement is to assist “customer” in testing the security infrastructure of the organization. The activities to be performed may include but are not limited to the following:

a) Vulnerability scanning
b) Penetration Testing

“Customer” acknowledges that AIF may use tools, including cloud-based technologies, penetration testing operating systems, vulnerability scanning tools and penetration testing tools on “Customer” systems and networks. While performing the service, “Customer” agrees that AIF may use all tools at its discretion within the risk boundaries. If AIF determines that “Customer” Technology cannot adequately support the performance of some services, cloud technology stacks may be utilized for the environment and invoiced separately to “customer” for such use cases.

2.1. Internal Vulnerability Scanning:

Internal Vulnerability Scanning aims to assess the security strength of internal systems and services in “customer” environment. AIF will identify and validate vulnerable or misconfigured systems, services, and applications. AIF will perform limited testing against exposed applications, if necessary, which may include hosted web applications, the vulnerability assessment would be focusing on critical vulnerabilities. AIF will use a combination of internally developed tools and scripts in addition to open source and commercial tools.

2.2. External Vulnerability Scanning:

External Vulnerability Scanning aims to assess the security strength of Internet accessible systems, services, and applications as defined in the scope of work. AIF will enumerate the accessible systems and services, which may include publicly accessible cloud infrastructure like Office 365 or G Suite, within the defined scope parameters. AIF will then identify and validate vulnerable or misconfigured systems, services, and applications. AIF will use a combination of internally developed tools and scripts in addition to open source and commercial tools.

2.3. Internal Penetration Testing:

Internal penetration testing aims to assess the strength of the defensive technologies of internal systems and services as well as to determine missing defensive components in ”customer” environment. AIF will perform penetration test against systems, services and applications to determine its ability to detect/withstand a cyber intrusion.

2.4 External Penetration Testing:

External penetration testing aims to assess the strength of the defensive technologies of external facing systems and services as well as to determine missing defensive components in “customer” environment. AIF will perform penetration test against systems, services and applications to determine its ability to detect/withstand a cyber intrusion.

3. Deliverables

The following deliverables would be produced for this service:

Regular Status Reporting: AIF will provide regular status reporting on a weekly basis that summarizes activities completed, significant findings, issues requiring attention and plans for the next reporting period.

Vulnerability Scanning and Penetration Test Report: AIF will provide a detailed written summary for each phase of the assessment. This typically includes an executive summary, key findings, the methodologies followed, and detailed findings. Each finding includes an explanation of the systemic cause, risk rating, and detailed remediation steps.

Executive Briefing – AIF will provide an executive brief that summarizes the assessment in executive format.

4. Schedule and Staffing

The scheduling of Services under this SOW will be as mutually agreed to by all parties. The Services under this SOW will be provided within the twelve (12) weeks period from the SOW Effective Date.

5. Service Fees

All work will be performed on a time and resources basis at the rate of $xxx per day for vulnerability management and $xxx for penetration testing performed. “customer” will pay all invoices as set forth in the agreement. All fees are non-cancelable and non-refundable. “customer” agrees that this SOW represents the complete, final, and exclusive terms and conditions governing the services. As such, AIF may invoice “customer” in advance, unless otherwise stated in this SOW, without the requirement that “customer” provides a subsequent purchase order. Any such subsequently issued purchase order shall be for administrative purposes only.

6. Technology Fees

AIF will determine the technology that is required to support the Services under this SOW. “customer” agrees to pay technology fees from the date of delivery at the price per unit quoted in the table below. These fees will be invoiced monthly and charged to the nearest whole month; they are not pro-rated.

UNIT DESCRIPTION	**PRICE PER UNIT**
Compute Optimized Machine Type	
Minimum (1) cloud node for credential attack	$700 per week
Vulnerability Assessment software	$2000 per engagement

In addition to the technology listed in the table above, AIF may require the use of other tools to facilitate the assessment. AIF will request written (emailed) authorization from “customer” for any charges related to the use of technologies not detailed in the above table.

7. Fee Estimates

DESCRIPTION	ESTIMATED QUANTITY	ESTIMATED COST
External Vulnerability Scanning		
Scanning activities including, but not limited to: - Best effort host and service discovery on up to 15,000 IP addresses - Vulnerability scanning on up to 750 IP addresses - Status reporting - Vulnerability Scanning report	15 Days	$xxxxxx
Internal Vulnerability Scanning		
Scanning activities including, but not limited to: -Vulnerability scanning on up to 70 live systems as provided by "customer" - Internal Vulnerability Scanning reporting - Status Reporting - Vulnerability Scanning report	15 Days	$xxxxxx

DESCRIPTION	ESTIMATED QUANTITY	ESTIMATED COST
Internal Penetration Testing		
Offensive Security activities include, but not limited to: - Reconnaissance - Weaponization - Delivery - Exploitation - Installation - Command and Control - Actions on Objective - Status Reporting - Penetration Test Report	20 Days	$xxxxxx
External Penetration Testing		
Offensive Security activities include, but not limited to: - Reconnaissance - Weaponization - Delivery - Exploitation - Installation - Command and Control - Actions on Objective - Status Reporting - Penetration Test Report	20 Days	$xxxxxx

+234 807 238 9851 aif secure@protonmail.com 13 Olufunmilola Okikiolu Street Ikeja, Lagos.

