MyanmarPay - Digital Payment System

Code of Conduct

&

Rules and Procedures for Person to Merchants (P2M)

2024

Statement of Agreement
with Central Bank of Myanmar

We, the undersigned, _____Bank/ MFSP/ Acquirer will commit to the followings:

1. Adhere to and comply with the spirit of values and practices under this Code:

2. Apply this Code to the relevant types of Banking and Financial Institutions' activities:

3. Promote and strengthen the sustainability of the digital payment sector by promoting this digital payment scheme and inclusive digital financial services in compliance with the regulations of the Central Bank of Myanmar:

4. Fairly conduct the activities without illegal competitive advantage or unethical practices:

5. Make this code available for all stakeholders and ensure the compliance of the signee institution.

Signatories

Name:
Position:

Table of Contents

1. Introduction 6
   1.1 Interoperable Real-Time Retail Payments System: 6
   1.2 Central Merchant Repository: 6
   1.3 Clearing and Settlement capability: 6
   1.4 Dispute Settlement capabilities: 6
   1.5 QR Generation: 6
   1.6 QR Repository: 6
   1.7 Certification of QR: 6
   1.8 White Label Merchant/ Consumer Applications: 7
2. Purpose 7
   2.1 Ensure Operational Sustainability and Security: 7
   2.2 Foster Trust and Transparency: 7
   2.3 Promote Digital Financial Inclusion 7
   2.4 Mitigate Risks: 7
   2.5 Enhance Consumer Experience: 7
3. Definitions 7
   3.1 Definitions 7
   3.2 Participants: 9
   3.3 Market Discount Rate 9
   3.4 RTRP (Real-Time Retail Payment): 9
   3.5 P2P (Person-to-Person): 10
   3.6 P2M (Person-to-Merchant): 10
   3.7 P2G (Person-to-Government): 10
   3.8 B2G (Business-to-Government): 10
   3.9 TPS (Transactions Per Second): 10
   3.10 On-Us Transaction 10
   3.11 Off-Us Transaction 10
   3.12 Anti-Money Laundering (AML): 10
   3.13 Combating the Financing of Terrorism (CFT): 10
   3.14 Know-Your-Customer (KYC): 10
   3.15 Fraud Management: 10
   3.16 Blacklist Screening: 10
   3.17 Dispute Management 11
   3.18 RI 11

3.19 OI 11
3.20 Centralized Merchant Repository: 11
3.21 System Integration Testing (SIT): 11
3.22 User Acceptance Testing (UAT): 11
4. Participant Onboarding 11
4.1 Eligibility Requirements 11
4.2 Application Process 11
4.3 Qualification of Participation 12
5 Centralized Merchant Repository (Repo) 12
5.1 Centralized Merchant Onboarding Process 13
5.2 Merchant Application 13
5.3 Due Diligence: 13
5.4 System Integration and Testing 13
5.5 Go-Live 14
5.6 Merchant Onboarding Limits: 14
5.7 Merchant Change of RI: 14
5.8 Inactive Merchant IDs: 15
5.9 Ongoing Compliance Merchant IDs: 15
5.10 Merchant Categorization 15
5.11 Merchant Data Management: 16
5.12 Merchant Reporting and Settlement 16
5.13 Merchant Risk Management 17
6 Security and Compliance 17
6.1 Security Mechanisms 17
6.2 Consumer Data Protection 18
7 Dispute Management 18
7.1 Dispute Escalation and Categories 18
7.2 Dispute Resolution Process 19
7.3 Dispute Management Team 19
7.4 Reporting and Documentation 19
7.5 Dispute Resolution Timelines 20
7.6 Dispute Resolution 20
7.7 Dispute Cost 21
8 Technical Requirements 22
8.1 System Integration 22
8.2 Data Security and Encryption 23
8.3 Testing and Certification 23

8.4 Branding Requirements 23
8.5 Operation Readiness 23
8.6 Testing Environment Support 23
9 Termination and Suspension of Participants 24
9.1 Right to Terminate 24
10 Risk Management Mechanisms 25
10.1 Fraud and Risk Management 26
10.2 AML/CFT 27
10.3 Incident Response and Reporting 27
11 Roles and Responsibilities 27
11.1 Roles & Responsibilities of the Central Bank of Myanmar 28
11.2 Roles & Responsibilities of the Digital Payment Switch 28
11.3 Roles & Responsibilities of the Participants 29
12 Reporting Requirements 30
12.1 Financial and Operational Reports 30
12.2 Risk and Security Reports 30
12.3 Customer and Merchant Reports 31
12.4 Branding and Commercial Reports 31
12.5 Commercial Reporting 32
12.6 Commercial Agreement 32
13 Policy for Settlement Banks and non-bank payment service providers 32
13.1 Pre-joining Requirements 32
13.2 Liquidity Management and Float Allocation 33
13.3 Limit on Non-bank payment service providers relationships per Settlement Bank for MyanmarPay 33
14 General Provisions 33
14.1 Amendment of the Code of Conduct 33
14.2 Governing Law 33
14.3 Confidentiality 33
14.4 Dispute Resolution 34

1. Introduction

All participants of the **MyanmarPay, Digital Payment Switch,** shall effectively comply with the MyanmarPay's Code of Conduct. For the purposes of this document, the Digital Payment Switch shall hereinafter be referred to as 'MyanmarPay'. The MyanmarPay is owned and regulated by the Central Bank of Myanmar (CBM) as part of a nationwide effort to embrace digital transformation. It is designed to promote digital financial inclusion, improve the use of the Digital Payment, and provide a seamless, secure payment experience for individuals, businesses, and government agencies.

MyanmarPay enables financial inclusion and cross-border remittances, supporting interoperability between Southeast Asian payment systems via switch to switch connection. The participants of the MyanmarPay Digital payment switch are expected to uphold the highest standards of integrity, operational excellence, and consumer protection

The Digital Payment Switch includes a number of key components, including:

1.1 Interoperable Real-Time Retail Payments System:

MyanmarPay ensures seamless electronic transactions by promoting compatibility among various payment service providers.

1.2 Central Merchant Repository:

MyanmarPay's Central Merchant Repository serves as a centralized database, consolidating merchant information. This repository streamlines payment processes by providing a centralized source of merchant data, contributing to a smoother user experience during transactions.

1.3 Clearing and Settlement capability:

The Clearing and Settlement capability of MyanmarPay ensures prompt and secure settlement of financial transactions. This functionality contributes to the reliability of the payment switch by efficiently managing the clearing and settlement processes.

1.4 Dispute Settlement capabilities:

MyanmarPay's Dispute Settlement capabilities address conflicts and discrepancies in transactions. This feature promotes fair and efficient dispute resolution, contributing to user confidence in the reliability of the payment system.

1.5 QR Generation:

MyanmarPay supports Static QR Generation, allowing for the creation of Quick Response codes for transactions. This feature enhances the user experience by providing a standardized and convenient method for initiating payments.

1.6 QR Repository:

The QR Repository within MyanmarPay stores and manages Quick Response codes, ensuring easy retrieval and referencing. This functionality contributes to a standardized and organized approach to QR code usage in the digital payment ecosystem.

1.7 Certification of QR:

The system includes Certification of QR, ensuring the authenticity and compliance of generated QR codes. This feature adds an additional layer of security and reliability to QR-based transactions.

1.8 White Label Merchant/ Consumer Applications:

White Label Merchant/ Consumer Applications: MyanmarPay supports White Label Merchant and Consumer Applications, allowing technically unable Financial Institutions to customize and brand applications while leveraging the underlying infrastructure of the national digital payment switch. White Label Merchant/ Consumer Applications

2. Purpose

In alignment with global best practices and the vision to build a robust, secure, inclusive, and trust-based digital payment ecosystem, the MyanmarPay **Code of Conduct** serves as a cornerstone for responsible and ethical practices for banking and financial institutions operating within the Union of Myanmar. This document provides the guidelines that govern the activities of participants, ensuring transparency, security, and fairness for all stakeholders, including consumers, merchants, financial institutions, and regulatory bodies.
The purpose of this Code of Conduct is to ensure the smooth operation of MyanmarPay and clearly define the rights and obligations of stakeholders, along with prudential guidance for the MyanmarPay. By adhering to this Code, participants commit to:

2.1 Ensure Operational Sustainability and Security:

Establish and maintain an operationally sound, secure, and compliant digital payment switch.

