SELCOM PAYTECH LTD

ANTI-MONEY LAUNDERING & COMBATING FINANCING OF TERRORISM POLICY

TABLE OF CONTENT

Document Control

Date	Version	Implementer	Change/Review
24-07-2019	V2.0	Compliance department	Sarah Mohamed
15-09-2019	V3.0	Compliance department	Mohammedjawaad Kassam
17-10-2022	V4.0	Internal Controls & Risk Department	Viola Urasa

Confidentiality Agreement and Notice of Proprietary Information

This document contains information proprietary to **Selcom Paytech Ltd** and by reading it you agree to protect its confidentiality and not to disclose the information herein to any third parties outside your organization. You further agree to ensure that any and all parties within your organization that are availed any information herein abide by this confidentiality obligation.

This document shall not be reproduced in whole or in part without the express written consent of **Selcom Paytech Ltd**. The disclosure of information, ideas or concepts presented and contained herein is solely meant for review by your organization and does not constitute any license or authorization to use the same for purposes other than the intended purpose.

1. POLICY CONTEXT

1.1. Introduction

The Anti-Money Laundering Policy, hereafter referred to as “the policy”, specifies the control objectives to evaluate respond to monitor Money Laundering Risk within appetite.

Selcom is committed to acting with integrity in all our business dealings and conducting our activities in accordance with applicable laws and regulations relating to Money Laundering, Terrorist Financing and Proliferation Financing Risk Assessment.

1.2. Purpose

The primary objectives of this policy are to:

- Provide an overview of Anti-Money Laundering
- Provide the Anti-Money Laundering Control Objective requirements

This document addresses the implementation of Anti Money Laundering (AML) and Counter Terrorism Financing (CTF) control measures as applicable for Selcom Paytech Ltd. Corruption, money laundering and the financing of terrorism are major threats to sound economic development and corporate governance. They also pose challenges to employees who, by virtue of the services or products on offer, have a social and legal duty to adhere to anti-money laundering controls and those relating to preventing terrorist financing.

2. DEFINITIONS

2.1. Customers

a. A person or entity that maintains and or has a business relationship with the organization
b. Any person or entity connected with a financial transaction which can pose significant reputation or other risks to the organization

2.2. Money Laundering

Engagement of a person or persons, direct or indirectly in conversion, transfer, concealment, disguising, use or acquisition of money or property known to be of illicit origin and in which such engagement intends to avoid the legal consequence of such action

2.3. Terrorism Financing

Terrorist Financing is the act of providing financial support from either legitimate or illegitimate sources to terrorist(s), terrorist groups or terrorist organizations.

2.4. Suspicious Transactions

Suspicious transaction includes; complex, unusual or large business or non-business transactions, currency transaction, cross border currency, electronic funds transfer, whether completed or not, proposed or attempted with unusual patterns of transactions; insignificant but periodic transactions, which have no apparent economic or lawful purpose; funds or property which are proceeds of crime or are related or linked to persons or are to be used for commission or continuation of a predicate/specified offence.

2.5. Customer due diligence

Means the process by which a reporting person identifies and verifies the identity of the customer

2.6. Financial Intelligence Unit (FIU)

A Government entity (an Extra-Ministerial Department) under the Ministry of Finance and Planning, established by AMLA under section 4, primarily to receive suspicious transaction reports and other reports from reporting persons, to analyze those reports and to disseminate intelligence to LEAs for investigation and possible prosecution, if there are reasonable grounds to suspect ML, TF or any other crime;

3. CONTROL REQUIREMENTS

Money laundering risk is the risk that Selcom employees, third parties or product and services are used to facilitate Money Laundering. This may undermine market integrity resulting in regulatory breaches and/or detriment to customers/clients, counterparties or employees. Money laundering risk events may also result in financial penalties, diminished market performance and damage to Selcom's reputation.

This Policy:

- Is based on applicable legislation, regulatory rules and best practice guidance. It is designed to ensure that Selcom and its employees and its employees know how to detect, prevent and manage Money Laundering risk and the legal and regulatory risks associated with failure to comply with AML requirements. These risks could occur as a result of the actions of our employees, our customers, or third parties or as a result of our failure to establish and maintain an effective control environment to mitigate money laundering risk
- Is mandatory and applies across Selcom and to every employee
- Supports the ERM framework and risk management and compliance programme. The control objectives set out in this policy cover the high level overarching principles in relation to Money laundering risk and more detailed control requirements designed to achieve these objectives are described in the risk management and compliance programme.

