Palremit ICT Security Policy

)ocument Information

olicy Type: Risk Management

olicy Owner: Compliance

\pproval: Management

\pproval Date: Apr 30, 2025

)ocument Location: Compliance/KYC/Risk Policy

ecommendation for Approval	Head of Compliance
Recommendation for Approval	Chief Operating Officer

)ocument Version : 1.0

\pproved By: Management

I hereby certify this document is a true and correct original copy

Authorized by me: .....
Date: .....
Signature: .....

PalRemit

Regulatory Compliance Framework

1. Purpose

This Regulatory Compliance Framework articulates Palremit's unwavering commitment to full compliance with all applicable Nigerian laws, financial regulations, data protection mandates, and industry-specific guidelines that govern the secure and ethical operation of digital financial services.

As a licensed and trusted fintech provider, Palremit processes large volumes of sensitive customer information, including personally identifiable data, cardholder information, and financial transaction records. The security, integrity, and lawful handling of this data are not only operational imperatives but also legal obligations and foundational to the company's license to operate.

By embedding regulatory compliance into its ICT governance framework, Palremit aims to:

1.1. Preserve customer trust by ensuring transparency, accountability, and responsible data stewardship;

1.2. Mitigate legal, financial, and reputational risks arising from non-compliance or security lapses;

1.3. Uphold the integrity of Nigeria's financial system, by actively aligning with regulatory bodies such as the Central Bank of Nigeria (CBN), the Nigeria Data Protection Commission (NDPC), and the Economic and Financial Crimes Commission (EFCC);

1.4. Promote sustainable business operations through proactive compliance with evolving regulatory expectations, including those governing Anti-Money Laundering (AML), Know Your Customer (KYC), Open Banking, and data privacy laws.

This Framework serves as a binding policy directive across all departments, systems, and personnel within Palremit. It ensures that regulatory obligations are not treated as isolated legal requirements but are deeply integrated into the company's security architecture, digital strategy, employee conduct, and customer engagement models.

2. Scope

This policy applies to all personnel and entities who interact with, manage, or influence the security posture of Palremit's Information and Communication Technology (ICT) environment. This includes, but is not limited to, employees, contractors, consultants, vendors, partners, and third-party service providers who are granted access to Palremit's digital infrastructure, financial platforms, customer data, and critical applications.

The scope extends across the entire ICT ecosystem, covering:

2.1. All individuals and teams responsible for the operation, maintenance, or development of Palremit's core banking systems, wallet infrastructure, card services, and USD account platforms;

2.2. All parties involved in the collection, processing, transmission, storage, or destruction of sensitive or regulated data, including personally identifiable information (PII) and financial records;

2.3. Any internal or external stakeholders responsible for ensuring compliance, executing audits, or enforcing controls aligned with legal and regulatory mandates;

2.4. Personnel and service providers engaged in the identification, containment, and resolution of ICT security incidents, vulnerabilities, or breaches;

2.5. All business units and individuals accountable for business continuity, disaster recovery, and the resumption of critical operations in the event of a disruption.

This policy is **binding and enforceable** across all Palremit locations, departments, systems, and external engagements. It establishes the minimum security and compliance expectations that must be upheld to ensure the protection of Palremit's digital assets, legal standing, and customer trust.

3. Policy Details

3.1 Nigeria Data Protection Regulation (NDPR)

Palremit recognizes data privacy as a fundamental right and shall ensure full and demonstrable compliance with the Nigeria Data Protection Regulation (NDPR), issued by the National Information Technology Development Agency (NITDA). As a digital financial service provider, Palremit is classified as a data controller and is thus legally obligated to implement and maintain comprehensive safeguards for the processing of personal data.

To fulfil these obligations, Palremit shall:

3.1.1. Appoint a Data Protection Officer (DPO):
A suitably qualified and competent DPO shall be appointed with full authority and independence to oversee the implementation of data protection strategies, monitor compliance with the NDPR, advise on data-related risks, and serve as the primary liaison between Palremit, regulatory authorities (including the Nigeria Data Protection Commission – NDPC), and data subjects.

