Information Security Management System (ISMS)

I. Definitions

Confidential Information:

Any information, whether oral, written, electronic, or other form, disclosed by one Party ("Disclosing Party") to the other Party ("Receiving Party") that is designated as confidential or that should reasonably be understood to be confidential given the nature of the information and the circumstances of disclosure. This includes, but is not limited to, business plans, financial data, technical specifications, customer information, operational details, processes, and any data or information concerning the Disclosing Party's business or affairs.

Data:

Any information, structured or unstructured, that is collected, processed, stored, transmitted, or utilized by a Party. This includes, but is not limited to, personal data, transactional records, metadata, operational data, and information derived from the Party's systems or platforms.

Systems:

The hardware, software, platforms, networks, databases, applications, and other digital or physical components utilized by a Party to process, store, manage, or transmit data, including any proprietary or third-party systems used in connection with the services under this Agreement.

Intellectual Property (IP):

All patents, copyrights, trademarks, trade secrets, designs, databases, source code, algorithms, business processes, methodologies, and other proprietary rights, whether registered or unregistered, including any registration applications owned, developed, or licensed by a Party.

Network:

The interconnected infrastructure, including wired and wireless connections, devices, servers, routers, switches, and other hardware and software components, that facilitates the transfer, access, and exchange of data within or between Parties' systems or with external systems, as utilized in connection with the services under this Agreement.

II. Confidentiality

1.1 Ownership of Confidential Information

- All Confidential Information disclosed under this Agreement remains the exclusive property of the disclosing party ("Disclosing Party").
- The receiving party ("Receiving Party") shall treat the Confidential Information as proprietary to the Disclosing Party and safeguard it against unauthorized access, disclosure, or misuse.
- The Receiving Party acknowledges the importance and sensitivity of the Confidential Information and agrees to implement appropriate measures to maintain its confidentiality.

1.2 Authorized Disclosure

- Confidential Information may only be disclosed by the Receiving Party under the following conditions:
    - **Internal Access:** To employees, officers, agents, affiliates, advisors, consultants, potential investors, or board members ("Authorized Representatives") who require the information for the intended purpose. The Receiving Party must ensure such Authorized Representatives adhere to equivalent confidentiality obligations. Any breach by Authorized Representatives shall be treated as a breach by the Receiving Party.
    - **Legal or Regulatory Obligation:** When disclosure is mandated by applicable law, regulation, or court order. The Receiving Party shall, to the extent legally permissible, notify the Disclosing Party in advance to allow them to seek protective measures or remedies.

1.3 Exemptions from Confidentiality

The obligations under this Agreement do not apply to information that:

- **Publicly Available:** Becomes publicly available through no breach by the Receiving Party.
- **Pre-existing Knowledge:** Was in the Receiving Party's possession before disclosure, provided it was not obtained under an obligation of confidentiality.
- **Independent Development:** Is independently developed by the Receiving Party without reference to the Disclosing Party's Confidential Information.
- **Third-Party Disclosure:** Is lawfully obtained from a third party not bound by confidentiality obligations to the Disclosing Party.
- **Mandatory Disclosure:** Must be disclosed under applicable laws, regulations, or governmental requirements, provided such disclosure does not exceed what is legally required.

1.4 Remedies for Breach

- In the event of an actual or threatened breach, the Disclosing Party has the right to seek injunctive relief to prevent further breaches, in addition to other legal or equitable remedies.
- The Receiving Party agrees to indemnify the Disclosing Party for any losses, damages, or liabilities arising from unauthorized disclosure, misuse, or breach of Confidential Information.

1.5 Intellectual Property Rights

- All intellectual property rights associated with the Confidential Information remain the sole property of the Disclosing Party.
- The Receiving Party shall not acquire any rights, title, or interest in the Confidential Information except as expressly authorized by the Disclosing Party in writing.

1.6 Regulatory Compliance

- The Receiving Party acknowledges that the Disclosing Party may operate in a regulated environment and agrees to provide necessary information promptly to ensure regulatory compliance.