4. APPOINTMENT OF MLRO

Selcom has appointed a Money Laundering Reporting Officer (MLRO) who will be responsible for maintaining the risk management programme, and will be entitled to make formal recommendations to maintain or improve risk management policies to be followed. The compliance programme is risk based and subject to oversight by the MLRO to ensure appropriate coverage across businesses and co-ordination among risk management functions. In addition, the MLRO will be responsible to:

- Report any suspicious activity and all AML activities recorded to the financial intelligence Unit (FIU)
- Ensure all staff that meet or contact clients and potential clients of this firm are required to acknowledge that the policy and procedures have been read and understood before meeting or contacting clients.
- Maintain a list of all staff who have read and signed the AML Policy
- Identify all new and existing clients will be verified to a reasonable level of certainty
- Establish and maintaining the program to identify, assess, monitor and manage risks related to AML, fraud and any related criminal financial activities.
- Receive Anti-Money Laundering Internal Suspicious Activity Reports from staff and escalating to the Financial Intelligence Unit where appropriate. The officer submits an annual report to senior management outlining the status of AML controls and any recommendations for improvement. The MLRO reports to the Selcom Compliance Unit giving an appropriate degree of independence from the commercial aspects of the business.

5. RISK CATEGORISATION

For proper risk assessment of business relationship with customers and evolving suitable monitoring mechanism, all customers are to be categorized as High risk, Medium risk and Low risk. The risk categorization is meant for proper monitoring of clients and their transactions. Risk Categorization done by the responsible staff should not be disclosed to the client. The extent of knowledge/information available on clients to prove their identity sufficiently will determine the risk perception and concomitantly risk categorization. The list below provides an overview of clients who may be assigned different risk categories:

Low Risk	Medium Risk	High Risk
Entities/Individuals based in low risk or no risk country (Nationality irrelevant).	Entities/Individuals based in Moderate Risk Countries (Nationality irrelevant).	Entities/Individuals based in High Risk Countries, Very High Risk and Non Co-operating Countries (NCCT) (Nationality irrelevant).
Small-to-medium enterprises with small turnover in the account		Politically Exposed Persons (PEPs) i.e. individuals who are or have been entrusted with prominent public functions in the country or a foreign country, important political party officials, etc.
Clients which are listed companies, regulated entities etc. where sufficient knowledge in public domain is available		Trusts, Clubs, Associations, charities, NGOs receiving donations
Government Departments and Government owned companies, regulators and statutory bodies etc.		Firms with sleeping partners. Companies whose shareholders are family members.
		Entities dealing in antiques, arms, money services bureaus (entities and not its employees)

Responsible staff members need to review risk categorizations of clients periodically. Such review of risk categorization of customers should be carried out at frequency of not less than once in twelve (12) months.

6. AML CONTROL OBJECTIVES

This policy establishes a risk-based approach to managing Money Laundering risk. A risk based approach means that the processes and controls implemented to comply with this policy will vary depending on the assessment of Money Laundering risk.

6.1. On boarding - Customer Due diligence

Prior to establishing a business relationship, the business must assess the Money Laundering risk posed by the customer. A Know-Your-Client (KYC) policy is established to ensure that the identities of all new and existing clients are verified to a reasonable level of certainty. This will include all individual clients, all directors and shareholders with a stake holding of 25% or more of client companies, all partners of client partnerships, and every board member of client charities. Identities will be verified either online or face-to face or by a combination of both.

6.2. KYC for Clients

The following documentation may be presented by the prospective client, partner or third party. Selcom's portfolio of customers includes corporate, banks, mobile network operators (mobile money) and merchants.

Selcom as a payment system provider switches and facilitates movement of digital funds between sending and receiving parties. For the services where Selcom does not directly interact with senders and receivers of funds, the collection of KYC on senders becomes the onus of the sending institution and collection of KYC on receivers, the onus of the receiving institution. As reporting institutions under Tanzanian regulation, the sending and receiving entities collect KYC on their customers which allows the determination of the origin and destination of funds.