3.1.2. Ensure Lawful Basis for Processing:
All personal data shall be processed only when a lawful basis under the NDPR has

been established. Explicit and informed consent shall be obtained from data subjects prior to the collection or processing of their personal data, except where another lawful ground (e.g., contractual necessity or legal obligation) applies. Palremit will clearly communicate the purpose, legal basis, and scope of processing to all customers and users.

3.1.3. Implement Technical and Organizational Measures:
Palremit will adopt and regularly update robust security controls—including but not limited to encryption, access restrictions, intrusion detection, data masking, and secure authentication to protect personal data from unauthorized access, loss, or misuse. All technical controls will be aligned with the principles of data minimization, purpose limitation, and storage limitation.

3.1.4. Facilitate Data Subject Rights:
Palremit will establish accessible processes and service channels for individuals to exercise their rights under the NDPR, including the rights to:

i. Access their personal data;

ii. Request corrections to inaccurate or incomplete data;

iii. Request deletion (“right to erasure”) where applicable;

iv. Withdraw consent without prejudice to the lawfulness of prior processing;

v. Object to certain forms of processing or automated decision-making.

3.1.5. Maintain Audit Trails and Processing Records:
A central Data Processing Register will be maintained to log all categories of data processing activities. This includes documentation of data flows, lawful bases, processing purposes, data recipients, retention periods, and data transfer mechanisms. These records will enable accountability and transparency during audits or investigations.

3.1.6. Manage Data Breaches Responsibly:
In the event of a data breach or suspected compromise of personal data, Palremit shall initiate its Incident Response Plan without delay. The DPO will lead the investigation, risk assessment, and mitigation efforts, and where required, notify the NDPC and affected individuals in accordance with NDPR breach notification timelines.

3.1.7. Conduct Regular Audits and Compliance Assessments:
Palremit shall carry out annual data protection compliance audits, conducted either internally or by a licensed Data Protection Compliance Organization (DPCO). Identified gaps or deficiencies will be documented, risk-assessed, and addressed through structured remediation plans, with board-level oversight.

3.2 Central Bank of Nigeria (CBN) Regulatory Compliance

Palremit, as a regulated fintech operating within the Nigerian financial system, affirms its full compliance with all applicable Central Bank of Nigeria (CBN) regulations, frameworks, circulars, and directives. These regulatory instruments form the bedrock of financial stability, digital trust, and consumer protection within the Nigerian financial services sector.

To uphold its obligations as a regulated entity, Palremit shall:

3.2.1. Implement and Maintain Open Banking Standards:
In line with the CBN Operational Guidelines for Open Banking, Palremit will ensure secure, standardized, and consent-driven data sharing protocols across its platforms. This includes the use of secure APIs, strong customer authentication, and data access governance that prioritizes customer privacy and transaction integrity.

3.2.2. Comply with QR Code Payments Framework:
Palremit shall fully implement controls prescribed under the CBN QR Code Payments Framework, including:

i. Transactional encryption standards;

ii. Real-time fraud detection mechanisms;

iii. Secure QR code generation, storage, and interpretation to prevent spoofing and payment redirection.

3.2.3. Integrate Regulatory Change Management:
Palremit's Compliance and Risk Management teams will actively monitor new CBN circulars, advisories, and supervisory communications. Identified regulatory changes will be assessed for risk and impact, integrated into business operations, and communicated organization-wide to ensure timely adoption and continued alignment with CBN expectations.

3.2.4. Enforce Licensing and Operational Guidelines:
Palremit will comply with any specific fintech licensing requirements issued by the CBN, including minimum capital thresholds, transaction limits, reporting obligations, cybersecurity standards, and customer service protocols. Palremit shall ensure all operations fall within the scope of its CBN-issued license.

3.2.5. Ensure Timely Regulatory Reporting:
Required reports—including suspicious activity reports, transaction summaries, and compliance attestations—shall be prepared with accuracy, approved by authorized

personnel, and submitted to the CBN within mandated timelines.