2.2 Foster Trust and Transparency:

Build consumer and merchant trust through clear, consistent communication of fees, terms, and services.

2.3 Promote Digital Financial Inclusion

Support the transition from a cash-dominant society to a cashless economy, with a focus on underserved and unbanked populations.

2.4 Mitigate Risks:

Implement necessary safeguards, including anti-fraud measures, data protection, and compliance with AML and CFT regulations.

2.5 Enhance Consumer Experience:

Provide seamless, reliable, and secure digital payment services that cater to the evolving needs of consumers and businesses.

This Code applies to all participants within the MyanmarPay ecosystem, including banks, financial institutes, mobile financial service providers (MFSPs), merchant acquiring services, payment system operators, and merchants.

3. Definitions

For the purposes of this **Code of Conduct**, the following terms are defined as follows:

3.1 Definitions

Backbone Feature:
Refers to the core infrastructure that supports an open and interoperable payment acceptance ecosystem, including non-card payments, MMQR terminals, eCommerce for domestic payments, cross-border payments, and Real-Time Retail Payment (RTRP) systems.

Backbone Feature: MyanamarPay-Digital Payment Switch
The **MyanmarPay Digital payment switch** refers to the real-time electronic payment platform regulated by the **Central Bank of Myanmar (CBM)**, enabling transactions between individuals, merchants, businesses, and government agencies.

MyanmarPay-Digital payment switch Operator:
The **Digital payment switch Operator** is the entity appointed by the **Central Bank of Myanmar** to manage, operate, and maintain the technical and operational infrastructure of the **MyanmarPay Digital payment switch**. This operator is responsible for ensuring the secure and efficient processing of transactions, settlement and clearing, compliance with regulatory requirements, system integration for participants, fraud prevention, and dispute resolution. The operator also provides technical support and oversees system updates, ensuring that all participants in the payment system, including financial institutions, merchants, and consumers, can interact seamlessly within the ecosystem. **PayPlus Company Limited** currently serves as the designated **Digital payment switch Operator** for the **MyanmarPay** system.

Central Bank of Myanmar
The primary regulatory authority responsible for overseeing and governing the **MyanmarPay Digital payment switch** and ensuring compliance with the applicable laws and regulations within Myanmar.

Settlement Account:
An account held by participants with the **Central Bank of Myanmar** for settling transactions processed through the **MyanmarPay Digital payment switch**.

Bank Account
Refers to a savings or current account held by a customer at a licensed financial institution that is used for storing funds and making transactions.

E-Wallet:
A digital wallet that stores electronic money for use in making payments. E-wallets are typically offered by financial institutions, payment service providers, or mobile financial service providers.

Mobile Banking App:
A mobile application provided by a financial institution that allows customers to access their bank accounts and make transactions via the **MyanmarPay Digital Payment System**.

Calendar Days:
Refers to the total number of days in a given calendar, including weekends and public holidays, unless otherwise stated in the specific context of the system's operations.

Customers:
Individuals, businesses or merchants who are registered with participating banks or financial institutions to use the services provided by the **MyanmarPay Digital Payment System**.

Force Majeure
Refers to extraordinary events or circumstances beyond the reasonable control of the parties involved in the **MyanmarPay Digital Payment Switch** that prevent one or more parties from fulfilling their obligations under this **Code of Conduct**. Such events are typically unforeseeable and unavoidable and are not the result of any fault or negligence by the affected party. **Force Majeure** events may include, but are not limited to:

3.1.1. **Natural Disasters**: Acts of nature such as earthquakes, floods, hurricanes, tornadoes, tsunamis, volcanic eruptions, or other natural calamities that disrupt the ability of participants or the system operator to provide services.

3.1.2. **War and Armed Conflict**: Outbreaks of war (declared or undeclared), invasions, hostilities, civil wars, rebellions, insurrections, or military operations that compromise the normal operations of the payment system.

3.1.3. **Civil Unrest**: Riots, civil disturbances, widespread strikes, protests, lockouts, or labour disputes that significantly disrupt business continuity and prevent normal operations.

3.1.4. **Governmental Actions**: Any legal or regulatory changes, sanctions, orders, or actions taken by local or international governments, including expropriation, confiscation, requisition, or imposition of laws that affect the operations of the **MyanmarPay Digital Payment Switch** or its participants.

3.1.5. **Terrorism and Sabotage**: Acts of terrorism, sabotage, or other criminal activities aimed at causing destruction or disrupting the operations of the payment system.

3.1.6. **Pandemics and Epidemics**: Widespread outbreaks of contagious diseases, pandemics, or government-imposed quarantines and health-related restrictions that affect the ability of participants or the operator to meet their obligations.

3.1.7. **Cyber Attacks**: Large-scale cyber-attacks, hacking incidents, malware, or other cybercrimes that severely disrupt or compromise the integrity and security of the **MyanmarPay Digital Payment System**.

3.1.8. **Infrastructure Failures**: Major failures in public infrastructure, including power outages, telecommunications breakdowns, or transport disruptions, which prevent the normal operation of the payment system or its participants.

3.2 Participants:

Any institution authorized by the **Central Bank of Myanmar** to participate in the **MyanmarPay Digital Payment System**, including banks, financial institutes, mobile financial service providers (MFSPs), merchant acquiring services, payment system operators, and merchants.

3.3 Market Discount Rate

Merchant discount rate is a fee charged to a merchant which include issuing fees, acquiring fees and processing fees that a merchant and/or customer is charged by the RI/OI or system operator for accepting payments by **MyanmarPay Digital Payment System.**

3.4 RTRP (Real-Time Retail Payment):

A system within the **MyanmarPay Digital Payment Switch** that enables real-time, low-value transactions between individuals, businesses, and government entities.

3.5 P2P (Person-to-Person):

P2P (Person-to-Person): Refers to payments made between individuals for personal or non-business purposes. These transactions are typically low in value and processed in real-time through the system.

3.6 P2M (Person-to-Merchant):

Payments made by an individual to a merchant in exchange for goods or services. These transactions form the backbone of the retail payment system within **MyanmarPay**.

3.7 P2G (Person-to-Government):

Payments made by individuals to government agencies for services such as taxes, fines, or public utilities. These transactions may be facilitated through the **MyanmarPay Digital Payment System**.

3.8 B2G (Business-to-Government):

B2G (Business-to-Government): Payments made by businesses to government agencies. Examples include tax payments, regulatory fees, and other business-related charges.

3.9 TPS (Transactions Per Second):

A metric used to measure the processing speed of the **MyanmarPay Digital Payment System**, indicating the number of transactions that can be completed within one second.

3.10 On-Us Transaction

On-Us Transactions: Transactions in which both the issuing and acquiring institutions belong to the same entity, resulting in faster processing times and potentially lower fees for the merchant.

3.11 Off-Us Transaction

Off-Us Transactions: Transactions in which the issuing and acquiring institutions are different, requiring the involvement of external networks for processing and settlement.

3.12 Anti-Money Laundering (AML):

Anti-Money Laundering (AML): A set of policies, procedures, and regulations designed to prevent the laundering of money obtained through illegal activities. Participants in the **MyanmarPay Digital Payment Switch** must comply with AML requirements as enforced by the **Central Bank of Myanmar**.

3.13 Combating the Financing of Terrorism (CFT):

Combating the Financing of Terrorism (CFT): A regulatory framework that seeks to prevent the funding of terrorist activities. Participants must follow CFT protocols as part of their compliance with local and international regulations.

3.14 Know-Your-Customer (KYC):

Know-Your-Customer (KYC): A process by which financial institutions verify the identity of their customers before allowing them to use services. KYC ensures that customers meet legal requirements and helps prevent fraud and money laundering.

3.15 Fraud Management:

A set of strategies, technologies, and procedures used by participants to detect, prevent, and respond to fraudulent activities within the **MyanmarPay Digital Payment System**.