Selcom shall take reasonable measures to satisfy themselves of the identity of the Sending and Receiving clients. The entities shall be required to produce an official record reasonably capable of establishing the identity of the applicant.

- The registered name the entity;
- The registered address of the entity;
- Any government issued document that provides the date of birth such as a government ID and as
- Business license
- TIN
- Certificate of incorporation
- Additional documents may include passport copy of directors and audited financials

In addition to the above, during on boarding, Selcom shall collect from the entities the following:

a. Signed Agreement or Merchant Application Form, Partner Due Diligence Form or vendor application form
b. Additional KYC for the entity being on boarded:
    i. Directors'/Managers' ID (National Identification Card or Passport)
    ii. Business License
    iii. Certificate of Incorporation
    iv. TIN Certificate of Registration
    v. VAT Certificate of Registration (where applicable)

Low KYC exceptions will be made and any changes as per BOT law will be implemented and aligned on.

Selcom screens each of its merchants and service providers and each other representative and agent (including, but not limited to, each Third Party Processor at the time of onboarding), and regularly thereafter on an ongoing basis, against applicable sanctions lists.Every entity and individual is subjected to OFAC screening during the time of onboarding, as well as whether any associated individuals that are Politically Exposed Persons, or relatives thereof.

No activity shall be conducted in a geography (country or region or other geographic area) that is the subject of applicable sanctions as identified by OFAC. In addition, no activity shall be conducted with a person, entity, or government on the OFAC sanctions lists.

*****Annexure I provides the Partner Due Diligence Form and Merchant Application Form and associated on boarding forms.

6.3. Enhanced due diligence and monitoring

Selcom shall apply enhanced due diligence and monitoring to its products and services when used by people that the company deems to be

- High risk, as the result of an assessment of relevant risk factors
- Politically Exposed Persons (PEPs)

- Employees who are able to administer payment accounts or close associates or relatives of employees
- In any case where-
    (i) A transaction is complex and unusually large
    (ii) There is an unusual pattern of transactions, and the transactions have no apparent economic or legal purpose; or
    (iii) In any other case which by its nature can present a high risk of money laundering, terrorist financing or proliferation financing.

6.4. Ongoing Customer Screening

Selcom must conduct screening on the customer and their related parties on an ongoing basis as set out in the merchant agreement.

6.5. Ongoing Due Diligence

Selcom must undertake effective ongoing due diligence in line with regulatory requirements.

6.6. Third Party requirements

Prior to entering into a business relationship with any third party, including entering into a commercial relationship with a supplier or client, or permitting any consumer to use its products or services, Selcom shall undertake due diligence on the third party in order to establish that the relationship is:

- Legal;
- Within the company's risk parameters;
- Free from excessive reputational or financial risk

Selcom will as well perform an ongoing Risk Analysis to assess the level of risk exposure considering the customers, products, services, entities and geographic locations risk and to derive appropriate security measures from this analysis. Safeguards are derived from the results of the analysis.

6.7. Prohibited and Restricted Relationships

Selcom must not establish a business relationship or conclude a single transaction with an anonymous client or a client with an apparent false or fictitious name.

Selcom must not establish business relationship or conclude a single transaction with individual entities that Selcom has deemed prohibited (Refer to sanctioned countries as per BOT)

6.8. Reporting of suspicious transactions

6.8.1. Suspicious Activity Management Process

A Selcom staff is required to disclose any suspicious activities or evidence of financial crime or terrorist financing immediately to the internal controls and risk department who shall then complete an internal suspicious activity report (iSAR) to the Compliance Manager who is the chosen MLRO.

The MLRO shall review the iSAR to determine whether there are any grounds for suspicion and if so further investigations shall be done. Upon completion of the investigation conducted by the internal controls and risk department and if any such investigation is warranted, a disclosure to the law enforcement agencies must be made.

According to the Anti-Money Laundering Act of Tanzania Sections 16(1) states that, "Upon reasonable suspicion that the transactions described in sub regulation (1) may constitute or be related to money laundering, terrorist financing, proliferation financing or predicate offence, a reporting person (the

appointed MLRO) shall promptly report the suspicious transaction to the Financial Intelligence Unit (FIU)".