1.7 Return or Destruction of Confidential Information

- Upon termination or expiration of this Agreement, or at the Disclosing Party's request, the Receiving Party shall promptly return or securely destroy all copies of the Confidential Information and confirm in writing.

1.8 Survival of Obligations

- The confidentiality obligations under this Agreement remain in effect for five (5) years after termination or expiration, or as required by law.

1.9 Acknowledgment of Sensitivity

- Both parties recognize the critical nature of the Confidential Information. The Receiving Party agrees to exercise the highest degree of care to protect it, understanding that any breach may result in significant harm to the Disclosing Party.

III. Vendor Information Security/Cybersecurity

2.1 Supplier Responsibilities for System Security

- **Physical and Digital Security:**
  - Implement physical controls to restrict unauthorized access.
  - Ensure digital infrastructure adheres to industry standards for secure operations.
- **Access Control:**
  - Enforce stringent access controls with unique credentials.
  - Prohibit unauthorized password sharing.
- **Malware Protection:**
  - Maintain up-to-date antivirus software and perform regular patching.
- **Network Security:**
  - Utilize firewalls that meet industry standards to protect data traffic.
- **Audit and Forensics Support:**
  - Maintain secure logs of system access and modifications to support investigations.

2.2 Communication Security

- **Email Authentication:**

- Authenticate all communication with the organization's channels using Sender Policy Framework (SPF) and preferably DKIM and DMARC.

2.3 System Access and Incident Management

- **Access Restrictions:**
  - Limit system access to authorized personnel.
  - Notify the organization promptly of personnel changes to revoke access.
- **Incident Reporting:**
  - Notify the organization of security incidents or breaches impacting its systems or data within 24 hours.
  - Submit a root cause analysis (RCA) report within five (5) business days post-incident.

2.4 Compliance with Security Standards

- **Periodic Audits:**
  - Conduct regular internal security audits and share summaries upon request.
  - Include provisions for unannounced audits in case of suspected non-compliance or security incidents.
- **Scalability of Obligations:**
  - Adhere to relevant clauses based on the level of access or service provided.

2.5 Central Bank Oversight

- **Review and Audit by State Bank of Pakistan (SBP):**
  - Vendors must comply with requests for audits, reviews, or inspections conducted by the SBP or its appointed representatives.
  - Provide timely access to all requested documents, systems, and personnel to facilitate such reviews.
- **Compliance Obligations:**
  - Ensure all operations align with applicable SBP guidelines and directives. Non-compliance may result in immediate termination of the contract and legal proceedings.

2.6 Ongoing Risk Assessments

- Vendors are required to perform regular risk assessments to identify vulnerabilities and mitigate risks. Results of these assessments must be shared upon request.

2.7 Data Encryption Standards

- All data in transit and at rest must be encrypted using industry-standard protocols (e.g., AES-256 for encryption and TLS for transmission).

2.8 Vendor Training

- Vendors must ensure their employees undergo regular cybersecurity training.
- Training must include awareness of phishing, secure handling of data, and compliance with Mobilink Microfinance Bank Ltd policies.

2.9 Awareness Campaigns

- Vendors must participate in security awareness campaigns conducted by Mobilink Microfinance Bank Ltd if required.

IV. Audit and Review Rights for Cybersecurity and Information Security

3.1 Audit Rights of Mobilink Microfinance Bank Ltd

- **Audit Scope:**
  - Mobilink Microfinance Bank Ltd reserves the right to audit the Supplier's information security practices, including compliance with laws, regulations, and industry standards.
- **Audit Notice:**
  - Provide fourteen (14) business days' notice before conducting an audit.
- **Audit Support:**
  - The Supplier shall provide full support, including access to documents, systems, and personnel.

- **Audit Findings:**
    - Share findings and require the Supplier to address issues within a defined timeframe.
- **Material Deficiencies:**
    - Mobilink Microfinance Bank Ltd may conduct verification reviews after remediation.

3.2 Regulatory Oversight

- **State Bank of Pakistan (SBP) Audits:**
    - Vendors shall ensure full cooperation with SBP audits, including the provision of necessary access and documentation.
- **Regulatory Reporting:**

Provide periodic compliance reports as required by SBP or Mobilink Microfinance Bank