3.3 Anti-Money Laundering (AML) and Know Your Customer (KYC) Regulations

Palremit is committed to the highest standards of integrity and transparency in financial operations. To support national and international efforts against money laundering, terrorist financing, and other financial crimes, Palremit shall establish and enforce a robust Anti-Money Laundering (AML) and Know Your Customer (KYC) compliance framework in accordance with applicable laws, including:

3.31. **Customer Due Diligence (CDD):**
Palremit shall establish and maintain tiered KYC protocols tailored to the risk category of each customer segment. CDD procedures shall include identity verification, validation of official documents, biometric authentication (where applicable), and enhanced due diligence for high-risk or politically exposed persons (PEPs).

3.32. **Ongoing Customer Monitoring:**
Palremit shall implement automated and manual transaction monitoring systems capable of flagging suspicious behavior, such as structuring, unusually large transactions, inconsistent behavior patterns, and cross-border anomalies. All flagged activities will be reviewed by a trained compliance team.

3.33. **Timely Regulatory Reporting:**
All Suspicious Transaction Reports (STRs) and Currency Transaction Reports (CTRs) will be submitted in accordance with regulatory timeframes to the Nigerian Financial Intelligence Unit (NFIU). Palremit will also comply with all EFCC and CBN directives related to AML investigations and data access.

3.34. **Recordkeeping and Retention:**
Detailed records of customer identification, transactional history, communications, and compliance actions will be securely retained for a minimum of five (5) years after the cessation of the customer relationship or transaction, in accordance with regulatory requirements.

3.35. **Staff Training and Awareness:**

AML/KYC compliance is the responsibility of every employee. Palremit shall conduct mandatory, periodic training for all relevant staff to ensure awareness of financial crime risks, reporting obligations, red flags, and escalation procedures.

3.36. **Independent Audits and Program Review:**
Palremit's AML/KYC framework shall be subject to regular independent audits to assess effectiveness, detect gaps, and recommend improvements. Results will be reported to senior management and regulators as required.

4. Core Security Policy Components

Overview

Palremit's foundational security controls and operational standards are designed to protect its information systems, data assets, and digital services from unauthorized access, misuse, loss, or disruption. These security components are critical to the company's mission of delivering safe, reliable, and compliant financial technology solutions.

This phase of the policy establishes the baseline security requirements that must be adhered to by all departments and personnel, ensuring that security is not treated as a one-time activity, but rather as a continuous, organization-wide responsibility integrated into daily operations, system architecture, and customer interactions.

4.1 Data Security and Governance

Palremit shall establish and maintain comprehensive data security controls that ensure the confidentiality, integrity, and availability (CIA) of both customer and internal data across all environments (production, staging, and development).

To that end:

4.1.1. **Encryption**: All sensitive and regulated data shall be encrypted both at rest and in transit using industry-accepted cryptographic protocols (e.g., AES-256, TLS 1.2+). Encryption keys must be securely stored and managed in accordance with best practices.

4.1.2. **Access Control:** Access to data and systems will be governed by Role-Based Access Control (RBAC) principles and enforced using least privilege and need-to-know criteria. Privileged access will be reviewed and audited on a scheduled basis.

4.1.3. **Data Classification:** Palremit shall implement a data classification framework that identifies data according to sensitivity (e.g., Public, Internal, Confidential, Restricted) and prescribes handling requirements for each classification level.

4.1.4. **Security Assessments:** Regular vulnerability assessments, penetration tests, and configuration audits will be conducted to detect and remediate weaknesses. High-risk findings must be remediated within defined service-level agreements (SLAs).

4.1.5. **Backup and Recovery:** All critical data will be backed up regularly using secure, redundant systems. Backups must be tested periodically to verify restorability and meet Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO).

4.1.6. **Data Retention and Disposal:** Palremit shall enforce a data lifecycle policy in alignment with regulatory, operational, and legal requirements. Data no longer required must be securely deleted using methods that prevent reconstruction or recovery.

4.2 Privacy and Consent Management

Palremit is committed to upholding data subject rights and privacy principles as outlined in the Nigeria Data Protection Regulation (NDPR) and global best practices.