Section 17 of the AML Act states, a report made shall be submitted to the FIU as soon as possible but not later than twenty four working hours after a reporting person becomes aware or has knowledge of a suspicious transaction.

The report shall contain:

i. A full description of the suspicious transaction, including the reasons for suspicion
ii. Action taken by the reporting person in connection with the suspicious transaction concerning which the report is made
iii. Copies of supporting documents in respect of the suspicious transaction.

******The MLRO should use the form attached in the AML Act of Tanzania to report to Tanzania FIU*

6.9. Transaction Monitoring

- Continuous monitoring is an essential ingredient of effective KYC procedures and the extent of monitoring should be according to the risk sensitivity of the account and the monitoring of transactions shall equally be done in line with all regulatory requirements.
- Special attention will be paid to all complex, unusually large transactions and all unusual patterns which have no apparent economical or visible lawful purpose.
- All suspicious transactions shall be reported to the respective financial intelligence units within the set timelines as per the respective regulations.

Selcom has developed and operationalized a system which is capable of capturing transactions suspected to be of the nature of money laundering or terrorist financing. This system is updated periodically. All transactions are processed through this monitoring system.

Selcom has defined various thresholds as provided in a section below, the crossing of which will generate alerts for transactions that exceed these predefined thresholds for investigation.

The system has a capability to audit the transactional history of a transaction initiator and perform analysis for any abnormal behavior to identify potential money laundry activities. This is post event analysis that will be carried out by the MLRO on daily basis.

6.10. Record retention and deletion

In compliance with AML regulation and Selcom data privacy policy, Selcom must maintain transactions and where applicable related parties information, data and documentation captured in accordance with the AML policy and standards and ensure that they are deleted /destroyed at the expiration of the applicable data retention period which is a maximum of 10 years.

6.11. Risk Management

- This AML & CFT policy and related procedures cover management oversight, systems and controls, segregation of duties, training and other related matters which ensure effective AML & CFT risk management and implementation Selcom's AML & CFT policy.
- To ensure effective AML & CFT risk management, the following tenets shall be observed:
    a. A customer's identity shall be verified at all times
    b. Ongoing due diligence on business relationships and scrutiny of transactions shall be conducted to ensure that the transactions conducted are consistent with the customer profile.
    c. AML & CFT risk assessment

d. Internal audit function shall bear the important role of evaluating and ensuring adherence to the AML/CFT policies and procedures
e. The compliance report in this regard shall be put up before the audit and risk committee of the board on quarterly intervals.

6.12. Training

The business are required to develop and maintain an effective ongoing risk based AML training programme that ensure all relevant employees are aware of their legal and personal responsibilities.

The MLRO is required to provide training to staff members on an annual basis at a minimum on the firm's policies and procedures, the relevant anti-money laundering, countering terrorist financing and countering proliferation financing laws and regulatory requirements. The training will be tailored down depending on staff roles with high risk profiles. AML training is given to all staff in the Reconciliation, Finance, Business Operations, Data Analysis, Compliance and Customer Care Departments. Training may also involve third party vendor who are directly involved with transactions.

6.13. Ongoing training and awareness

The Risk manager will be responsible to ensure that staff, in particular those responsible for transaction monitoring or establishing business relationships are aware of different possible patterns and techniques of money laundering which may occur in their everyday business. Training also covers the general duties arising from applicable external (legal & regulatory) requirements, internal requirements and individual duties which must be adhered to recognize money laundering or financial criminal activities.

Refresher training shall take place:

- At least once every six months
- Immediately upon regulatory change
- Immediately upon being aware of a failure to comply with company policy or legal obligation in relation to financial crime or terrorist financing.

6.14. Management Information

The business must provide appropriate management information and reports which are relevant, reliable and timely to senior management regarding business compliance with this policy.

6.15. Policy Update

Updates or modification of this policy shall be initiated by the business needs in line with regulatory requirements on AML and CFT or shall be put up for review to the Board of Directors once every two years whichever comes earlier.

APPROVAL

Name: **Sameer Hirji**

Title: **Executive Director**

Date: **28th October 2022**

Signature:.....