3.16 Blacklist Screening:

The process of checking customers and transactions against national blacklists to ensure compliance with laws prohibiting transactions involving sanctioned entities or individuals.

3.17 Dispute Management

The formal process for resolving conflicts between participants, or between participants and their customers, related to the operation of the **Myanmar Pay Digital Payment System**.

3.18 RI

RI: The RI, or Receiving Institute, is the financial institution that receives the funds on behalf of the payee. In a QR payment scenario, this is typically the bank or payment service provider where the payee (such as a merchant) has their account. When a customer makes a payment using a QR code, the funds are transferred to the RI, which then credits the payee's account accordingly.

3.19 OI

OI: The OI, or Originating Institute, is financial institution that initiates the transaction on behalf of the payer. This is usually the bank or payment service provider where the payer (such as a customer) has their account. The OI debits the payer's account when a payment is made using a QR code and facilitates the transfer of funds to the RI.

3.20 Centralized Merchant Repository:

A database maintained within the **MyanmarPay Digital Payment Switch** that stores merchant information, allowing for efficient onboarding, verification, and transaction processing.

3.21 System Integration Testing (SIT):

The testing phase where a participant's system is integrated into the **MyanmarPay Digital Payment Switch** to ensure technical compatibility, functionality, and security.

3.22 User Acceptance Testing (UAT):

A phase of testing where the participant confirms that the integrated system meets their operational and business requirements before going live.

4. Participant Onboarding

The **MyanmarPay** welcomes eligible financial institutions, mobile financial service providers, and merchant acquirers to join the ecosystem. The onboarding process is designed to ensure that all participants meet the necessary technical, operational, and compliance standards.

4.1 Eligibility Requirements

Eligible institutions include:

4.1.1. **Direct Participants**: Licensed commercial banks, payment service providers, and mobile financial service providers authorized by the Central Bank of Myanmar.

4.1.2. **Indirect Participants**: Government agencies and regional financial services can participate in MyanmarPay with approval from the Central Bank of Myanmar. Their participation aligns with Myanmar's National Payment Strategy, emphasizing the digitalization of government bill payments and fostering efficient, nationwide digital payment solutions.

4.2 Application Process

Participants must follow the four-step onboarding process:

4.2.1 **Application Submission**: Submit an official request to the Central Bank of Myanmar, along with supporting documentation, including business plans, KYC policies, project plan, and technical readiness reports. Please note that the FI's system for the security standards should be in accord with section (6.10) Security Mechanism, and the network requirements should align with the network readiness documents issued by the Digital Payment Switch operator. FIs should ensure that the system will be ready for Cross-border QR payment; if any changes are needed for cross-border functionality, they must adjust accordingly. The KYC process must comply with at least Level 2 verification standards to ensure compatibility with the eID system for identity authentication and validation for cross-border transactions.

4.2.2 **Approval in Principle**: Upon initial review, participants may receive an **Approval in Principle** letter, allowing them to proceed with system integration and compliance testing.

4.2.3 **System Integration and Testing**: Participants must integrate their systems with **MyanmarPay** and undergo the required testing and certification process. A project plan detailing the timeline and resources must be submitted for approval.

4.2.4 **Go Live**: After successful testing and certification, participants must launch their services within two months. Participants who fail to launch within this period will be required to recertify and may incur additional charges.

The specifics of this onboarding process are detailed in the Onboarding Standard Operating Procedure (SOP), which is incorporated herein by reference.

4.3 Qualification of Participation

A Participant must satisfy all of the conditions set out below:

4.3.1 Execute, undertake and agree to be irrevocably bound by the terms and conditions of the Agreement for Participating in this Code of Conduct;

4.3.2 The Participant must hold, and must have done all things required to hold, every registration, license, permit, authorization or approval required in connection with its business from each regulatory body having jurisdiction over the Participant; and

4.3.3 The Participant and each of its partners, directors and officers must be in compliance with all applicable regulations, Guidelines, orders or directions of each regulatory body having jurisdiction over the Participant, including such minimum capital requirements and financial stability standards as are applicable to the Participant.

5 Centralized Merchant Repository (Repo)

The Centralized Merchant Repository (Repo) is a critical component of the MyanmarPay, designed to streamline the onboarding, verification, and management of merchants. This repository acts as a centralized database containing detailed information about all registered merchants within the MyanmarPay ecosystem. The Centralized Merchant Repo enables real-time updates, efficient merchant categorization, and compliance monitoring across the system.

5.1 Centralized Merchant Onboarding Process

The Centralized Merchant Repository ensures the orderly and transparent onboarding of merchants by participating institutions. The onboarding process involves the following key steps:

5.2 Merchant Application

5.2.1 Merchants submit applications through their Receiving Institution (RI) to

5.2.2 participate in the **MyanmarPay**. Applications must include essential business information such as legal business name, registration details, tax identification, product or service offerings, and contact information.

5.2.3 The RI is responsible for submitting the detailed merchant onboarding format and procedures to the Central Bank of Myanmar for review before integration with the Centralized Merchant Repo.

5.3 Due Diligence:

5.3.1 The Receiving Institution (RI) conducts due diligence to assess the risk of onboarding the merchant. This may include background checks, financial assessments, and compliance checks to ensure the merchant meets all regulatory and operational requirements.

5.3.2 The RI must submit its due diligence procedures to the Central Bank of Myanmar for approval before integrating the merchant into the Centralized Merchant Repo.

5.4 System Integration and Testing

5.4.1 Once due diligence is successfully completed, the RI and the merchant enter into a formal Merchant Services Agreement. This agreement outlines the terms of participation, including the Merchant Discount Rate (MDR), transaction fees, and the responsibilities of both parties.

5.4.2 The template for the agreement must be submitted to the Central Bank of Myanmar for review before merchant onboarding.

5.4.3 System Integration and Testing:
The RI must ensure that their system is integrated with the MyanmarPay's APIs and undergoes thorough testing to ensure smooth processing of payments and merchant onboarding.

5.4.4 The Central Bank of Myanmar and the system operator, PayPlus Company Limited, will oversee this integration and testing process to ensure compliance.

5.5.5 The Receiving Institution (RI) shall be required to submit CBM the following documentation for review and approval: (1) a comprehensive merchant onboarding plan and process, (2) details of merchant support channels, (3) a standard template of the merchant contract, and (4) a projection of the number of merchants it intends to acquire within the first year. The Central Bank of Myanmar (CBM) reserves the

right to assess and determine the adequacy of these submissions and may issue directives should any adjustments be deemed necessary.

5.5 Go-Live

After successful onboarding, testing, and certification, the merchant can begin accepting payments through the MyanmarPay. All payments must be processed through the RI's system and adhere to the terms outlined in the Merchant Services Agreement.

5.6 Merchant Onboarding Limits:

A merchant can only be associated with one bank, one mobile financial services provider (MFSP), and one acquirer institution. Violating this rule may result in merchant deactivation or sanctions.

5.7 Merchant Change of RI:

In case of Merchants changing RIs, Following procedure and business rules applies:

5.7.1 Change request

5.7.2 The New RI submits a formal change request to MyanmarPay, specifying the merchant wishing to change RI.

5.7.3 The request must be submitted through the official channels designated by MyanmarPay, accompanied by the required documents (e.g., business registration, identification, proof of address, etc.).

5.7.4 The new RI conducts its own due diligence on the merchant to ensure compliance with its policies and requirements set forth by CBM.

5.7.5 Acknowledgment and Preliminary Review:
The MyanmarPay acknowledges receipt of the change request within one working day and inform to the old RI.

5.7.6 Notification the acceptance to the New RI:

5.7.6.1 Condition 1 - If the preliminary review is unsuccessful, the old RI has three (3) business days to appeal. If the merchant agrees to remain with the old RI within this period, no change will occur, and the MyanmarPay will require proof of the merchant's communication.

5.7.6.2 Condition 2- If there is no appeal within 3 working days, MyanmarPay will make accept change request from new RI.

