Information Security Policy

Consumer Microfinance Bank Ltd

1. Introduction

Consumer Microfinance Bank Ltd is committed to protecting the confidentiality, integrity, and availability of its information assets. This Information Security Policy outlines the principles, guidelines, and practices that must be followed by all employees, contractors, vendors, and other stakeholders who access, process, store, or transmit information on behalf of Consumer Microfinance Bank Ltd.

2. Information Classification

All information assets of Consumer Microfinance Bank Ltd must be classified based on their sensitivity and criticality. The following classification levels are defined:

a) Confidential: Information that is highly sensitive and must be protected from unauthorized access or disclosure. This includes customer personal information, financial data, trade secrets, and any other information designated as confidential by the bank.

b) Internal Use Only: Information that is for internal use within Consumer Microfinance Bank Ltd and should not be disclosed to external parties without proper authorization. This includes internal policies, procedures, and other proprietary information.

c) Public: Information that is intended for public disclosure and does not require any special protection.

3. Access Control

Access to information assets of Consumer Microfinance Bank Ltd must be granted based on the principle of least privilege. Employees, contractors, and other stakeholders should only be granted access to the information they need to perform their job responsibilities. Access to confidential information must be restricted to authorized personnel only.

4. Password Security

All employees and stakeholders with access to Consumer Microfinance Bank Ltd's information assets must use strong, unique passwords for their accounts. Passwords must be changed periodically and must not be shared with anyone else. Multi-factor authentication (MFA) should be used wherever possible to provide an additional layer of security.

5. Data Privacy

Consumer Microfinance Bank Ltd is committed to protecting the privacy of customer information in accordance with applicable laws and regulations. All employees and

stakeholders must comply with the bank's data privacy policies and procedures, including obtaining proper consent from customers for the collection, use, and disclosure of their personal information.

6. Information Handling and Transmission
All information assets of Consumer Microfinance Bank Ltd must be handled and transmitted securely. This includes using encrypted communication channels for transmitting sensitive information, not using personal email or cloud storage for storing or sharing bank information, and not transmitting information to unauthorized parties.

7. Incident Reporting and Response
All employees and stakeholders of Consumer Microfinance Bank Ltd must report any suspected or actual security incidents, such as data breaches, security vulnerabilities, or unauthorized access, to the designated security team immediately. The bank will follow an incident response plan to promptly investigate and mitigate any security incidents.

8. Physical Security
Physical access to Consumer Microfinance Bank Ltd's premises, data centers, and other sensitive areas must be restricted to authorized personnel only. Physical security measures, such as access controls, surveillance cameras, and alarms, must be in place to protect against unauthorized access or theft of information assets.

9. Information Disposal
Information that is no longer required must be disposed of securely to prevent unauthorized access. Employees and stakeholders must follow Consumer Microfinance Bank Ltd's information disposal procedures, which may include shredding paper documents, securely erasing electronic media, or using approved data destruction methods.

10. Compliance with Laws and Regulations
Consumer Microfinance Bank Ltd must comply with all applicable laws, regulations, and industry standards related to information security, including but not limited to data protection, privacy, and financial regulations. Employees and stakeholders must be aware of and comply with these requirements in their day-to-day activities.

11. Training and Awareness
Consumer Microfinance Bank Ltd will provide regular training and awareness programs to educate employees and stakeholders about information security policies, procedures, and best practices. All employees and stakeholders must participate in these training programs and demonstrate their understanding of information security requirements.

12. Non-Compliance
Non-compliance with Consumer Microfinance Bank Ltd's Information Security Policy may result in disciplinary action, up to and including termination of employment or

contract, and legal actions, as applicable. Non-compliance can have serious consequences, including but not limited to:

Breach of Confidentiality: Failure to follow the policy may result in unauthorized access, use, or disclosure of confidential information, such as customer personal information, financial data, or trade secrets, which can lead to reputational damage, financial losses, and legal liabilities.

Data Breaches: Non-compliance with information security policies may increase the risk of data breaches, which can result in the loss, theft, or unauthorized disclosure of sensitive information, leading to financial losses, regulatory penalties, and legal actions.

Legal and Regulatory Compliance Issues: Non-compliance with laws, regulations, and industry standards related to information security, such as data protection and privacy laws, can result in regulatory fines, legal actions, and damage to the bank's reputation.

Disruption of Operations: Failure to follow information security policies may result in disruptions to the bank's operations, such as system downtime, loss of data, or inability to provide services to customers, which can result in financial losses, customer dissatisfaction, and reputational damage.

Reputational Damage: Non-compliance with information security policies can erode consumer trust and confidence in the bank, leading to reputational damage, loss of customers, and negative impact on the bank's brand image, which can have long-term consequences for the bank's success.

Legal Liability: Non-compliance with information security policies may result in legal liabilities for the bank, including lawsuits, claims, and financial damages, which can have a significant financial impact on the bank's operations and profitability.

It is the responsibility of all employees, contractors, vendors, and stakeholders to comply with Consumer Microfinance Bank Ltd's Information Security Policy to protect the bank's information assets and maintain the confidentiality, integrity, and availability of information. Any suspected or actual non-compliance should be immediately reported to the designated security team for appropriate actions to be taken.