SELCOM PAYTECH LIMITED
8th Floor, Uhuru Heights
Bibi Titi Mohamed Road
P. O. Box 20656
Dar es Salaam - Tanzania

7. Annexure

7.1. Annexure 1: Due Diligence form

DUE DILIGENCE FORM

1	Registration Information	Response
	Registered Name of Company	
	Country of Registration	
	Registration Number	
	Registration Certificate (provide copy)	
	Registered Address	
	Brand name if different from Registered Name	

2	Presence in Other Countries *(Please attach a list with the following information for each entity)*	Response
	Local Registration Information	
	Local Registered Name	
	Country of Registration	
	Local Registration Number	
	Local Registration Certificate (Provide copy)	
	Brand name if different from Registered Name	
	Local Registered Address	
	Local Tax Registration Number	

3	Type of Service	Response
	Brief Description	
	Scope of service (No of Countries, service categories etc)	

4	Ownership Information	Response
	Name of Shareholder and % of shareholding (include details on beneficial owners if any)	
	For listed companies please provide list of shareholders holding more than 10% shareholding and where these are natural persons, attach certified copies of their Identity cards.	
	For non-listed companies, provide a list of shareholders holding more than 20% shareholding individually and if natural persons, attach certified copies of their identity.	
	If the shareholders greater than 10% and 20% above are companies or persons other than natural entities, attach registration documents as well as certified copies of their directors.	

5	Management	Response
	Name of CEO/Managing Director or equivalent	
	Current List of Board Members or equivalent	

6	Regulatory Status	Response
	Name of the Regulatory Authority	
	Countr(y) (ies) to which the approval applies.	
	Reference ID/ number of the license to provide the service	
	Copy of Regulatory approval to offer the service	

7	Third Party Partners	Response
	Does the organization rely on third parties to carry out any component of the service it is offering to Selcom?	
	Please provide list of all such third party partners and the service components that they are responsible for.	

8	Anti-Money Laundering & Counter Terrorist Financing	Response
	Provide updated copy of your organization's AML policy	
	Does the organization rely on third parties to carry out any component of the AML& CTF policy?	
	Please provide list of all such third party partners and the components that they are responsible for.	

9	Know Your Customer	Response
	Provide updated copy of your organization's KYC policy	
	Does the organization rely on third parties to carry out any component of KYC?	
	Please provide list of all such third party partners and the components that they are responsible for.	
	Does the organization have a policy on the monitoring of local and international transactions and detection of suspicious or unusual activities?	
	Please provide a copy of such policy.	

10	Anti- Bribery and Corruption (ABC)	Response
	Does the organization have a policy on ABC?	
	Please provide a copy of such policy.	

11	Data Protection and Information Security	Response
	Does the organization have in place a Data Protection and Information Security Policy?	
	Please provide a copy of such policy	
	Please indicate jurisdiction in which servers containing customer information regarding the service will be located	

12	Required Documents *(List of documents to be submitted (tick all submitted))*	Response
	Company Charter – Memorandum & Articles of Association	
	Ownership and Management Structure, individual persons holding more than 10% of the company	

	Ownership and Management Structure, including details of shareholding, up to listed company	
	Company Certificate of Incorporation	
	Financial Services License from Central Bank or other Regulator	
	Trade License, if applicable	
	AML/CFT Registration, if applicable	
	Chamber of Commerce Certificate, if applicable	
	Passport or National ID Copies of Directors and Executive Management	
	Audited Accounts - last 3 years	
	Credit Rating by external agency, if available	
	Latest Inspection / Audit Report from Regulator, External Auditor or Internal Auditor	
	Compliance Manual	
	Board Resolution / Power of Attorney authorising signatory for the PDD	
	Company Profile with Organisation Chart	
	AML and Sanctions Policy, together with other relevant compliance policies or handbooks outlining processes for KYC and Sanctions	
	List Screening	
	Anti-Bribery & Corruption Policy	
	Data Protection Policy	
	Agent/Partner Oversight policy document, outlining how the network is onboarded and oversight is maintained	
	List of all transaction limits applicable to the service intended to be undertaken with the partner	
	A copy of your PCI-DSS Attestation of Compliance (AoC), where applicable	

13	**Declaration**	
	By signing this form, the Company identified in Section 1 (the "Company"), hereby certifies that the information the form contains as well as documentation. Selcom must be informed of any material changes to the information I have provided within 14 calendar days of the change. and supporting documents provided in accordance with Section 13 is accurate, true and to the best of its knowledge represent factual information	
	Signed:	Name:
	Title:	Date:

14	Disclaimer
	Selcom Disclaimer Notice
	By signing this form, the Company identified in Section 1 (the "Company"), hereby certifies that the information the form contains as well as documentation and supporting documents provided in accordance with Section 12 is accurate, true and to the best of its knowledge represent factual information. The Company understands that Selcom may contact and obtain additional information about your Company from all necessary and relevant individuals, governmental and/or regulatory bodies for purposes of verifying the information contained in this Due Diligence form.
	Selcom General Notice
	Please ensure that the information contained in this questionnaire is accurate, complete and up to date. Material inaccuracies in the business or personal information provided in this questionnaire may cause Selcom to reject a business relationship and may constitute an offence under applicable law. Selcom, who relies on the information contained in this form to decide whether to enter into a business relationship with the Company, reserve its rights to take appropriate measures should it be revealed that any of the information provided herein is inaccurate or untrue. The Company hereby permits Selcom, its associates and Affiliates to obtain, verify and check any information relating to the Company and any of its directors, shareholders or associates, including credit information at part of this Due Diligence process or at any time thereafter. The Company recognizes and accepts that a credit check conducted by Selcom has the potential to impact the Company's credit score and that Selcom takes no responsibility for any losses or damages resulting from any credit check or any verification process.
	Selcom Confidentiality Notice
	Selcom understands that the information provided by the Company as part of the Due Diligence Form is confidential and refer to strategic information known, Selcom requires that the Company signs a Non-Disclosure Agreement ("NDA") in order to ensure that (i) the Confidential Information be used not necessarily known to third parties. As the disclosure of this information could cause irreparable harm if it were to be disclosed and/or publicly at least with the same reasonable degree of care as Selcom' associates uses to protect its own confidential Information to prevent disclosure or unauthorized use of confidential information and (ii) only disclose Confidential Information to Selcom' respective employees who need to know it for the purpose indicated in the NDA, provided that these employees are required to abide and be bound by confidentiality obligations.

7.2. Annexure 2 – Merchant Application Form

SELCOM PAY MERCHANT APPLICATION FORM

Section I: Company Registration Information

i. Company Registered Name: _____
ii. Trading Name: _____
iii. Registered Address: _____
iv. Town/City: _____
v. GPS Lat._____ GPS Long._____
vi. Type of ownership _____
( ) Sole Owner ( ) Corporation ( ) Partnership/Joint Venture ( ) Limited Liability Com
( ) Public Liability Company ( ) Government ( ) Non-Profit Organization (NGO) ( ) Religi
( ) Other (Specify)_____
vii. Merchant Category/Type of Business: _____

Section II: Primary Authorised Contact Information

This section gathers information about the contact person for your organization who will rec
information, transaction portal credentials and invoices. All correspondence between Selco
to the person specified below.

i. Authorized Contact Name:
ii. Designation: _____
iii. E-mail Address: _____
iv. Mobile Phone: _____

Phone Number		Phone Number	
Email Address		Email Address	
Pay Number 3		**Pay Number 4**	
Push Printer		Push Printer	
Name of Account		Name of Account	
Contact Name		Contact Name	
Phone Number		Phone Number	
Email Address		Email Address	

Section IV: Push Printer Details

i. Selcom Pay push printer required? ( ) Yes ( ) No

ii. No. of Printers Requested:_____

iii. Payment:_____

By signing section IV, I/we hereby acknowledge that I/we have been assigned thermal pu
I/we am/are desirous to operate said thermal Push Printer at my/our premises. I/We a
remain with Selcom. I/We will use said device only for purposes of providing Masterca
damage to or destruction of the thermal push printer, as well as its loss. I/We shall be sol
thermal push printer, including but not limited to thermal paper, electricity, security, and any

Section V: POS Device Request

POS Device Requested? ( ) Yes ( ) No
No. of POS devices requested_____ Payment:_____

By signing this Selcom Pay Merchant Application Form, I/we hereby agree that: The POS
Selcom's instructions. Any tampering or attempts to modify the hardware or software of the de
warranty over the continuous operation of such POS Device or its fitness as to my/our purpose
POS Device runs on the latest upgrade software provided by Selcom. From time to time, at my/
facilitate the exchange of faulty equipment/device, subject to the standard warranty terms of su
In the event that the device is out of warranty, such POS Device will be replaced/repaired
reparation and replacements shall be borne by me/us and will be charged on the actual cost incu