5.7.6.3 Condition 3 -Upon successful preliminary review of merchant's intention to change, the current RI notifies MyanmarPay and MyanmarPay notifies the new RI about the merchant's intention to switch.

5.7.7 Onboarding by the New RI:
On condition 2 and 3, the new RI communicates to the merchant about approval and start onboarding on MyanmarPay centralized merchant repository within 3 working days of change request accept.

5.7.8 Approval and Transition Period:
Once the new RI initiates the onboarding process, it must establish transaction capabilities with the merchant and send the merchant's QR code within five (5) working days after receiving approval.

5.7.9 Finalization of Transfer:
The current RI ensures that any customer transactions or payments are processed without disruption until the effective transfer date.

5.7.10 Cooling Period:
If a merchant changes their RI more than once, starting from the second change, they will be required to wait a 30-calendar-day cooling period.

5.8 Inactive Merchant IDs:

In case Merchant IDs issued has no transaction whatsoever for 180 days, the DPS will inform the responsible RI to communicate this transparently with the merchants.

5.9 Ongoing Compliance Merchant IDs:

RIs must provide ongoing support to merchants for any technical or operational issues related to the MyanmarPay. This includes updating merchant records, providing customer service, and ensuring continued compliance with system guidelines.

5.10 Merchant Categorization

Central Bank of Myanmar reserve the rights to revise the MDR and Merchant categories from time to time based on the following conditions:

5.10.1 Economic and Market Dynamics: The financial and economic landscape is subject to change over time. Factors such as inflation, technological advancements, changes in consumer behaviour, and market competition can all impact the costs and dynamics of payment processing. Allowing for revisions in the MDR enables the central bank to adapt to these changes.

5.10.2 Regulatory Oversight: Regulatory authorities, including central banks, have the ability to respond to evolving financial regulations and standards. CBM need the flexibility to adjust MDR and merchant categories to align with updated or newly introduced regulations.

5.10.3 Industry Innovation: The payments industry is marked by rapid innovation and the emergence of new payment methods and technologies. These innovations may require adjustments in MDR structures and merchant categorization to promote fair pricing and competition.

5.10.4 Merchant Dynamics: The nature and scale of businesses can evolve over time. New types of merchants may emerge, and existing businesses may change their operations Revising merchant

categories ensures that the MDR structure accurately reflects the diverse landscape of merchants.

5.10.5 Cost Management: Central Bank of Myanmar often aim to strike a balance between ensuring fair pricing for merchants and promoting the sustainability of payment systems. The ability to revise MDR allows CBM to manage costs effectively while maintaining the stability of payment infrastructure.

Upon successful onboarding, each merchant must be categorized according to the appropriate Merchant Category Code (MCC). This categorization is essential for determining the correct MDR and interchange rates. The following rules apply:

5.10.6 **MCC Code Assignment**: The Receiving Institution (RI) must assign an appropriate MCC code based on the merchant's business activities. Failure to properly categorize a merchant may result in penalties imposed by the **Central Bank of Myanmar**.

5.10.7 **MDR and Merchant Categories**: The **Central Bank of Myanmar** reserves the right to periodically revise MDR and merchant categories based on economic conditions, market dynamics, and regulatory changes. Adjustments may be made to reflect advancements in technology, payment methods, and market needs.

5.11 Merchant Data Management:

5.11.1 **Data Storage**:
Merchant data must be securely stored in the **Centralized Merchant Repository** for a minimum of five (5) years, even after the termination of the merchant's account. Transactional data must be stored in the system for the same period.

5.11.2 **Merchant Data Security**:
The Receiving Institution (RI) is responsible for ensuring that all merchant-related data is securely managed and protected against unauthorized access. This includes ensuring that merchant funds are not diverted to unauthorized accounts.

5.11.3 **Regular Data Updates**:
The RI must ensure that merchant data in the **Centralized Merchant Repository** is regularly updated to reflect changes in business operations, contact information, or legal status. Failure to maintain accurate data may result in system penalties.

5.12 Merchant Reporting and Settlement

5.12.1 **Real-Time Settlement**:
The **MyanmarPay Digital Payment Switch** ensures real-time settlement of transactions, with funds credited to merchants' accounts immediately. Any delays or discrepancies must be reported to the **Central Bank of Myanmar** within one business day.

5.12.2 **Reporting**:
The RI is responsible for submitting monthly and quarterly reports to the **Central Bank of Myanmar**, detailing the number of onboarded

merchants, transaction volumes, and any service disruptions or compliance issues.

5.12.3 **Merchant Promotions and Incentives**:
In cases where the **Central Bank of Myanmar** or MyanmarPay initiates promotional campaigns (e.g.,cashback or other incentives), the RI must manage the distribution of incentives to merchants and ensure accurate reconciliation with the RI and MyanmarPay system.

5.13 Merchant Risk Management

5.13.1 **Ongoing Monitoring**:
The RI must continuously monitor merchant transactions for any signs of fraud or suspicious activity. This includes tracking high-risk transactions, monitoring unusual patterns, and ensuring compliance with **AML/CFT** regulations.

5.13.2 **Risk Categorization**:
Merchants are classified into different risk tiers based on their transaction history, business category, and compliance record. High-risk merchants may be subject to additional scrutiny or higher MDR rates.

5.13.3 **Data Protection and Privacy**:
All merchant data, including transactional information, must be protected under stringent data protection protocols. The RI is responsible for ensuring that merchant data is encrypted and that access is restricted to authorized personnel only.

6 Security and Compliance

6.1 Security Mechanisms

To ensure the safety, reliability, and operational integrity of the MyanmarPay Digital Payment System, all participants must implement comprehensive security controls, adhering to both national and international security standards. Participants are required to:

6.1.1 **Data Encryption**: All sensitive data, including transaction and customer information, must be encrypted during transmission and at rest to ensure data integrity and confidentiality.

6.1.2 **Vulnerability and Patch Management**: Participants are required to conduct regular vulnerability assessments and deploy patches for any identified security flaws in a timely manner. A formal vulnerability management plan should be in place, with a focus on proactively identifying and addressing system weaknesses.

6.1.3 **Access Control**: Implement strict access control mechanisms that limit data access to authorized personnel based on the principles of "need to know" and "right to know."

6.1.4 **Fraud Detection and Prevention**: Develop real-time fraud detection systems that utilize advanced analytics and data analysis techniques to monitor transaction patterns and identify suspicious activity.

6.1.5 **Disaster Recovery**: Establish and regularly test disaster recovery plans to ensure business continuity in the event of cyberattacks, system failures, or natural disasters. Plans must include robust backup systems and recovery procedures.

6.2 Consumer Data Protection

Protecting consumer data is paramount to maintaining trust in the digital payment system. All participants must:

6.2.1 **Sets terms and conditions on MyanmarPay** - Digital Payment Switch service usage including stakeholders' responsibilities.

6.2.2 **Provides and explains terms and conditions on MyanmarPay** - Digital Payment Switch service usage to their customers.

6.2.3 **Notifies their customers if there is any amendment to the terms and conditions on MyanmarPay** - Digital Payment Switch service usage at least fifteen (15) business days before the amendments become effective.

6.2.4 **Consumer Consent**: Obtain explicit consent from consumers before collecting, storing, or processing personal information. Consumers must also be informed of their rights to access, correct, or delete their data.

6.2.5 **Data Security Policies**: Implement strong and healthy data security policies that cover encryption, access control, and secure storage. These policies must be communicated to all employees and updated regularly.

6.2.6 **Third-Party Risk Management**: Ensure that any third-party service providers handling consumer data are compliant with this Code of Conduct and adhere to the same data protection standards.

6.2.7 **Incident Response**: In the event of a data breach, participants must notify the Central Bank of Myanmar and affected consumers within three business days, detailing the nature of the breach and the steps being taken to mitigate its effects.

7 Dispute Management

To ensure transparency and fairness in resolving disputes arising from the use of the **MyanmarPay Digital Payment System**, participants must adhere to the following dispute management guidelines. Disputes can arise from consumer transactions, technical issues, compliance violations, or fraud. Effective and timely dispute resolution is critical to maintaining trust within the ecosystem.