To support this commitment:

4.2.1. **Transparent Privacy Practices:** Palremit will maintain clear, accessible, and comprehensive privacy notices, detailing the nature, purpose, and lawful basis of data collection, use, sharing, and retention. These notices will be communicated at onboarding, and made readily available to all stakeholders through its website and digital platforms.

4.2.2. **Consent Management:** Systems will be in place to capture, record, and manage explicit customer consent for personal data processing activities. Consent shall be granular, revocable, and recorded as part of an auditable trail.

4.2.3. **Data Subject Rights:** Customers will be enabled to exercise their rights under the NDPR, including:

i. Right to access their personal data;

ii. Right to rectification;

iii. Right to erasure (where applicable);

iv. Right to object to processing or withdraw consent.
These requests shall be processed promptly and transparently.

4.2.4. **Privacy Impact Assessments (PIAs):** For any new or significantly changed systems, processes, or partnerships that involve personal data, a Privacy Impact

Assessment will be conducted to identify and mitigate privacy risks before deployment.

4.3 Third-Party Risk Management

Palremit acknowledges that third-party vendors, suppliers, and service providers introduce additional layers of risk. As such, the organization will implement a structured Third-Party Risk Management Program to ensure all external relationships maintain Palremit's security and compliance posture.

Key requirements include:

i. **Pre-Engagement Risk Assessments:** All vendors and third parties who access or process Palremit's data or systems must undergo a security and compliance assessment prior to onboarding.

ii. **Contractual Controls:** Vendor contracts shall include explicit clauses on data protection, security controls, incident response responsibilities, and compliance with Nigerian regulatory standards (e.g., NDPR, CBN).

iii. **Ongoing Monitoring:** All active third-party relationships shall be subject to periodic reviews, including assessments of their security practices, audit reports, and compliance status. Critical third parties will be monitored continuously.

iv. **Termination Controls**: Upon disengagement, third parties must return or securely delete all Palremit data in their possession and confirm compliance in writing.

4.4 Employee Training and Security Awareness

Human behavior remains one of the most significant risk vectors in cybersecurity. Palremit will foster a security-conscious culture by equipping all employees with the knowledge and tools necessary to uphold their responsibilities.

To ensure this:

4.4.1. **Mandatory Security Training:** All new employees will undergo **onboarding security training**, which must be completed before accessing Palremit's systems. Annual refresher courses will be mandatory for all staff.

4.4.2. **Awareness Campaigns:** Palremit will conduct **continuous awareness programs** covering current threat vectors, such as phishing, social engineering, insider threats, and mobile security.

4.4.3. **Simulated Attacks:** Controlled phishing simulations and other attack scenarios will be used to test user behavior and reinforce learning. Metrics from these simulations will guide additional training as needed.

4.4.4. **Policy Acknowledgement:** Employees are required to formally acknowledge all relevant security policies, and violations may lead to disciplinary action in line with internal HR and compliance protocols.

4.4.5. **Incident Reporting Culture:** All personnel must report security incidents, suspicious activities, or policy violations **immediately**, without fear of retaliation. Reporting channels will be clearly communicated and always accessible.

4.5. Roles and Responsibilities

4.5.1. The IT Security Team is responsible for incident monitoring, response coordination, and reporting.

4.5.2. Senior management will support incident response efforts and approve business continuity strategies.

4.5.3. The Data Protection Officer (DPO) is responsible for overseeing the implementation and monitoring of data protection measures and regulatory compliance related to the NDPR.

4.5.4. The Compliance Officer will manage adherence to CBN regulations, AML, and KYC processes and coordinate regulatory reporting activities.

4.5.5. The IT Security Team shall design, implement, and maintain security controls and conduct audits.

4.5.6. Managers are responsible for ensuring their teams comply with security policies and complete required training.

4.5.7. All employees, contractors, and third parties are required to understand and comply with this policy and report any suspected violations or breaches immediately and participate in relevant training and exercises.
.