Section VI: Company Settlement Details

Complete this section with information about the bank or mobile money wallet where you w

Bank Name		Bank Name	
Branch Address		Branch Address	
Account Name		Account Name	

( ) VAT Certificate of Registration
( ) TIN Certificate of Registration *(mandatory)*
( ) Director's ID *(For Tanzanian citizens, NIDA is mandatory)*

Section VIII: Acknowledgement

I/We hereby declare that all information furnished herein is true and complete to my kno
Selcom Pay Merchant Agreement. I/We further acknowledge and confirm that I/we have
Pay Merchant Agreement which are attached to this Form and have understood them
representation or waiver made by Selcom Paytech LTD other than that set out in the Sel
irrevocably and unconditionally agree to observe, fulfill and comply with the provisions of th

7.3. Annexure 3 – Merchant Agreement

Selcom Pay Mastercard QR Merchant Agreement

This Agreement is effective as of the DATE_____

BETWEEN

Selcom Paytech Ltd, whose registered office is at 8th Floor, Uhuru Heights, Bibi Titi Moha Salaam, Tanzania (hereinafter referred to as "SELCOM");

AND _____

The Party named and described in Section I of the Selcom Merchant Application form (h "MERCHANT") of the other part.

Whereas, SELCOM is a provider of electronic payment processing solutions and the ME services, expertise and infrastructure to offer mobile payment options to its End Users.

NOW, THEREFORE, in consideration of the terms and conditions herein contained, and receipt and sufficiency of which is hereby acknowledged, it is agreed as follows;

1. Definitions

The following terms are defined for use in this Agreement, unless the context of

1.1 "Business Day" means a day (other than a Saturday, Sunday or public holiday)

1.6 "POS Device" means a point of sale device issued by that can be utilised for the

1.7 "SELCOM Delivery Channels" means the various electronic payment channels u payments;

1.8 "Selcom Pay" means SELCOM's electronic merchant payment platform that facil to, the acquisition and onboarding of merchants, Merchant payments through the and payment settlements;

1.9 "Services" means the Selcom Pay electronic payment processing service operat MERCHANT;

1.10 "Service Charges" means a transaction processing fee due to SELCOM for each Selcom Pay Services.

2. Formation of Contract

2.1 The Parties acknowledge that no representations, warranties or statements mad forms any part of the contract, nor has induced either Party.

2.2 SELCOM may vary any provision in this Agreement, without prior consent from M as a direct result of new legislation, statutory instrument, Government regulations imposition or alteration of government tax or as a result of any review of SELCOI the industry, recommendations from regulator bodies or for such other reasons a SELCOM shall in such circumstances endeavor to give MERCHANT thirty (30) d

3.1.2 MERCHANT shall ensure that it has acquired all necessary approvals, permissic offered to its End Users. MERCHANT shall be responsible for the content, qualit for ensuring that these services comply with this Agreement.

3.1.3 MERCHANT shall display prominently, the Pay Number and/or QR Code, as wel trade or service marks or copyright material as SELCOM may provide and stipul premises or website of the MERCHANT.

3.1.4 MERCHANT shall ensure that the access password for the web portal provided I unauthorized persons at all times during the Term.

3.1.5 MERCHANT shall not deduct any charges for the transaction from the End User. by the End User shall be exactly equivalent to the price(s) of goods and/or servic

3.1.6 MERCHANT shall ensure the attendance of its staff, personnel and/or agents at SELCOM.

3.1.7 MERCHANT shall immediately notify SELCOM in writing if there is any change i services offered by the MERCHANT.

3.1.8 MERCHANT agrees to hold in confidence this Agreement and all information, do disclosed to it by SELCOM and shall not disclose to any third Party or use confic connection with the performance of this Agreement or any part thereof without S

3.1.9 MERCHANT shall provide SELCOM on request with information or material rega Users or agents.

3.1.10 MERCHANT shall ensure that goods and/or services provided are not used for a transmission or offering of any information or services which are libelous, unlawf defamatory, or in any way infringe the laws governing copyright, intellectual prop material that is slanderous or may cause offence in any way.