7.1 Dispute Escalation and Categories

Dispute escalation follows a tiered approach to ensure prompt resolution. Disputes are categorized into the following types:

7.1.1 **Transaction-Related Disputes**: These involve discrepancies or issues with financial transactions, such as unauthorized charges, incorrect amounts, or billing errors.

7.1.2 **Technical Disputes**: Issues arising from system errors, such as transaction failures, duplication of transactions, or system outages that prevent transaction completion.

7.1.3 **Fraud-Related Disputes**: These include unauthorized transactions, fraudulent behavior, or instances of identity theft that affect the security of the payment system.

7.1.4 **Compliance-Related Disputes**: These involve violations of AML/CFT laws, breaches of the Code of Conduct, or failure to adhere to participant agreements and regulatory requirements the ecosystem.

7.2 Dispute Resolution Process

7.2.1 **Level 1 - Step -1: Originated Institution**: Disputes may first be raised by the Originated Institution (OI) to MyanmarPay dispute team to help investigate it.

Level 1 – Step -2: MyanmarPay dispute team investigation: The MyanmarPay Disputes Team will investigate the dispute and forward it to the Receiving Institution (RI)

Level 1- Step -3: Receiving Institution: The Receiving Institution will investigate and decide to accept or reject the dispute.

7.2.2 **Level 2 – Arbitration Committee:** In case the dispute remains unresolved at level- 1, the matter may be escalated to Arbitration committee for final decision. The Arbitration Committee will include representatives from Central Bank of Myanmar, MyanmarPay Dispute team, Receiving Institution (RI), and Originated Institution (OI), with an equal number of representatives from both RI and OI.

7.3 Dispute Management Team

Participants are required to have dedicated dispute management teams to work in tandem with the **MyanmarPay Dispute Handling Team**. Dispute handling teams must ensure the timely and transparent handling of disputes between customers and institutions. The MyanmarPay team is responsible for managing disputes between participants and overseeing the escalation process.

7.4 Reporting and Documentation

All disputes must be logged and reported in a dedicated system for auditing and compliance purposes. Participants are required to maintain detailed records of all disputes and their resolutions for a minimum of five years. These records will be reviewed during regular audits by the Central Bank of Myanmar and submit monthly report to CBM.

7.5 Dispute Resolution Timelines

7.5.1 Maximum timeframe for a customer to file a dispute and Originated Institute (OI) investigation timeframe: 30 working days after the transaction is made.

7.5.2 MyanmarPay dispute team checks in the system and forwarding to Receiving Institute (RI): 5 working days

7.5.3 Receiving Institute (RI) and Merchant response timeframe: 20 working days

7.5.4 Level 2 Arbitration: Originated Institute (OI) must escalate to the committee within 10 days of Receiving Institute (RI) rejection. If 10 days pass, it is considered that the Receiving Institute (RI) rejection of the dispute is accepted.

7.5.5 Committee Decision Timeframe: The committee, upon receiving the Originated Institute (OI) submission of disputes, will take 30 working days to decide.

The working days referenced exclude both weekends and official Myanmar government holidays.

7.6 Dispute Resolution

Followings are recommended steps for resolving a dispute related to digital payment switch transactions:

7.6.1 Resolution Proposal and Notification: Digital Payment Switch operator can help investigate the dispute, and upon completion of the investigation process, a resolution proposal is to be prepared by participants for those disputes that are out of ordinary. This proposal may include recommendations for actions to resolve the dispute, such as refunds, adjustments, or corrective measures. The participant responsible for proposing the resolution will notify all relevant parties.

7.6.2 Acknowledgment and Acceptance: The OI or RI (the other party) should acknowledge receipt of the resolution proposal. If they accept the proposed resolution, the dispute is considered resolved, and the agreed-upon actions should be promptly executed. This may involve reversing unauthorized charges, processing refunds, or making necessary adjustments to accounts or records.

7.6.3 Reconciliation: In cases where financial adjustments are required, the OI, RI, and the Digital Payment Switch Operator should reconcile their financial records to ensure that the agreed-upon resolution is accurately reflected in their systems. This step is crucial for ensuring that financial discrepancies are corrected.

7.6.4 Dispute Closure: After the proposed resolution has been executed, and both parties are satisfied with the outcome, the dispute is considered closed. The investigation team from Digital Payment Operator's designated personnel will also document the closure of the dispute, including the resolution details and acceptance by the parties involved.

7.6.5 Appeals Process: If the OI or RI is dissatisfied with the proposed resolution or believes that it was not handled fairly during the initial

investigation, they may have the option to initiate an appeals process. This process may involve a secondary review by a neutral third party or an appeals committee. The findings and decisions of the appeals process should be communicated to all parties involved. The final decision will sit with Central Bank of Myanmar.

7.6.6 Documentation and Record-Keeping: Throughout the dispute resolution process, it is essential to maintain detailed records of the steps taken, communication, findings, resolutions, and any actions or adjustments made. This documentation is valuable for audit purposes and may be required for regulatory compliance.

7.6.7 Compliance with Regulatory Requirements: Ensure that all actions taken during the dispute resolution process are in compliance with relevant legal and regulatory requirements. This includes data protection, consumer rights, and any specific industry or payment network regulations.

7.6.8 Continuous Improvement: After resolving a dispute, consider conducting a post resolution review to identify any process improvements that can prevent similar issues in the future. This may involve revising internal procedures, enhancing security measures, or providing additional training to staff members.

7.6.9 Customer Communication: Throughout the dispute resolution process, clear and timely communication with customers is vital. Customers should be informed about the progress, outcome, and any actions taken to resolve their disputes.

7.7 Dispute Cost

Responsibility for Bearing Dispute Resolution Costs - Clarity regarding the allocation of costs associated with dispute resolution is essential to ensure fairness and efficiency in the process. The following defines

7.7.1 Originator's Responsibility - The Originator who initiates the dispute generally bears the initial costs (if any) filing a dispute.

7.7.2 Investigation Costs- Both the participants and MyanmarPay - Digital Payment Switch Operator's bear their respective cost for investigation including the expenses related to assigning personnel, gathering information, and conducting the necessary analysis.

7.7.3 Shared cost: In certain cases, where the investigation reveals errors or negligence on the part of both OI or RI, a portion of the investigation and/or appeal costs may be shared between the OI and RI, as deemed appropriate by the Arbitration Committee.

7.7.4 Appeals Process Costs:

7.7.4.1 Appellant's Responsibility: If an appeal is initiated by one of the parties (e.g., OI or RI), that party is typically responsible for covering the costs associated with the appeals process. This includes any fees related to the submission of an appeal and the expenses of presenting their case.

7.7.4.2 Appeals Authority's Costs: The expenses related to the appeals process, such as the fees of the appeals authority or third-party mediator, are generally covered by the appealing party. However, in some cases, these costs may be shared among RI and OI. The decision will be settled by CBM.

7.7.4.3 Legal and Regulatory Compliance: All cost-sharing arrangements must comply with the legal and regulatory requirements of the relevant jurisdictions.

7.7.5 Arbitration Fees for disputes going through Arbitration will incur a fee of 300,000 MMK per case. The losing party, either OI or RI, will bear the cost after the final decision.

7.7.6 Resolution Costs: The network fees of the resolution in refunds will be borne by OI side as stated in the refund commercial agreement. Any other adjustments, or financial remediation if any, are typically shared or borne by the party responsible for the resolution.

7.7.7 Transparency and Clarity Cost Allocation: The allocation of costs should be transparent and communicated clearly to all parties involved. This ensures that each party understands its financial responsibilities throughout the dispute resolution process.

7.7.8 Review and Revision: The allocation of costs can be reviewed and revised periodically by Arbitration Committee to ensure that it remains fair and equitable for all parties involved

8 Technical Requirements

To ensure seamless integration with the **MyanmarPay Digital Payment System**, participants are required to comply with the following technical and operational standards. This will ensure interoperability, security, and efficiency across the ecosystem.