8. Assumptions

a. All work activities will be performed without day and time restrictions except explicitly stated.

b. If any factor outside AIF's control, including those caused by "customer" or "customer" requirements (such as requirements to refrain from performing tests during specific working times), causes delays in AIF ability to perform the Services or cause the Services to take longer than expected, then notwithstanding any fixed fees, "customer" will be invoiced for technology and time fees for the period of any such delays.

c. Estimated professional fees do not include any hardware, software, licensing, maintenance, or support costs of any AIF or other third-party product or service suggested by AIF as we conduct the activities outline within this SOW.

d. AIF will provide Deliverables to "customer" throughout this engagement. Draft Deliverables are considered final upon confirmation from "customer" (written or oral) or ten business days after the submission date from AIF to "customer", whichever is earlier.

e. When AIF's personnel are performing Services on site at "customer's" premises, "customer" will allocate appropriate working space and physical access for all AIF assigned personnel.

f. "customer" represents that all information provided is true and accurate and that "customer" owns or is authorized represent the owners of the systems, facilities, and/or devices described in connection with the services. "customer" represents that it has obtained all permissions necessary for AIF to perform the service described herein. "customer" will hold AIF harmless against any claims, disputes, or issues arising or relating to foregoing representations.

g. "customer" will make available key individuals that can best help plan operations around network architecture, servers and systems location, and IP addresses.

h. Any changes to the scope of Services or this SOW must be mutually agreed upon in writing by all parties.

9. Additional Security Testing Terms and Condition

i. As a part of the penetration testing, AIF may, among other things, (a) scan "customer" network and systems for ports, services and other entry points that can be exploited; and (b) probe those entry points to try and gain access to "customer" network and systems and determine the severity of the vulnerability.

ii. "customer" UNDERSTANDS THAT, ALTHOUGH AIF TAKES PRECAUTIONS TO AVOID DAMAGE TO "customer" NETWORK AND SYSTEMS, DISRUPTIONS, OUTAGES AND/OR DATA LOSS MAY OCCUR AS A RESULT OF THE PENETRATION TESTING. "customer" represents and warrants that all systems on its network or otherwise accessible during the penetration test have been backed up, and that any data loss or other damage caused by the penetration testing can be easily and quickly reversed.

iii. "customer" will provide to AIF certain information required for performing its tests, including a description and location (e.g., an IP address) of the systems and networks to be tested. "customer" represents and warrants that all information provided is true and accurate and that "customer" owns or is authorized to represent the owners of the systems and networks described in connection with the penetration testing.

iv. "customer" may inform all or a selected group of its employees, contractors, and other third parties about
the penetration testing to be undertaken by AIF. If "customer" decides not to inform anyone of the penetration testing, "customer" understands that people may spend time and money on behalf of "customer" in detecting, blocking, investigating or responding to activities of AIF. IN LIGHT OF THE POSSIBILITY THAT SUCH ACTIONS MAY BE TAKEN AND EXPENDITURES MAY OCCUR, "customer" SHOULD CONSULT WITH "customer" LEGAL COUNSEL AND/OR A MEMBER OF EXECUTIVE MANAGEMENT PRIOR TO ANY SUCH ZERO KNOWLEDGE ENGAGEMENTS. " customer" may also want to consider contacting such third-party service providers as "customer" telecommunications carrier to alert them to the testing.

v. User data contained on systems that are being tested may be accessible to AIF and AIF may download/screenshot portions of such data (e.g., as proof of access).

vi. At any point during the testing, either party may pause or stop the test. Should the testing be terminated, a rationale for such termination shall be provided by the party requesting such termination and such rationale shall be clearly documented and payment for the number of active days and any other additional fees (if any) would be deposited.

10. Contact Information

"customer" will provide AIF with points of contact information in the following table:

Business Line Contact	
Name:	
Title:	
Email:	
Phone:	
Address:	
City:	
State:	

Payables Contact	
Name:	
Title:	
Email:	
Phone:	
Address:	
City:	
State:	

11. Signatures

AIF and "customer" have executed this Statement of Work as of the SOW Effective Date.

Statement of Work

AIF Technology Services	**Customer**
_____	_____
Signature	***Signature***
_____	_____
Name	***Name***
_____	_____
Title	***Title***
_____	_____
Date	***Date***

References:

https://www.mandiant.com/
https://www.telstra.com.au
Frederick County Public Schools (FCPS) Department of Technology Infrastructure (DTI)