3.1.11 MERCHANT shall ensure that any relevant third Party using its facilities shall be

3.1.12 MERCHANT shall only use the Selcom Pay Trademarks and Trade names for pr services during the Agreement period and for no other purposes whatsoever.

3.2.3 SELCOM shall provide MERCHANT with appropriate and reasonable technical s

3.2.4 Selcom will supply POS Devices and accessories at MERCHANT's cost.

3.2.5 A Payer may make Payments to the MERCHANT utilising a POS Device, the Se channel made available by Selcom for such purposes in accordance with this Ag

3.2.6 SELCOM may, from time to time, make changes to equipment used to handle ar are at the sole discretion of SELCOM, and shall be made without prior consent f

3.2.7 SELCOM shall settle the total value of funds collected on the MERCHANT's beh Channels, less Service Charges, into the MERCHANT's preferred bank account Business Day (on a T+1 basis).

3.2.8 SELCOM shall provide branding and advertising material to facilitate the promot that have been supplied to MERCHANT at no cost shall remain the property of S upon demand or upon termination of this Agreement.

3.2.9 SELCOM shall provide an online web portal through which MERCHANT shall ha payment collections.

3.2.10 SELCOM shall have the right at any time during the Agreement period to inspect

5. Limitation of Liability

5.1 MERCHANT shall be responsible at all times for maintaining the security of its shall bear no liability for the loss or damage in part or whole, of such data, to th been caused or contributed to by MERCHANT.

5.2 SELCOM shall not be liable for any indirect, incidental, special or consequentia communications, lost data, or loss of profit, or economic loss arising out of or ir any consequent negligence by its officers or employees. This Agreement does agency/principal relationship between the MERCHANT and SELCOM.

6. Chargeback Processing

6.1 The MERCHANT shall assist SELCOM when requested to investigate any of th through the Selcom Pay Service. The MERCHANT permits SELCOM to share End User, the End User's SELCOM Delivery Channel, and the MERCHANT's fi and/or mediate a Chargeback. SELCOM shall request the necessary informatic Chargeback.

6.2 If a Chargeback dispute is not resolved in the MERCHANT's favor or the MERC Chargeback, SELCOM shall recover the Chargeback amount and any associat the MERCHANT's electronic payment collections. The MERCHANT acknowled timely manner when investigating a transaction, including providing necessary the request, may result in an irreversible Chargeback. SELCOM reserves the ri charge a fee for mediating and/or investigating Chargeback disputes.

7. Suspension

7.1 SELCOM shall not be liable or responsible to the MERCHANT in any manner v

9. Prevention of Money Laundering and the Financing of Terrorism

9.1 The transfer of funds through the Selcom Pay service which is or which forms par is intended to facilitate, aid or finance the commission of any crime is expressly pr

9.2 SELCOM shall monitor and report any suspicious activity by the MERCHANT and Compliance Officer who may eventually escalate the suspicious activity to the rele

9.3 Notwithstanding anything to the contrary contained in this Agreement, SELCOM s this Agreement in the event that SELCOM reasonably and in good faith determine any of its obligations contained in this clause.

10. General

10.1 This Agreement together with the Selcom Pay Merchant Application Form constitu Parties and supersedes any previous Agreement or relationship of whatsoever na the Services. A variation of these Terms and Conditions is valid only if it is in writir Party.

10.2 Either Party's rights and powers under this Agreement are not affected if it fails to at any time. If any part of this Agreement is not enforceable it will not affect the re

10.3 Neither Party shall be deemed to be in breach of this Agreement for any failure in of its reasonable control, to include, but not limited to any act of God, inclement w drought, lightning, fire, lockout, trade dispute, labor disturbance, act or omission c MNO or other authority, war, military operators, or riot.

10.4 Any dispute arising out of or in connection with this Agreement shall be referred to (Cap 15) of the laws of the United Republic of Tanzania R.E. 2002. Notwithstandi meet its costs incurred in exercising this provision.

IN WITNESS WHEREOF the Parties hereto have executed this Agreement in the mann

For and on behalf of MERCHANT on this DATE _____

Merchant Name _____
Name _____
Signature _____
Designation _____

For and on behalf of SELCOM on this DATE_____
Recruited By: Name _____
Signature