8.1 System Integration

Participants are required to comply their systems with **MyanmarPay** by adhering to the technical specifications provided by the **Central Bank of Myanmar**. Integration includes:

8.1.1 MMQR Standardization: Participants must comply with the **MyanmarPay QR Code** standard issued by Central Bank of Myanmar for all point-of-sale (POS) transactions. This ensures a uniform and secure QR code system across all merchants and financial institutions.

8.1.2 API Integration: All participants must integrate their systems using secure Application Programming Interfaces (APIs) provided by the MyanmarPay operator in the API set of documents. These APIs support transaction processing, merchant registration, and fraud management.

8.1.3 Real-Time Settlement: Participants must ensure that all transactions, including cross-border payments, are settled in real-time. The system must be capable of handling peak transaction volumes and scaling in line with network demands.

8.2 Data Security and Encryption

8.2.1 **Encryption**: All transaction data must be encrypted in transit and at rest, ensuring compliance with global data security standards (e.g., PCI-DSS).

8.2.2 **Data Storage**: Participants must store transaction and consumer data in secure environments that comply with local data protection laws. Data retention policies must ensure that records are maintained for at least five years.

8.3 Testing and Certification

8.3.1 **Technical Testing**: Prior to going live, all participants must undergo extensive testing, including System Integration Testing (SIT) and User Acceptance Testing (UAT), according to SIT sign off criteria and UAT sign off criteria set up by MyanmarPay Operator, to ensure operational readiness. The **MyanmarPay Operator** will oversee the testing process and certify systems based on their performance.

8.3.2 **Certification**: Once testing is successfully completed, participants must receive formal certification from the **Central Bank of Myanmar** to operate within the **MyanmarPay Digital Payment System** in accord with QR certification and Application certification guideline issued by MyanmarPay operator.

8.4 Branding Requirements

Participants must adhere to the **MyanmarPay Branding Guidelines** detailed below to ensure proper integration with the MyanmarPay Digital Payment System:

8.4.1 MyanmarPay Brand Guidelines
8.4.2 MyanmarPay QR Stand Printing Guidelines
8.4.3 MyanmarPay QR Stand Digital Guidelines

8.5 Operation Readiness

In order to integrate into Digital Payment System, the Applicant Financial Institutions are required to submit the following operational related information:

8.5.1 Organizational structure of Digital Payment Switch Operation Team
8.5.2 A comprehensive outline of the training programs designed for the Operation Team.
8.5.3 A procedure for managing customer complaints within the Digital Payment Switch Operation Team.
8.5.4 A guideline detailing the allocation of Responsibilities, Authority, and Accountability within Digital Payment Switch team.

8.6 Testing Environment Support

8.6.1 Existing Participants are required to establish and maintain a System Integration Testing (SIT) environment upon request from the MyanmarPay Digital Payment Switch Operator. This is necessary to facilitate system updates, upgrades, and participant onboarding.

8.6.2 The MyanmarPay Digital Payment Switch Operator shall provide Existing Participants with a formal SIT environment request at least three (3) working days in advance.

8.6.3 The MyanmarPay Digital Payment Switch Operator is also responsible for providing a SIT environment in collaboration with the participants during testing activities.

8.6.4 Existing Participants must set up and operate SIT environments as per their designated roles, whether as Receiving Institutions (RI), Originating Institutions (OI), or both, based on their participation in the system.

9 Termination and Suspension of Participants

9.1 Right to Terminate

9.1 The **Central Bank of Myanmar** reserves the right to terminate or suspend participants in the following cases:

9.1.1 **Voluntary Termination**: Participants may request termination by submitting a formal request with proper reasoning. All outstanding obligations must be settled before termination.

9.1.2 **Regulatory Breaches**: The Central Bank may suspend or terminate participants found in violation of the **Code of Conduct**, security guidelines, or AML/CFT requirements.

9.1.3 **Non-Performance**: Participants that fail to meet technical or operational standards, or fail to fulfil financial obligation or who cause significant disruptions to the system, may face suspension until the issues are resolved.

9.2 Central Bank terminates the participants with prior notice, participants are obligated to publicly notify their customers and any related parties, settle related MyanmarPay transactions, and resolve any disputes within a time period specified by the Central Bank of Myanmar.

9.3 On condition that participants fail to fulfil the above mentioned obligations within given time period, or the Central Bank of Myanmar terminates the participant with prior notice, the CBM shall proceed as follows:

9.3.1 Settle the balances in the participant's settlement accounts to terminate their rights and obligations toward other participants

9.3.2 Notify the participant's customers and merchants that they will no longer be operating with MyanmarPay and instruct them to transition to another participant, using the participant's system and/or communication channels

9.3.3 MyanmarPay team reserves the right to disclose merchant information to other participants for potential future engagement. Interested parties will be onboarded through another participant.

9.3.4 Digital payment switch operator will take 3 working hours from the receipt of suspension notice from the CBM.

9.4 The CBM may exclude any Participant provisionally or permanently from the MyanmarPay System. Immediately upon the suspension of a Participant, the

CBM shall restrict the right and ability of the Participant to use all system functionality. Such restriction may be lifted in whole or in part by the CBM in its discretion as may be required to complete an orderly discharge of the Participant, its obligations within the MyanmarPay system.

9.5 The CBM may suspend a Participant if it determines, in good faith that the Participant is in such financial or operating condition that its continuation as a Participant would cause material disruption to the services or would jeopardize the interests of the MyanmarPay system or other Participants.

9.6 Appeal of Suspension - A Participant who is suspended by the CBM pursuant to this section: 10.4 and 10.5 above may appeal the suspension. The CBM shall convene a meeting to give the Participant an opportunity, within ten (10) working days after the effective date of the suspension, to make representations on its behalf. At its option, the Participant may also be represented by counsel. The CBM, its decision to accept or deny the appeal may take from one week to one month, depending on the time needed for a thorough review of the case and the seriousness of the case itself.

9.7 Reinstatement: A Participant who has withdrawn or been terminated may later request reinstatement by doing the following:

- 9.7.1 Meet the standards and qualification criteria for participation;
- 9.7.2 Submit a written request to the CBM for reinstatement;
- 9.7.3 Pay any entrance or reinstatement fee determined by the CBM; and
- 9.7.4 Demonstrate to the satisfaction of the CBM that it has discharged all of its liabilities and indebtedness to the MyanmarPay System and the other Participants arising from its prior use of the system.
- 9.7.5 The CBM may in its sole discretion approve or reject a request for reinstatement. If approved, the CBM shall promptly inform the relevant regulatory authority and all other Participants of the reinstatement and of the effective date.

9.8 Liability: The CBM shall not incur any liability to any Participant, including the suspended or terminated Participant, as a result of any action taken in good faith in the exercise of any power or the discharge of any function or duty provided for in these Guidelines. The CBM shall not be liable for any loss, damage, cost, expense or claim suffered or incurred by any Participant, arising from the suspension of a Participant or the termination of an entity's designation as a Participant, or the exercise by the CBM of its discretion whether to suspend or take such action against a Participant, including any indirect or consequential loss, expense, liability or claim. Each Participant irrevocably releases the CBM from any such liability.

10 Risk Management Mechanisms

To ensure the stability and security of the MyanmarPay Digital Payment System, all participants must adopt a comprehensive risk management framework. This framework should encompass fraud prevention, data security, operational risk management, and business continuity planning. Financial institutions are required to adhere to the Technology Risk Management Guidelines (TRMG) that will be issued by the Central Bank of Myanmar.

10.1 Fraud and Risk Management

Fraud prevention is a key component of ensuring the integrity of the **MyanmarPay Digital Payment System**. Participants are required to implement fraud management solutions that leverage real-time transaction monitoring, machine learning, and rule-based algorithms to detect suspicious activities. Key fraud management measures include:

10.1.1 **Transaction Monitoring**: Participants must continuously monitor transactions to detect unusual patterns or suspicious activities. This includes monitoring for anomalies such as unusually high transaction volumes, transactions from high-risk regions, and behaviour inconsistent with the customer's typical activity.

10.1.2 **Velocity Checks**: Implement velocity checks to detect multiple rapid transactions from a single account or user, which may indicate fraudulent behavior.