5.0 Incident Management and Business Continuity

5.1 Purpose

Palremit is committed to maintaining the resilience, integrity, and availability of its digital services and information systems. This section outlines the processes, controls, and responsibilities established to ensure timely detection, response, recovery, and learning from ICT security incidents and service disruptions.

The goal of this policy is to:

i. Minimize operational, reputational, financial, and legal impact from ICT incidents;

ii. Safeguard customer trust and service continuity;

iii. Ensure compliance with incident reporting obligations under applicable Nigerian laws and regulatory frameworks (e.g., NDPR, CBN directives, and cybersecurity regulations).

5.2 Policy Details

5.2.1 Incident Detection and Reporting

Palremit shall deploy **continuous monitoring systems**, including automated threat detection and real-time logging tools, to detect anomalous activity and potential security breaches across its ICT infrastructure.

I. All employees, contractors, and relevant third parties are mandated to report any observed or suspected security incidents—including data breaches, malware infections, unauthorized access, system outages, or policy violations—to the IT Security Team or designated incident response coordinator immediately.

II. A clear and accessible incident reporting process shall be maintained and communicated to all staff, with predefined escalation paths based on incident severity and system criticality.

III. All alerts, anomalies, or user-reported issues will be assessed by the IT Security Team and escalated in accordance with Palremit's Incident Classification Framework.

5.2.2 Incident Response

Palremit shall maintain and regularly update a formal Incident Response Plan (IRP) that provides structured guidance for responding to a broad spectrum of ICT security incidents.

Key components of the IRP include:

i. Defined roles and responsibilities for the incident response team (including IT, legal, compliance, communications, and executive leadership);

ii. Step-by-step procedures to contain, investigate, mitigate, and recover from incidents;

iii. Preservation of digital evidence and logs to support forensic analysis and potential legal or regulatory investigations;

iv. Clear communication protocols to notify affected internal stakeholders, customers (if applicable), and external authorities (e.g., NDPC or CBN) within mandated timelines;

v. Use of incident severity ratings (e.g., Low, Medium, High, Critical) to guide urgency and resource allocation.

5.2.3 Incident Investigation and Documentation

All confirmed incidents will undergo a thorough post-incident analysis to identify root causes, contributing factors, and control failures.

I. A central **Incident Register** shall be maintained to document:

- Description of the incident;
- Timeline of events;
- Systems and data affected;
- Actions taken during containment and recovery;
- Communication activities and regulatory notifications;
- Lessons learned and recommended improvements.

II. **Post-Incident Reviews (PIRs)** shall be conducted for medium and high-severity incidents to evaluate response effectiveness, identify systemic issues, and update policies, procedures, and training materials as needed.

5.2.4 Business Continuity and Disaster Recovery

Palremit shall develop and maintain comprehensive Business Continuity Plans (BCP) and Disaster Recovery Plans (DRP) to ensure the continued delivery of critical services in the event of a disruption or disaster.

These plans shall:

I. Identify key business functions, dependencies, and associated recovery priorities;

II. Define Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs) for all essential systems;

III. Specify alternate communication channels, recovery sites, and escalation procedures;

IV. Include detailed data backup strategies, with regular testing of both data restorability and system failover capabilities;

V. Be reviewed and tested at least annually, including through simulated exercises involving both technical and non-technical staff.

Participation in these exercises is mandatory for critical team members and will be used to assess readiness and identify gaps.

5.3 Enforcement

All employees, vendors, and contractors are required to comply fully with Palremit's Incident Management and Business Continuity policies and procedures.

Failure to do so may result in:

5.3.1. Disciplinary action, up to and including termination of employment or contract;

5.3.2. Legal and regulatory exposure, including financial penalties or sanctions imposed by bodies such as the NDPC, CBN, or EFCC;

5.3.3. Loss of customer trust and reputational damage.

Palremit reserves the right to audit compliance and take corrective action where breaches of this policy are identified.

6. Review

This policy and associated plans will be reviewed and updated annually or as needed based on incident trends, technological changes, or regulatory requirements.

I hereby certify this document is a true and correct original copy

Authorized by me: .....
Date: .....
Signature: .....