10.1.3 **Geographical Restriction**: Participants should define geographical restrictions to identify transactions that originate from high-risk regions or countries in case of cross border transactions. Transactions from these regions may require additional verification or scrutiny to mitigate the risk of fraud.

10.1.4 **Usage Patterns:** Analyzing usage patterns can help identify suspicious activities.
Participants should monitor for unusual spending patterns, such as multiple transactions on the same consumer account within a short time frame or transactions that deviate significantly from the that particular consumer typical spending behaviour.

10.1.5 **Anomalous Behavior:** Participants should establish rules to detect anomalous behavior, such as a sudden change in transaction volume, transaction types, or transaction locations. These rules can help identify activities that deviate from normal customer behaviour and may be indicative of fraudulent actions.

10.1.6 **Blacklist Management:** Maintaining a blacklist of known fraudulent users and blocking transactions associated with these users is an effective way to prevent fraud. Transactions associated with blacklisted entities must be automatically blocked or flagged for further review. Participants should regularly update the blacklist to stay up to date with the latest fraud trends.

10.1.7 **Device Fingerprinting:** Device fingerprinting techniques can be used to identify suspicious devices or IPs associated with fraudulent activities. Participants should implement rules to detect devices that have been flagged for previous fraudulent behaviour.

10.1.8 **Unusual Timing:** Monitoring transactions that occur during unusual hours or outside of regular customer patterns can help identify potential fraud. For example, transactions made at odd hours or transactions that occur simultaneously from different locations may warrant further investigation.

10.1.9 **High-Risk Transaction Types:** Certain transaction types, such as cash advances, balance transfers, or international transactions, are often associated with higher fraud risks. Participants should implement additional scrutiny and verification processes for these transaction types.

10.2 AML/CFT

To ensure compliance with Anti-Money Laundering (AML) and Combating the Financing of Terrorism (CFT) laws and regulations, participants in the MyanmarPay Digital Payment System must adhere to several key obligations. These include establishing effective internal controls, defining and implementing Know-Your-Customer (KYC) and Customer Due Diligence (CDD) measures, monitoring transactions for suspicious activity, and promptly reporting such activities to the Central Bank of Myanmar. Financial Institutions are responsible for implementing comprehensive end-to-end monitoring and control of Anti-Money Laundering (AML) and Countering the Financing of Terrorism (CFT) measures, encompassing every stage of the transaction process—from consumers initiating transactions, to merchants processing payments, and vendors facilitating services. This responsibility includes the oversight of all parties involved in the payment chain, ensuring compliance with AML/CFT regulations and mitigating potential risks at each point of interaction.

10.3 Incident Response and Reporting

In the event of a security breach or fraud incident, participants are required to follow a formal incident response plan. This plan must include the following steps:

10.3.1 **Immediate Containment**: Upon detecting an incident, participants must take immediate steps to contain and mitigate the impact of the breach.

10.3.2 **Notification to Authorities**: Participants must notify the **Central Bank of Myanmar** within 24 hours of discovering a security breach, providing details on the nature of the incident, affected systems, and planned remediation efforts.

10.3.3 **Post-Incident Review**: After the incident is resolved, a post-incident review must be conducted to identify the root cause and recommend corrective actions to prevent future occurrences. Detailed incident reports should be shared with the **Central Bank of Myanmar** for auditing purposes.

11 Roles and Responsibilities

The successful operation of the MyanmarPay Digital Payment Switch depends on the collaboration of multiple stakeholders, including the Central Bank of Myanmar, system operators, and participants (e.g., banks, financial institutions, and mobile financial service providers). The following outlines the roles and responsibilities of each party:

11.1 Roles & Responsibilities of the Central Bank of Myanmar

The Central Bank of Myanmar (CBM) serves as the primary regulatory authority for the MyanmarPay Digital Payment System. Its key responsibilities include:

11.1.1 **Ownership:** The CBM is the system owner if the Myanmar Pay – Digital Payment Switch and the regulator of the system. The CBM has the right to store, access and use any data or information from and related to Digital Payment Systems in line with system.

11.1.2 **Oversight and Supervision**: The CBM is responsible for monitoring and supervising the activities of all participants in the payment system. It ensures compliance with the **Code of Conduct** and oversees the implementation of AML/CFT regulations.

11.1.3 **Policy and Standards Development**: The CBM develops and enforces the regulatory framework, technical standards, and policies required for the operation of the **MyanmarPay Digital Payment System**.

11.1.4 **System Audits and Compliance Reviews**: The CBM conducts regular audits and compliance reviews to ensure that participants adhere to security, operational, and regulatory requirements. Participants may be required to submit regular reports on their activities, including risk assessments, audit findings, and customer transaction data.

11.1.5 **Participant Onboarding and Certification**: The CBM has the authority to approve or reject new participants based on their technical readiness, financial stability, and compliance with the relevant regulatory requirements.

11.1.6 **Participant Suspension and Termination**: Suspend or Terminate the participation of any participants who violates any rules and procedures or causes any possible risks to Digital Payment System.

11.2 Roles & Responsibilities of the Digital Payment Switch

The Digital payment switch Operator, appointed by the Central Bank of Myanmar, is responsible for managing and maintaining the technical infrastructure of the MyanmarPay Digital Payment Switch. Its key responsibilities include:

11.2.1 **System Development and Maintenance**: The operator ensures that the technical infrastructure, including APIs, payment gateways, and the centralized merchant repository, functions seamlessly and is regularly updated to reflect security and performance enhancements.

11.2.2 **Fraud Monitoring and Reporting**: The operator works closely with participants to detect and mitigate fraudulent activities. It oversees the deployment of real-time monitoring systems and provides timely reports to the CBM and participants on detected fraud or suspicious activities.

11.2.3 **Technical Assistance and Support**: The operator provides technical support to participants during the integration process and ongoing

system use. This includes managing onboarding, technical testing, and certification for participants.

11.2.4 **Dispute Resolution Management**: The operator oversees the dispute resolution process by facilitating communication between participants and ensuring that disputes are escalated and resolved promptly.

11.2.5 **Data Security and Cybersecurity Monitoring**: The operator monitors the cybersecurity posture of the **MyanmarPay Digital Payment Switch** and conducts regular security assessments to detect potential vulnerabilities. It is also responsible for implementing necessary security patches and updates.

11.3 Roles & Responsibilities of the Participants

Participants (including banks, financial institutions, mobile financial service providers, and merchants) play a critical role in the MyanmarPay Digital Payment Switch. Their responsibilities include:

11.3.1 **Compliance with the Code of Conduct**: All participants must adhere to the **Code of Conduct**, including compliance with all security, AML/CFT, and operational requirements outlined by the CBM.

11.3.2 **Fraud Prevention and Risk Management**: Participants are responsible for implementing fraud detection and risk management systems that monitor transactions for suspicious activity. They must also take immediate action in the event of a security breach or fraud incident.

11.3.3 **Customer Support and Service Delivery**: Participants must provide a seamless and transparent experience to their customers. This includes offering customer support for dispute resolution, providing clear communication on fees, and ensuring smooth transaction processing.

11.3.4 **Data Security and Confidentiality**: Participants must protect the confidentiality of customer data by following the security protocols outlined in the **Code of Conduct**. This includes encrypting data, implementing access controls, and preventing unauthorized access to customer information.

11.3.5 **Training and Awareness**: Participants must ensure that their staff are well-trained on the operational, technical, and regulatory aspects of the **MyanmarPay Digital Payment Switch**. This includes providing regular AML/CFT training to employees.

11.3.6 **Reporting to the Central Bank**: Participants are required to submit regular reports to the **Central Bank of Myanmar** on their transaction volumes, risk management practices, and compliance efforts. Reports should also include audit results, fraud detection metrics, and customer dispute resolutions.

12 Reporting Requirements

To ensure transparency, compliance, and operational efficiency, all participants in the MyanmarPay Digital Payment Switch must adhere to comprehensive reporting requirements. Regular reporting allows the Central Bank of Myanmar (CBM) to monitor system performance, financial health, and compliance with regulations.

12.1 Financial and Operational Reports

Participants are required to submit the following financial and operational reports on a regular basis:

12.1.1 **Daily Settlement Reports**:
Provide detailed information on the settlement of all transactions, including payment volumes, net positions, and reconciliation results.
The report must include both financial and non-financial transactions.

12.1.2 **Transaction Summary Reports**:
A daily summary of all transactions processed through the **MyanmarPay Digital Payment Switch**, categorized by transaction type (P2P, P2M, P2G, etc.).
Must include details on any failed or rejected transactions, with reasons for the failures.

12.1.3 **Fraud Detection Reports**:
A summary of all detected fraudulent activities, including suspicious transactions, fraudulent accounts, and blocked transactions.
Reports should include corrective actions taken and any open fraud cases under investigation.

12.1.4 **AML/CFT Compliance Reports**:
Monthly reports on anti-money laundering (AML) and combating the financing of terrorism (CFT) compliance activities.
Must include details on suspicious activity reports (SARs) filed, transaction monitoring activities, and any AML/CFT training conducted for staff.

12.1.5 **Compliance Audit Reports**:
Annual compliance audit reports assessing adherence to the **Code of Conduct**, including financial, operational, and security standards.
These reports must be submitted within 30 days of the audit's completion.

12.2 Risk and Security Reports

12.2.1 **Security Incident Reports**:
Participants must immediately report any security incidents, including cyber-attacks, data breaches, and system vulnerabilities.
Incident reports must detail the nature of the incident, containment measures, and corrective actions.

12.2.2 **Quarterly Risk Management Reports**:

A quarterly overview of the participant's risk management efforts, including the identification of key risks, the effectiveness of internal controls, and steps taken to mitigate risks.

The report should also include the results of any vulnerability assessments or penetration testing conducted.

12.3 Customer and Merchant Reports

12.3.1 **Customer Satisfaction and Complaint Reports**:

Participants must submit quarterly reports summarizing customer complaints, dispute resolutions, and overall customer satisfaction ratings.

Reports should highlight recurring issues and steps taken to improve the customer experience.

12.3.2 **Merchant Acquisition and Transaction Reports**:

A quarterly report on merchant onboarding and transaction volumes, categorized by merchant type and sector.

The report should include details on the performance of merchants, any service disruptions, and merchant compliance with the **MyanmarPay Code of Conduct**.

12.4 Branding and Commercial Reports

Participants are required to adhere to the **MyanmarPay Branding Guidelines** to ensure consistency across all platforms, marketing materials, and point-of-sale touchpoints. This section outlines the required branding reports and commercial activity updates.

12.4.1 **Branding Requirements**

Participants are required to adhere to the branding guidelines detailed below to ensure proper integration with the MyanmarPay Digital Payment System:

12.4.1.1 MyanmarPay Brand Guidelines (Appendix IV)

12.4.1.2 MyanmarPay QR Stand Printing Guidelines (Appendix V)

12.4.1.3 MyanmarPay QR Stand Digital Guidelines (Appendix VI)

12.4.2 **Branding Compliance**

12.4.2.1 **Branding Approval Reports**:

Any new marketing or promotional materials featuring the **MyanmarPay** logo or branding must be submitted to the **Central Bank of Myanmar** and it's delegate for approval at least three weeks before they are used.

The branding report must include design mock-ups, usage scenarios, and proposed distribution channels (e.g., print, digital, in-store).

12.4.3 **Branding Compliance Audits**:

Participants must conduct annual audits of their branding activities to ensure compliance with the MyanmarPay Brand Guidelines.

The audit report must detail any deviations from branding standards and corrective actions taken.

12.5 Commercial Reporting

12.5.1 **Go-to-Market Plan Proposal**:
Prior to launching any new product or service under the **MyanmarPay Digital Payment Switch**, participants must submit a detailed go-to-market plan to the **Central Bank of Myanmar**.
This plan must include product details, pricing structures, marketing strategies, and target customer segments.

12.5.2 **Marketing and Penetration Reports**:
Participants are required to submit quarterly reports on marketing activities and the penetration of the **MyanmarPay** system in their customer and merchant base.
This report should include key performance indicators (KPIs), such as the number of new customer sign-ups, transaction volume growth, and merchant acquisition rates.

12.6 Commercial Agreement

Participants must submit commercial agreements template made with merchants, and compliance obligations.
The **Central Bank of Myanmar** reserves the right to review and approve these agreements to ensure fairness and transparency.

13 Policy for Settlement Banks and non-bank payment service providers

13.1 Pre-joining Requirements

Non-bank payment service providers can join MyanmarPay directly by partnering with settlement banks for transaction settlement. To ensure transparency and readiness for settlement operations, non-bank payment service providers must submit the following documents and declarations to the Central Bank of Myanmar (CBM):

13.1.1 **Settlement Bank Agreement**:

- A signed agreement between the non-bank payment service providers and their settlement bank detailing their working relationship, roles, and responsibilities.

- Confirmation that the settlement bank is aware of and consents to process transactions for the non-bank payment service providers under MyanmarPay.

13.1.2 **Settlement Bank Certification**:

- A cover letter from the settlement bank confirming that they have the capacity to process the non-bank payment service providers' projected transaction volumes.

- Central Bank of Myanmar will issue a certification letter to the non-bank payment service providers and the settlement bank upon review and approval of the submitted documentation.

13.1.3 **Participants Relationship Disclosure**:
A complete list of any other non-bank payment service providers or mobile wallets working with the settlement bank, including the bank's own wallet services

13.2 Liquidity Management and Float Allocation

Liquidity management and float requirements must comply with the policies already established under CBM-Net. Settlement banks and non-bank payment service providers are required to adhere to these existing guidelines to ensure operational efficiency. Settlement banks must maintain a **dedicated minimum reserve** in their CBM Net account for non-bank payment service providers transactions.

13.3 Limit on Non-bank payment service providers relationships per Settlement Bank for MyanmarPay

13.3.1 **Participant Capacity Review:** Settlement banks if asked by Central Bank of Myanmar should collaborate to undergo a capability assessment by CBM to determine the maximum number of non-bank payment service providers they can service without compromising operational efficiency and liquidity.

13.3.2 **Cap Enforcement:** CBM reserve the right to impose a **limit on the number of** non-bank payment service providers each settlement bank can work with, based on factors such as:

- Transaction processing capacity.
- Historical settlement performance.
- Risk management frameworks

14 General Provisions

14.1 Amendment of the Code of Conduct

14.4.1 The **Central Bank of Myanmar** reserves the right to amend or modify this **Code of Conduct** at any time. Participants will be notified of any changes at least 30 days before the amended Code goes into effect. Participants are required to review and adapt their policies and procedures accordingly to ensure continued compliance. All participants will be notified of any changes, and updates will be published on the CBM's official platforms including but not limited to CBM official websites and MyanmarPay website.

14.2 Governing Law

This **Code of Conduct** is governed by the laws and regulations of the **Republic of the Union of Myanmar**. In case of any conflict between this Code and local laws, the provisions of local law will prevail.

14.3 Confidentiality

All participants are required to maintain the confidentiality of customer information, transaction data, and any proprietary information shared during the course of participating in the MyanmarPay Digital Payment Switch. Information may only be disclosed under the following conditions:

14.3.1 To comply with legal or regulatory obligations (e.g., court orders, regulatory investigations).

14.3.2 For dispute resolution purposes, as outlined in the **Dispute Management** section of this Code.

14.3.3 To authorized personnel involved in system operations, subject to confidentiality agreements.

14.3.4 In cases involving Anti-Money Laundering (AML) and Countering the Financing of Terrorism (CFT) concerns, participating Financial Institutions are required to collaborate and share relevant information with regulatory bodies including Central Bank of Myanmar and other institutions as necessary. This collaboration must be conducted in full compliance with applicable laws and regulations, ensuring that any exchange of information is done securely, as required to address the AML/CFT issue.

14.4 Dispute Resolution

Any disputes arising from the interpretation or enforcement of this Code of Conduct shall be resolved through the dispute management process outlined in Section 5. If a resolution cannot be reached through the established dispute resolution mechanism, the matter may be escalated to the Arbitration Committee for a final decision.